Doctoral Thesis

Post-Quantum Provable Security in Symmetric-Key Cryptography

共通鍵暗号技術の耐量子証明可能安全性

HOSOYAMADA Akinori

Graduate School of Engineering,
Nagoya University

Acknowledgments

First of all, I would like to express my sincere gratitude to my supervisor Associate Professor Tetsu Iwata for his kind and invaluable advice, patience, and continuous support of my Ph.D study. I could not obtain the results and write this thesis without his kind encouragement and guidance, and I was quite fortunate to be a student of such a good supervisor. Moreover, I greatly appreciate the jury members of this thesis, Professor Nobuo Kawaguchi, Professor Shinji Doki, and Associate Professor Tomoyuki Morimae (Kyoto University) for reviewing drafts and providing insightful comments.

My sincere thanks also goes to (ex-)members of cryptographic research groups in NTT Corporation, especially to Dr. Kazumaro Aoki (current Associate Professor of Bunkyo University), Dr. Yu Sasaki, Dr. Yosuke Todo, and Dr. Kan Yasuda, for teaching me lots of things from the very basics of symmetric-key cryptography such as what cryptographic primitives are to how to write papers. Discussions and experiences of collaborative works with other (ex-)members are also invaluable, and I thank all of them.

I also would like to thank my parents and grandparents for their long-standing supports. Lastly, I express hearty appreciation to my wife for her understanding, patience, and encouragement on writing this thesis.

Abstract

This paper studies provable security of symmetric-key schemes against adversaries that have quantum computers from both theoretical and practical perspectives.

Provable security is a way to mathematically guarantee the security of a cryptosystem, by showing a theorem that expresses the upper bound on the success probability of an adversary that has specified resources. Most of modern cryptosystems are shown to be secure in the provable security paradigm under some assumptions, e.g., the hardness of certain algebraic problems, or the existence of another secure cryptographic primitive. Sometimes security proofs are provided in an ideal model where the oracle of an ideally random primitive, e.g., a truly random function, is publicly available. Whether a cryptographic primitive can be built from another primitive is a central problem in the theory of cryptology. In addition, if an existing scheme is proven to resist more powerful attacks than previously thought, or if we can prove that a new efficient scheme is secure, the proofs have practical importance. Thus provable security is important both theoretically and practically.

In symmetric cryptology, (tweakable) block ciphers, pseudorandom functions (PRFs), and hash functions play central roles as fundamental underlying primitives to build other cryptosystems such as authenticated encryption schemes. Hence the provable security of such schemes is well-studied.

One of the most important results on provable security is the one on the Luby-Rackoff construction. The Luby-Rackoff construction, or the Feistel construction, is among the most important approaches to construct secure block ciphers from secure pseudorandom functions (PRFs). The 3-round and 4-round Luby-Rackoff construction are proven to be a pseudorandom permutation (PRP) and a strong PRP, i.e., they are secure against chosen-plaintext attacks (CPAs) and chosen-ciphertext attacks (CCAs), respectively. Another important result on block ciphers is the one by Liskov, Rivest, and Wagner. They showed constructions to convert secure block ciphers into secure tweakable block ciphers, which are called the LRW constructions. As for constructions to convert Merkle-Damgård hash functions into message authentication codes (MACs) or PRFs in a provably secure manner, there has been a long line of research on HMAC and NMAC. They are proven to be secure up to $O(2^{n/2})$ computations when the output length is n bits.

On the other hand, their security has not been studied enough in the setting where adversaries have quantum computers, and many important problems have yet to be solved. On the Luby-Rackoff construction, Kuwakado and Morii showed that a quantum superposed chosen-plaintext attack (qCPA) can distinguish the 3-round construction from a random permutation in polynomial time. In addition, Ito et al. showed a quantum superposed chosen-ciphertext attack (qCCA) that distinguishes the 4-round Luby-Rackoff construction. Since Kuwakado and Morii showed the result, a problem of much interest has been how many rounds are sufficient to achieve provable security against quantum query attacks. Though several years have passed since then, the problem still remains open. Similarly, since Kaplan et al. showed the LRW construction can be broken with a polynomial-time qCPA, it has been open whether there exists a mode of block ciphers to build quantum-secure tweakable block ciphers. For HMAC and NMAC, Song and Yun showed that they are quantum pseudorandom functions (qPRFs) under the standard assumption that the underlying compression function is a qPRF. Their proof guarantees security up to $O(2^{n/5})$ or $O(2^{n/8})$ quantum queries. However, there is a gap between the provable security bound and a simple distinguishing attack that uses $O(2^{n/3})$ quantum queries.

This paper settles these problems. First, we prove that the 4-round Luby-Rackoff construction is secure up to $O(2^{n/6})$ quantum queries, where n is the length of inputs and outputs of the construction. We also prove that the bound is tight by showing an attack that distinguishes the 4-round Luby-Rackoff construction from a random permutation with $O(2^{n/6})$ quantum queries. Our result is the first to demonstrate the tight security of a typical block-cipher construction against quantum query attacks, without any algebraic assumptions.

Second, we show the first design of quantum-secure tweakable block ciphers based on quantum-secure block ciphers, and present a provable security bound. Our construction is simple, and when instantiated with a quantum-secure n-bit block cipher, it is secure against attacks that query arbitrary quantum superpositions of plaintexts and tweaks up to $O(2^{n/6})$ quantum queries.

Third, we close the gap between the security bound and the distinguishing attack of HMAC and NMAC. Specifically,

we show that the tight bound of the number of quantum queries to distinguish HMAC or NMAC from a random function is $\Theta(2^{n/3})$ in the quantum random oracle model, where compression functions are modeled as quantum random oracles.

We use an alternative formalization of Zhandry's compressed oracle technique to provide security proofs in the quantum setting. In addition, to show the tight security bound of HMAC and NMAC, we introduce a new proof technique based on the compressed oracle technique, focusing on the symmetry of quantum query records.

Furthermore, we show the classical indifferentiability of the SKINNY-HASH internal function. SKINNY-HASH is a family of function-based sponge hash functions, and it was selected as one of the second round candidates of the NIST lightweight cryptography competition. Its internal function is constructed from the tweakable block cipher SKINNY. The construction of the internal function is very simple and the designers claim n-bit security, where n is the block length of SKINNY. However, a formal security proof of this claim is not given in the original specification of SKINNY-HASH. In this paper, we formally prove that the internal function of SKINNY-HASH has n-bit security, i.e., it is indifferentiable from a random oracle up to $O(2^n)$ queries, substantiating the security claim of the designers. Though the result on the SKINNY-HASH internal function is a classical one, it is unlikely to be broken by quantum attacks. In addition, when post-quantum security of the SKINNY-HASH internal function will be proved, the proof will be based on our classical proof. Thus we believe it will help understanding post-quantum security of hash functions.

The results on the Luby-Rackoff construction and quantum-secure tweakable block ciphers are significant mainly from a theoretical perspective. On the other hand, the results on HMAC and NMAC, and the SKINNY-HASH internal function, are important mainly from a practical perspective.

Contents

List of Figures

Chapter 1

Introduction

1.1 Overview

Cryptography is one of the most important technologies for today's information security. When we visit web sites of which URL begins with "https", use online meeting services, or pay with credit cards, cryptography is used to protect our data.

Very roughly speaking, cryptographic schemes can be classified into two types: symmetric-key schemes and public-key schemes. Symmetric-key schemes realize secure communication between two parties that have a common secret key, which has to be shared in advance. On the other hand, public-key schemes do not require pre-shared secret key.

Public-key schemes often use algebraic structures such as integer factoring and discrete logarithm to realize the high functionality that encryption key can be public, and their security is guaranteed under the assumption that certain algebraic problems are hard to solve. Operations such as encryption and decryption of public-key schemes are relatively slow since they require heavy computation to utilize algebraic properties. On the other hand, operations of symmetric-key schemes are very fast because they do not require algebraic structures usually. For instance, our experiments show a typical symmetric-key encryption scheme (AES-128 with CBC mode) requires only about 9×10^{-4} milliseconds to encrypt a single 2048-bit message on average, while 2048-bit RSA requires 5×10^{-2} milliseconds. [1]

Secure and efficient telecommunication is realized by combining the speed of symmetric-key schemes with the high functionality of public-key schemes. Both of the two types of schemes are indispensable.

In general, there are two ways to guarantee security of a cryptographic scheme $\mathcal{S}$. One is studying *attacks* on $\mathcal{S}$. If $\mathcal{S}$ is not broken after much efforts are devoted to cryptanalysis, the community reaches the consensus that $\mathcal{S}$ is secure. The other one is showing *provable security*. In the provable security paradigm, the security of a scheme $\mathcal{S}$ is shown as a theorem that provides an upper bound $p(t, d)$ of the probability that an adversary $\mathcal{A}$ succeeds to break $\mathcal{S}$, where the t and d represent the amount computational resources such as time and data available to $\mathcal{A}$. [2] Such a theorem strongly guarantees the security of $\mathcal{S}$ in the sense that there does not exist any adversary of which success probability exceeds the upper bound $p(t, d)$ as long as the amount of available time and data are up to t and d, no matter what strategy the adversary takes.

Post-quantum security of symmetric-key schemes. In 1994, Shor showed quantum algorithms that efficiently solve integer factoring and discrete logarithm problems [Sho94, Sho97], which lead to breaking widely used public-key schemes such as RSA and elliptic curve cryptosystems in polynomial time. Since then, much efforts have been devoted to realize schemes that will remain secure even after the realization of large-scale, reliable universal quantum computers. The area to study such schemes is called *post-quantum cryptography*, which is currently one of the most active research areas in cryptography. Though the power of today's quantum computers is not strong enough to break popular schemes such as 2048-bit RSA, the schemes that are broken by Shor's algorithm should be replaced with post-quantum ones soon because a significant technical breakthrough to build large-scale and reliable universal quantum computers may be realized just today. National Institute of Standards and Technology (NIST, the United States) is holding the standardization process for post-quantum *public-key* schemes such as public-key encryption, key-establishment algorithms, and signatures [Nat16]. Currently used public-key schemes such as RSA cryptosystems will be replaced with post-quantum ones in a near future.

[1] For the experiments, we used the `openssl speed [algorithm]` command (`algorithm = aes-128-cbc` or `rsa2048`) with Ubuntu 20.04, OpenSSL 1.1.1f, and AMD Ryzen 5 3500.

[2] What computational resources are taken into account in the theorem varies depending on how we model adversaries.

As mentioned before, both of symmetric-key and public-key schemes are indispensable for today's information security. In the post-quantum era, it is desirable that we have some evidence that *symmetric-key* schemes also have post-quantum security. Studying post-quantum security of typical symmetric-key schemes is also an interesting problem from the view point of cryptographic theories.

See Fig. 1.1 for a list of typical symmetric-key primitives. In Fig. 1.1, those at higher levels are relatively high-functioning ones, which are often built from relatively low-functioning ones at lower levels. For instance, some message authentication codes are built from hash functions or (tweakable) block ciphers. Sometimes low-functioning primitives are built from high-functioning ones to achieve a specific goal, e.g., data processing performance. (Note that the words "high-functioning" and "low-functioning" are not technical terms with precise definition. We ambiguously use them just for intuitive explanations. In addition, there is no special meaning to whether a primitive is located to the left/right of another primitive in Fig. 1.1.) Recall that a *mode of (tweakable) block ciphers* is a construction that converts block ciphers into other symmetric-key schemes, e.g., TBCs, MACs, and (authenticated) encryption schemes. "Encryption mode" in the figure denotes a mode to build encryption schemes. Besides, "Permutation / Function" at the bottom of the figure means public permutations and functions with fixed input/output length.

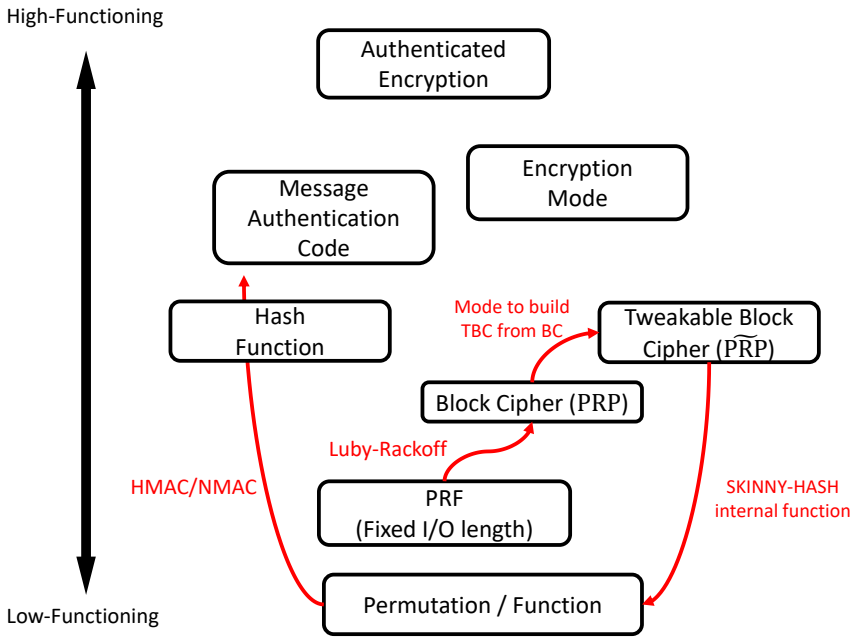


Figure 1.1: List of symmetric-key schemes.

Next, we explain two attack models for adversaries with quantum computers. One model is that there exists an adversary $\mathcal{A}$ that has a quantum computer and the *classical* keyed oracle of the target cryptographic scheme is available to $\mathcal{A}$. For instance, suppose we are considering about a block cipher E_k and the (classical) encryption oracle is available. $\mathcal{A}$ can query arbitrary n-bit string x and the oracle returns $E_k(x)$. $\mathcal{A}$ tries to break E_k by making queries and using its own quantum computer. This attack model is called Q1 model in [KLLN16b]. Another attack model is that $\mathcal{A}$ has a quantum computer and the *quantum* keyed oracle of the target scheme is available. Here, the quantum oracle of the block cipher E_k is the oracle such that, $\mathcal{A}$ can query arbitrary quantum superposition of $2n$-bit strings such as $\sum_{x,y} \alpha_{x,y} |x\rangle |y\rangle$, and the oracle returns the answer $\sum_{x,y} \alpha_{x,y} |x\rangle |y \oplus E_k(x)\rangle$ also in quantum superposition. The quantum oracle of other schemes is defined in the same way. This attack model is called Q2 model, and attacks in the Q2 model is called *quantum query attacks*.

If a scheme $\mathcal{S}$ is proven to be secure in the Q1 and Q2 model, $\mathcal{S}$ is said to have *standard security* and *quantum security*, respectively [Zha12a]. [3] It is a problem of much interest whether a classically secure and efficient scheme also

[3]Please do not confuse the notions of standard/quantum security with the standard model or the *quantum random oracle model* [BDF+11]. The two notions are independent of the models, and it is possible that a scheme has quantum security in the standard model or standard security in the quantum random oracle model. (The quantum random oracle model is the one where there exists the quantum oracle of an ideally random function and the standard model is the one where existence of such ideal primitives are not assumed. The term "quantum random oracle" may denote another notion in other research areas, but throughout the paper we assume that it denotes the quantum oracle of a random function, following the usual

has quantum security. In a future where much computations and communications are done in quantum superpositions, some cryptographic schemes that rely on classical primitives will be running on quantum computers. Indeed, some recently proposed quantum schemes are based on classical primitives. For instance, the candidate construction of pseudorandom unitary operators by Ji et al. [JLS18] is constructed from pseudorandom permutations (PRPs). In such a situation where classical cryptographic schemes are implemented on quantum computers, it is natural to assume that adversaries mount quantum query attacks on them.

The focus of this paper. There already exist many interesting results on quantum attacks on various concrete symmetric-key schemes [KM10, KM12, KLLN16a]. On the other hand, many basic and important problems about provable (post-)quantum security of symmetric-key schemes such as the Luby-Rackoff constructions have yet to be solved. For instance:

1. In the classical setting, the r-round Luby-Rackoff construction is proven to be secure against chosen-plaintext attack (CPAs). However, it is open whether it becomes secure against quantum chosen-plaintext attacks (qCPAs) for some r. Here, a qCPA on a block cipher E_k is a quantum query attack on E_k in the setting where the quantum oracle of E_k is available.
2. It is unknown whether there exists a mode of block ciphers to build quantum-secure tweakable block ciphers.
3. Song and Yun showed that HMAC and NMAC are quantum-secure pseudorandom functions (qPRFs) under the standard assumption that the underlying compression function is a qPRF [SY17]. Their proof guarantees security up to $O(2^{n/5})$ or $O(2^{n/8})$ quantum queries when the output length of HMAC and NMAC is n bits. However, there is a gap between the provable security bound and a simple distinguishing attack that uses $O(2^{n/3})$ quantum queries.

This paper settles these problems. That is, we show the following results.

1. A proof that the 4-round Luby-Rackoff construction is secure against qCPAs, i.e., it is a quantum-secure pseudorandom permutation (qPRP). We also prove that our security bound is tight by showing a matching attack.
2. A new mode of operation to build tweakable block ciphers from block ciphers and a proof that it has quantum security if the underlying block cipher is quantum-secure.
3. The tight quantum security proof of HMAC and NMAC in the quantum random oracle model (QROM) where the compression function is modeled as a quantum random oracle.

To provide these results, we heavily use an alternative formalization of Zhandry's compressed oracle technique [Zha19]. Moreover, we give a *classical* security proof that the SKINNY-HASH internal function is indifferentiable from a random oracle. Though we cannot prove its (post-)quantum security due to technical limitations, it will lead to understanding post-quantum security of hash functions. See also Fig. 1.1 about which result implies what kind of relations between symmetric-key schemes.

The following five sections provide a more detailed overview of each result. Section 1.2, Section 1.3, and Section 1.4 overview the results on the 4-round Luby-Rackoff construction, the new mode to build quantum-secure tweakable block ciphers, and HMAC/NMAC, respectively. Section 1.5 briefly explain the compressed oracle technique and our alternative formalization. Section 1.6 describes the result on the SKINNY-HASH internal function.

1.2 Tight qPRP Security Proof of the 4-Round Luby-Rackoff Construction

The Luby-Rackoff construction is one of the most important approaches to convert pseudorandom functions (PRFs) into PRPs. It is also called the Feistel construction. Due to its efficiency and security, a significant number of block ciphers including commonly used ones such as DES [Nat77] and Camellia [AIK+00] were designed on the basis of this construction.

For families of functions $f_i := \{f_{i,k} : \{0,1\}^{n/2} \to \{0,1\}^{n/2}\}_{k\in\mathcal{K}}$ that are parameterized by k in a key space $\mathcal{K}$ $(1 \le i \le r)$, the r-round Luby-Rackoff construction $\mathsf{LR}_r(f_1, \ldots, f_r)$ is defined as follows: First, keys $k_1, \ldots, k_r$ are chosen independently and uniformly at random from $\mathcal{K}$. For each input $x_0 = x_{0L}\|x_{0R}$, where $x_{0L}, x_{0R} \in \{0,1\}^{n/2}$, the state is updated as

$$x_{(i-1)L}\|x_{(i-1)R} \mapsto x_{iL}\|x_{iR} := x_{(i-1)R} \oplus f_{i,k_i}(x_{(i-1)L})\|x_{(i-1)L} \tag{1.1}$$

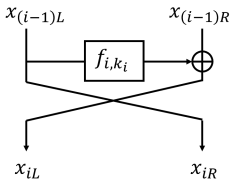


Figure 1.2: The i-th round state update.

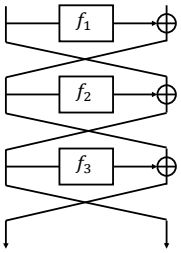


Figure 1.3: The 3-round Luby-Rackoff construction.

for $i = 1, \ldots, r$ in a sequential order. The output is the final state $x_r = x_{rL} \| x_{rR}$. Then the resulting function becomes a keyed permutation over $\{0,1\}^n$ with keys in $(\mathcal{K})^r$. See also Fig. 1.2 and see Fig. 1.3.

In the classical setting, if each f_i is a secure PRF, LR_r becomes a secure PRP against chosen-plaintext attacks (CPAs) for $r \geq 3$ and a secure PRP against chosen-ciphertext attacks (CCAs) for $r \geq 4$ [LR85]. (That is, LR_r becomes a strong PRP. Recall that a PRP P_k is called a strong PRP if it is indistinguishable from a random permutation, even if adversaries make queries not only to P_k but also its inverse P_k^{-1}.) However, in the quantum setting, Kuwakado and Morii showed that LR_3 can be distinguished in polynomial time from a truly random permutation by a qCPA [KM10] (qCPA).[4] Moreover, Ito et al. showed that LR_4 can be distinguished in polynomial time by a quantum chosen-ciphertext attack (qCCA) [IHM+19].[5] On the other hand, for any r, no quantum security proof of LR_r is known.

Importance of Proving Quantum Security of the Luby-Rackoff Construction. As we mentioned in Section 1.1, it is a problem of much interest whether a classically secure and efficient scheme also has quantum security. Though Zhandry have already shown that we can covert quantum-secure PRFs into quantum-secure PRPs by using constructions of format preserving encryption [Zha16], the conversion with the Luby-Rackoff constructions is much more efficient and thus preferable. Hence, it is important to study whether quantum security proof for the r-round Luby-Rackoff construction is feasible for some r, and if so, to determine the minimum number of r such that we can prove the post-quantum security of LR_r.

1.2.1 Our Contributions

As the first step to giving post-quantum security proofs for the Luby-Rackoff constructions, this paper shows that the 4-round Luby-Rackoff construction LR_4 is secure against qCPAs. Roughly speaking, a qCPA denotes an attack by an adversary that has a quantum computer and can access the quantum encryption oracle $O_{\mathsf{LR4}} : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus \mathsf{LR}_4(x)\rangle$, which allows the adversary to make quantum queries to LR_4. In particular, we give a security bound of LR_4 against qCPAs when all round functions are truly random functions. We also prove that the bound is tight by showing a matching attack. Concretely, we show the following theorems.

Theorem 1 (Lower bound and upper bound, informal)**.** *If all round functions are truly random functions, then the following claims hold.*

1. LR_4 *cannot be distinguished from a truly random permutation by qCPAs up to* $O(2^{n/6})$ *quantum queries.*
2. *A quantum algorithm exists that distinguishes* LR_4 *from a truly random permutation with a constant probability by making* $O(2^{n/6})$ *quantum chosen-plaintext queries.*

Theorem 2 (Construction of qPRP from qPRF, informal)**.** *Suppose that each* f_i *is a secure PRF against efficient quantum query attacks, for* $1 \leq i \leq 4$*. Then* $\mathsf{LR}_4(f_1, f_2, f_3, f_4)$ *is a secure PRP against efficient qCPAs.*

The proofs are provided in Chapter 4.

Remark 1. *Secure PRFs against quantum query attacks can be constructed from post-quantum secure pseudorandom generators or pseudorandom synthesizers, or based on the LWE assumption, as shown by Zhandry [Zha12a].*

convention in cryptology.)

[4]Strictly speaking, the attack by Kuwakado and Morii works only when all round functions are keyed permutations. Kaplan et al. [KLLN16a] showed that the attack works for more general cases.

[5]A qCCA on the block cipher E_k is a quantum query attack in the setting where not only the quantum oracle of E_k but also the quantum oracle of D_k is available.

1.3 Provably Quantum-Secure Tweakable Block Ciphers

Recall that a block cipher (BC) is a keyed permutation, i.e., it takes a plaintext and a key as input to output a ciphertext, and a tweakable block cipher (TBC) takes additional input called a tweak. TBCs have wide applications in symmetric key cryptography, as they can be used to construct message authentication codes and authenticated encryption schemes, see e.g. [Rog04, IMPS17, BGIM19, IKMP20]. The notion of TBC was first formalized by Liskov, Rivest, and Wagner [LRW02, LRW11]. They introduced two TBC constructions and proved that TBCs can be constructed from BCs in the classical setting[6]. However, Kaplan et al. showed that these constructions are broken in polynomial time when adversaries have access to quantum encryption oracles [KLLN16a][7]. There has been no proposal of modes of BCs to build TBCs that are proven to be secure against quantum query attacks so far, and the existence of such modes remains open. In this paper, we consider the following question:

Does there exist a mode to build quantum-secure TBCs from quantum-secure BCs?

1.3.1 Our Contributions

We give a positive answer to the question in the reduction-based provable security paradigm by giving the first construction of quantum-secure TBCs from quantum-secure BCs. Our construction, which we call LRWQ, has a simple structure and is based on one of the two constructions by Liskov, Rivest, and Wagner. If the underlying BC is an n-bit BC with k-bit keys, then LRWQ becomes an n-bit TBC with $3k$-bit keys and n-bit tweaks. We show that LRWQ is indistinguishable from tweakable random permutations up to $O(2^{n/6})$ quantum queries[8] in the setting that adversaries can query arbitrary superpositions of plaintexts and tweaks, i.e., we prove security against qCPAs.

Our result is theoretically significant in the sense that we for the first time showed that quantum-secure tweakable pseudorandom permutations ($\widetilde{\text{qPRP}}$s) can be constructed from qPRPs (which establishes the fact that the existence of $\widetilde{\text{qPRP}}$ is theoretically equivalent to the existence of qPRP). The problem of whether a cryptographic primitive can be constructed from another primitive (whether there exists a reduction) is fundamental and theoretically the most important in cryptology. In addition, since Theorem 2 guarantees that $\widetilde{\text{qPRP}}$s can be obtained from qPRFs through 4-round Feistel cipher, our result establishes the fact that $\widetilde{\text{qPRP}}$s can be obtained from qPRFs.

On a practical side, it is plausible to assume AES [Nat01] to be a qPRP given that there has been no devastating quantum attack despite of recent efforts on quantum cryptanalysis on it. Thus, we can certainly obtain $\widetilde{\text{qPRP}}$ by instantiating LRWQ with AES. This means that our result enables us to directly benefit from recent efforts for quantum cryptanalysis on AES [GLRS16, BNS19, JNRV20].

Remark 2. *To obtain a* $\widetilde{\text{qPRP}}$*, one obvious approach is to verify whether existing native TBCs are quantum-secure (or design new ones), instead of using our mode* LRWQ*. However, these two approaches do not negate the other, but complement each other, i.e., our result gives another choice to construct* $\widetilde{\text{qPRP}}$ *for users. Even if there exists a quantum-secure native TBC, this does not invalidate our result.*

Remark 3. *This paper does not provide security proofs against qCCAs, as our construction is broken if the decryption oracle is available even in the classical setting, which is also the case for one of the original constructions by Liskov, Rivest, and Wagner. Showing existence of TBCs that are secure against qCCAs is an interesting future work. Note that TBCs that are secure against chosen-plaintext attacks (which is not secure against chosen-ciphertext attacks) can be used to instantiate various efficient message authentication codes and authenticated encryption schemes, e.g., ZMAC [IMPS17], ZOTR [BGIM19], and Romulus [IKMP20]. Therefore, TBCs that are secure against qCPAs are relevant.*[9]

1.4 On Tight Quantum Security Bound of HMAC and NMAC in the QROM

Message authentication codes (MACs) are the most important symmetric-key schemes to achieve data integrity. Some of them including block cipher based MACs such as CBC-MAC [BKR94, BKR00, BR00, BR05, IK03] and PMAC [BR02]

[6]Only a single construction is introduced in the journal version of the paper [LRW11], but an additional construction is also introduced in the preliminary (conference) version of the paper [LRW02].

[7]Kaplan et al. showed a quantum attack only for one of the two TBC constructions by Liskov, Rivest, and Wagner, but the attack can also be applied to the other construction. See Section 5.1.1.

[8]Here, we consider n as a security parameter.

[9]We note that the argument here is to illustrate the relevance of TBCs that are secure against CPAs. We are not claiming that the modes are secure against quantum attacks. We also note that there are BC-based authenticated encryption modes that do not use the decryption of BCs, such as CCM [WHF02], GCM [MV04], and OTR [Min14].

do not have quantum security, since there exist polynomial time attacks on them [KLLN16a]. However, they have standard security since their classical security proofs remain valid if adversaries are allowed to make only classical queries to keyed oracles and the underlying block ciphers are post-quantum secure.

On the other hand, classical security proofs are not necessarily applicable to the (post-quantum) standard security for hash based MACs where the proofs use idealized models such as the random oracle model (when underlying hash functions are built on the Merkle-Damgård construction, e.g., SHA-2 [Nat15a]) or the ideal permutation model (when underlying hash functions are built on the sponge construction, e.g., SHA-3 [Nat15b]). Since adversaries can implement compression functions and permutations used in the hash functions on their own quantum computers to make quantum queries, the security of hash based MACs should be proven in the corresponding idealized quantum models such as the QROM [BDF+11] or quantum ideal permutation model [AR17, HY18].

The main focus here is to study the tight quantum pseudorandom function security (qPRF security) of HMAC and its variant NMAC [BCK96], which are the most basic and important constructions to convert Merkle-Damgård hash functions into pseudorandom functions (PRFs) or MACs, in the QROM where compression functions are modeled as quantum random oracles (QROs)[10].

1.4.1 HMAC and NMAC

For a compression function $h : \{0,1\}^{m+n} \to \{0,1\}^n$, the Merkle-Damgård construction MD^h is defined as follows[11]: Let $IV \in \{0,1\}^n$ be a fixed public initialization vector. For each input message $M \in \{0,1\}^*$, the construction pads M (with a fixed padding function) and splits it into m-bit message blocks $M[1], \ldots, M[\ell]$. The state is first set as $S_0 := IV$, and iteratively updated as $S_{i+1} := h(M[i+1]||S_i)$, and S_ℓ becomes the final output. We assume $m \geq n$, which is the case for usual concrete hash functions such as SHA-2.

For a key length $k \leq m$, HMAC is defined to be the keyed function $\mathsf{HMAC}^h : \{0,1\}^k \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$ such that

$$\mathsf{HMAC}^h(K, IV, M) := \mathsf{MD}^h(IV, K_{out}||\mathsf{MD}^h(IV, K_{in}||M)). \tag{1.2}$$

Here, $K_{in} := (K||0^{m-k}) \oplus \mathsf{ipad}$, $K_{out} := (K||0^{m-k}) \oplus \mathsf{opad}$, and $\mathsf{ipad}, \mathsf{opad} \in \{0,1\}^m$ are fixed and public constants such that $\mathsf{ipad} \neq \mathsf{opad}$. We sometimes write $\mathsf{HMAC}^h_K(IV, M)$ to denote $\mathsf{HMAC}^h(K, IV, M)$ for simplicity. See also Fig. 1.4.

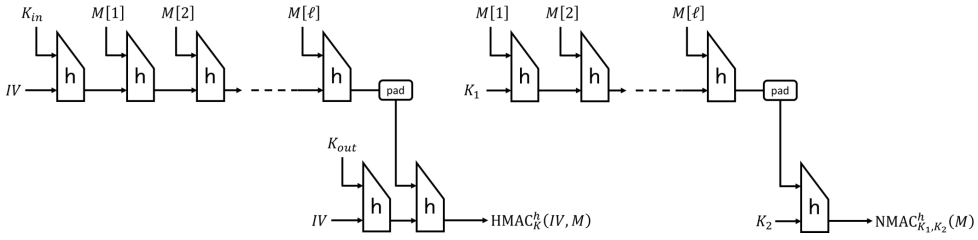


Figure 1.4: HMAC and NMAC. Note that $\mathsf{pad}(M) = M[1]||\cdots||M[\ell]$.

NMAC is a two-key variant of HMAC. Mathematically, it is a keyed function $\mathsf{NMAC}^h : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^* \to \{0,1\}^n$ defined by

$$\mathsf{NMAC}^h(K_1, K_2, M) := \mathsf{MD}^h(K_2, \mathsf{MD}^h(K_1, M)). \tag{1.3}$$

Here, $K_1, K_2 \in \{0,1\}^n$ are chosen independently and uniformly at random.[12] We sometimes write $\mathsf{NMAC}^h_{K_1,K_2}(M)$ instead of $\mathsf{NMAC}^h(K_1, K_2, M)$ for simplicity. See also Fig. 1.4.

1.4.2 Quantum Security of HMAC and NMAC

Simple Quantum distinguishing attacks on HMAC and NMAC. There are two simple quantum attacks to distinguish HMAC from a random function. Suppose that we are given an oracle O that is either of HMAC or a random function, in addition to the quantum random oracle h.

[10] "HMAC" is an abbreviation of "Hash-based MAC". "N" of "NMAC" is the initial of "Nested".

[11] n is the length of chaining values, and m is the length of message blocks.

[12] Note that there is no IV involved in NMAC.

The first attack is the one that tries to recover the secret key K. Once we succeed in recovering the correct key K (when O is HMAC) or realizing that there is no plausible candidate for K (when O a random function), we can distinguish HMAC from a random function. Since the exhaustive key search of k-bit keys can be done with $O(2^{k/2})$ queries by using Grover's algorithm [Gro96], we can distinguish HMAC from a random function with $O(2^{k/2})$ quantum queries.

The second attack uses a collision for O. Suppose that the padding function pad in the Merkle-Damgård construction satisfies the condition that there exists a function $\mathsf{p} : \mathbb{Z}_{\geq 0} \to \{0,1\}^*$ such that $\mathsf{pad}(M) = M||\mathsf{p}(|M|)$, which is the case for usual hash functions such as SHA-2. First, we try to find $M, M' \in \{0,1\}^m$ such that $O(M) = O(M')$, which can be done with $O(2^{n/3})$ quantum queries by using the BHT algorithm [BHT97, BHT98]. When we find such messages, we check whether $O(M||0^m) = O(M'||0^m)$ holds. This equality holds with a constant probability if O is HMAC, but it holds with a negligible probability if O is a random function. Thus, we can distinguish HMAC from a random function with $O(2^{n/3})$ quantum queries.

From the discussion above, HMAC can be distinguished with $O(\min\{2^{n/3}, 2^{k/2}\})$ quantum queries. This gives an upper bound of the query complexity to distinguish HMAC. The attacks are also applicable for NMAC, and $O(\min\{2^{n/3}, 2^{2n/2}\}) = O(2^{n/3})$ is an upper bound of the query complexity to distinguish NMAC.

Previous Results on Quantum Security of HMAC and NMAC. Song and Yun proved that HMAC and NMAC become quantum-secure pseudorandom functions (qPRFs) against polynomial-time quantum adversaries in the *standard model* under the assumption that $h(\cdot||K) : \{0,1\}^m \to \{0,1\}^n$ is a qPRF when $K \in \{0,1\}^n$ is randomly chosen [SY17]. They for the first time showed that HMAC and NMAC are secure even in the quantum setting, which has great importance in theory because it enables domain extension for qPRFs.

Roughly speaking, their proof guarantees security up to $O(2^{n/5})$ or $O(2^{n/8})$ quantum queries when the underlying function h_K is ideally random for each key K.[13] In other words, $\Omega(2^{n/5})$ or $\Omega(2^{n/8})$ is currently the best proven lower bound of quantum query complexity to distinguish HMAC or NMAC from a random function.

Results in standard models and those in (quantum) random oracles are not directly comparable, but there exists a large gap between the current best lower bound and the upper bound $O(2^{n/3})$ (when k is large enough) given in the above distinguishing attacks.

The gap between $\Omega(2^{n/5})$ (or $\Omega(2^{n/8})$) and $O(2^{n/3})$ may not be significant in an ideal world where adversaries are modeled as polynomial-time machines, but it is indeed significant in the real world applications, which we explain below.

Closing the Gap. In the real world, closing the gap between $\Omega(2^{n/5})$ (or $\Omega(2^{n/8})$) and $O(2^{n/3})$ is relevant for the following reasons.

Recall that there exist two security notions in the quantum setting: quantum security and standard security. The standard security of HMAC will have practical importance in a very near future because it is quite reasonable to assume that an adversary has a quantum computer on which h is implemented, but the attack target (HMAC) is implemented on a classical device.

Now, the problem is that exiting results guarantee the security of HMAC and NMAC only up to $O(2^{n/5})$ or $O(2^{n/8})$ queries, not only for the quantum security but also for the standard security (in the QROM). This is problematic since when HMAC is instantiated with SHA-256, where $n = 256$, the security is not guaranteed after about $2^{n/5} \approx 2^{52}$ (or $2^{n/8} \approx 2^{32}$) *classical* queries. It is completely unacceptable in practice, as the number is modest even with the current standard, and is too small to guarantee a longer term security.

In theory, the security up to $O(2^{n/3})$ queries can be guaranteed with the previous result if the security parameter is changed from n to $5n/3$ (or $8n/3$), by replacing the underlying hash function with the one with a longer output length. However, in the real world, it requires many years to change parameters or primitives of widely used symmetric-key cryptosystems such as HMAC, or sometimes it is simply infeasible, as we illustrate below:

- Some small IoT devices (e.g., RFID tags) need MACs but do not have enough area for hardware implementation of primitives with large parameters.
- Some banking systems are still using Triple-DES although 20 years have already passed after the standardization of AES [ANS17]. This is because even a small change (changing the block cipher) in financial systems is too costly.
- Artificial satellites require MACs to prevent accepting commands from malicious attackers. Changing primitives embedded as hardware is infeasible after satellites are launched into the outer space [SF12].

[13] Actually, the previous work [SY17] did not give concrete security bound, but we can reasonably deduce that the security is guaranteed up to $O(2^{n/8})$ quantum queries. We have the bound $O(2^{n/5})$ instead of $O(2^{n/8})$ if we assume a conjecture. We will elaborate this in Section 6.1.

Hence, giving a precise security bound is relevant from a practical view point, and is one of the most important topics to study in symmetric-key cryptography, even if the improvement will be from $O(2^{n/5})$ (or $O(2^{n/8})$) to $O(2^{n/3})$.

We also note that there has been a long line of research to close the gap for HMAC and NMAC in the classical setting, and it was eventually addressed by Gazi et al. at CRYPTO 2014 [GPR14] showing the upper bound and the matching lower bound. However, the analysis in the quantum setting does not reach this point, and closing the gap is important also from a theoretical view point.

1.4.3 Our Contributions

We show the following theorem, which shows that the tight bound of the number of quantum queries to distinguish HMAC or NMAC from a random function is in $\Theta(2^{n/3})$ (when k is large enough).

Theorem 3 (Lower bound, informal)**.** *Suppose that the maximum length of messages that we can query to HMAC, NMAC, or a random function* RF *(which is independent of h) is at most $m \cdot \ell$. Then, the following claims hold in the model where h is a quantum random oracle.*

1. *To distinguish HMAC from* RF *with a constant probability by making at most Q queries to HMAC or* RF *and at most q_h queries to h, $q_h \cdot \ell^{5/3} + Q \cdot \ell^{5/3} \geq \Omega(2^{n/3})$, or $q_h + Q \cdot \ell \geq \Omega(2^{k/2})$ have to be satisfied.*

2. *To distinguish NMAC from* RF *with a constant probability by making at most Q queries to NMAC or* RF *and at most q_h queries to h, $q_h \cdot \ell^{5/3} + Q \cdot \ell^{5/3} \geq \Omega(2^{n/3})$ has to be satisfied.*

Remark 4. *Our tightness claim focuses on the number of quantum queries, neglecting the effect of the lengths of the queries. Nevertheless, our result still has practical importance. For instance, when HMAC-SHA-256 is used to authenticate TCP/IP packets on Ethernet, $\ell < 32$ always holds since Maximum Segment Size (MSS) is about 1500-byte. In such a use-case our result guarantees about 85-bit security ($2^{n/3} \approx 2^{85}$ for $n = 256$), while previous works do only about 52-bit security or 32-bit security (in the QROM).*

Remark 5. *Some readers may think that results in the standard model are always superior to those in the (Q)ROM, but we emphasize that the standard model and (Q)ROM are theoretically incomparable.*

1.4.4 Limitations and Future Directions

Our security bound is tight and any further improvement is impossible in terms of the number of queries. However, there is a room for improvement in terms of the length of messages. When an adversary makes a single classical query of very long length (e.g., a message of $m \cdot 2^{n/5}$ bits, or equivalently $\ell = 2^{n/5}$) to the keyed oracle of HMAC or NMAC, our result no longer guarantees any security. (Note that this does not invalidate the practical importance of our result. See Remark 4 for details.) However, we do not find any quantum attack that actually breaks the security of HMAC or NMAC by making only a few queries of which length is $O(m \cdot 2^{n/5})$, and we expect that there does not exist such an attack. Improving the security bound in terms of message lengths is an interesting future work.

1.5 An Alternative Formalization of the Compressed Oracle Technique

One challenging obstacle to giving security proofs against adversaries that make quantum queries is that we cannot record *transcripts* of quantum queries and answers. Most classical security proofs implicitly rely on the property that we can copy and store queries made to oracles and their answers for free. However, it is highly non-trivial how to store them in the quantum setting, since measuring or copying (parts of) quantum states will lead to perturbing them, which may be detected by adversaries. (In Section 3.1 we will briefly explain the reason that copying and recording queries is important in classical security proofs, and why it is hard when adversaries make quantum queries.)

Zhandry's *compressed oracle technique* [Zha19] enables us to overcome the obstacle when oracles are truly random functions. The technique is so powerful that it is applied to prove quantum security of lots of schemes, e.g., Fujisaki-Okamoto transformation [Zha19] and Fiat-Shamir transformation [LZ19b]. It is also applied to show the tight security bound to find a multicollision of a random function [LZ19a]. His crucial observation is that we can record queries and answers without affecting quantum states by appropriately forgetting previous records. In addition, he observed that transcripts of queries can be recorded in an compressed manner, which enables us to simulate random functions (random oracles) extremely efficiently.

Zhandry's formalization enables us not only to record queries but also to compress recorded data, which leads to efficient simulation of a random oracle. However, security proofs of symmetric-key mode of operations often involve

the analysis of information theoretic adversaries, where we do not care about efficient simulation of a random oracle, and thus do not have to compress databases. With this in mind, we modify the construction of Zhandry's compressed standard oracle and give an alternative formalization of his technique without compressing databases that can be used when we focus on (quantum) information theoretic security. All the quantum security proofs we will provide in later chapters rely on the alternative formalization of the compressed oracle technique.

Our formulation is different from the original one not only in that efficient simulation of a random oracle is omitted but also in that the *encoding* and *decoding* of databases are realized so that the intuition behind them is clear as much as possible: Roughly speaking, when an adversary makes a query, the compressed oracle first decodes superposition of databases into the uniform superposition of all functions, responds to the adversary, and then encodes the functions into databases. The encoding and decoding in the original formulation are realized as a single theoretically sophisticated unitary operator, but their link to the intuition behind the encoding and decoding is not apparent. On the other hand, we represent the encoding and decoding as the composition of simple three unitary operators, each of which corresponds to an intuitive and concrete manipulation, so that the intuition behind each operation is clear as much as possible.

Moreover, we scrutinize the properties of our modified oracle and observe that its behaviors can be described in an intuitively clear manner by introducing some *error terms*. We also explicitly describe error terms, which enables us to give mathematically rigorous proofs. We name our alternative oracle the *recording standard oracle with errors*, because it records transcripts of queries and its behavior is described with error terms.

We believe that our alternative formalization and analyses for our oracle's behavior help us understand Zhandry's technique better, which will lead to the technique being applied even more widely.

Details on the compressed oracle technique and the alternative formalization are provided in Chapter 3.

1.6 Classical Security Proof of the SKINNY-HASH Internal Functions

The sponge construction is one of the most basic constructions to convert a function or permutation into a cryptographic hash function. It is used in many modern cryptographic hash functions including SHA-3 [Nat15b].

The sponge construction based on $F : \{0,1\}^b \to \{0,1\}^b$, where F is a public permutation or a public function, has two positive parameters r and c such that $r + c = b$. Given an input $M \in \{0,1\}^*$, the hash value is computed as follows: First, M is padded so that its length is a multiple of r. Let $M[1]||\cdots||M[L] \in \{0,1\}^{rL}$ be the message after padding, where $M[i] \in \{0,1\}^r$ for each i. Second, the internal states $st_0, \ldots, st_L \in \{0,1\}^b$ are computed in a sequential order as $st_0 := IV$ and $st_i := F(st_{i-1} \oplus (M[i]||0^c))$ for $1 \le i \le L$, where $IV \in \{0,1\}^b$ is an initialization vector. (This phase is called the absorbing phase.) Third, the internal states $st_{L+1}, \ldots, st_{L+h-1}$ and the output value $H = H[1]\cdots||H[h] \in \{0,1\}^{rh}$ ($H[i] \in \{0,1\}^r$) are computed as $st_{L+i} := F(st_{L+i-1})$ for $1 \le i \le h-1$ and $H[i] :=$ (the most significant r bits of st_{L+i-1}). (This phase is called the squeezing phase[14].) H is truncated if necessary. See Fig. 1.5.

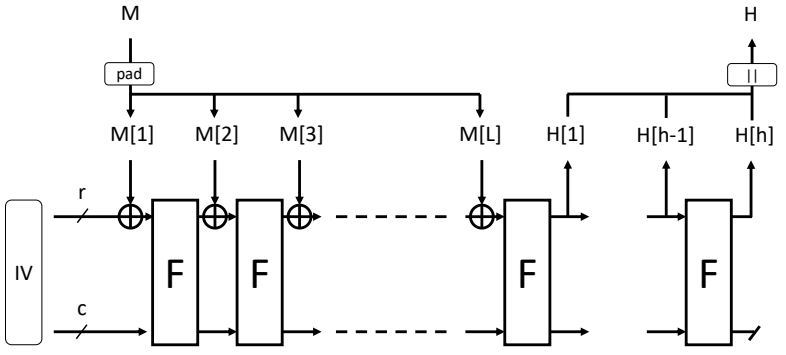


Figure 1.5: The sponge construction.

[14]In some concrete hash functions, the parameters r and c are changed to other parameters r' and c' such that $r' + c' = b$ in the squeezing phase.

The sponge construction is proven to be indifferentiable from a random oracle up to $O(2^{c/2})$ queries when F is a random oracle or an ideal permutation [BDPA08], and an appropriate padding function is chosen. That is, if a cryptosystem is proven to be secure in the random oracle model, the security of the cryptosystem does not decrease even if we replace the random oracle with the sponge construction, as long as the number of queries made to F through the sponge construction or the direct computation of F (and F^{-1}, if F is a permutation) is $O(2^{c/2})$.

Since the sponge construction is proven to be secure, to realize a secure cryptographic hash function, it is sufficient to construct a secure function or permutation F. There are two possible ways to realize such F.

One approach is to design a dedicated function or permutation from scratch. Most sponge-based hash functions including SHA-3 take this approach. For instance, SHA-3 uses a dedicated 1600-bit permutation as F. The other approach is to construct F from well-established primitives such as block ciphers or tweakable block ciphers, which is taken by the SKINNY-HASH function family.

1.6.1 SKINNY-HASH Internal Functions

SKINNY-HASH [BJK+20] is a family of function-based sponge constructions, which was the second-round candidate of the NIST lightweight cryptography competition [Nat20]. It consists of SKINNY-tk2-Hash and SKINNY-tk3-Hash, which are the sponge constructions with $b = 256$ and $b = 384$, and the internal functions are built with the tweakable block ciphers SKINNY-128-256 and SKINNY-128-384 [BJK+16], respectively.

SKINNY-128-256 is a tweakable permutation $\tilde{E}^{256}_{tk} : \{0,1\}^{128} \to \{0,1\}^{128}$, where the tweakey tk is chosen from $\{0,1\}^{256}$. Similarly, SKINNY-128-384 is a tweakable permutation $\tilde{E}^{384}_{tk}$ on $\{0,1\}^{128}$, where the tweakey tk is chosen from $\{0,1\}^{384}$. $\tilde{E}^{256}_{tk}$ and $\tilde{E}^{384}_{tk}$ are expected to be secure and suitable to instantiate ideal ciphers of which the block length is 128 bits and the key lengths are 256 bits and 384 bits, respectively.

The internal functions $F_{256} : \{0,1\}^{256} \to \{0,1\}^{256}$ and $F_{384} : \{0,1\}^{384} \to \{0,1\}^{384}$ of SKINNY-tk2-Hash and SKINNY-tk3-Hash are defined by

$$F_{256}(x) := \tilde{E}^{256}_x(c_1)||\tilde{E}^{256}_x(c_2)$$

and

$$F_{384}(x) := \tilde{E}^{384}_x(c_1)||\tilde{E}^{384}_x(c_2)||\tilde{E}^{384}_x(c_3),$$

respectively, where c_1, c_2, c_3 are distinct 128-bit constants (see Fig. 1.6).

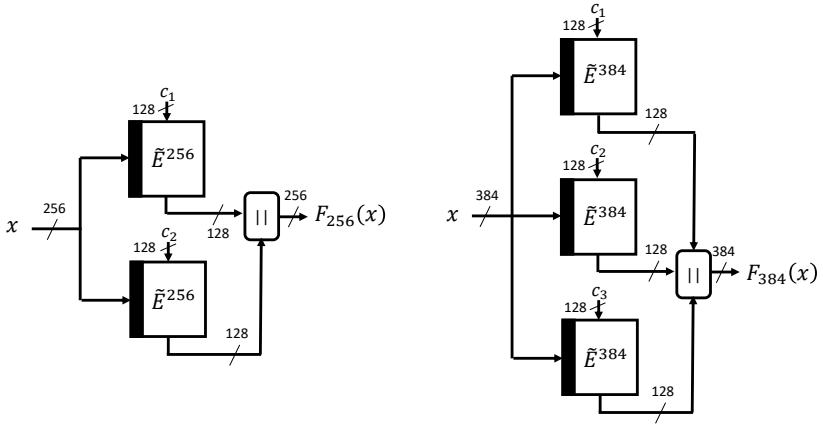


Figure 1.6: The SKINNY-HASH internal functions F_{256} and F_{384}.

In the specification of SKINNY-HASH, the designers claim that "The function F_{256} is indifferentiable from a 256-bit random function up to $O(2^{128})$ queries." and "The same intuitive argument applies to F_{384}. However, the bound is worse than the one for F_{256} by a factor of 3...".

Their design and security claim are notable since F_{256} and F_{384} achieve n-bit security from an n-bit tweakable block cipher although the designs of the functions are quite simple (just a few parallel applications of tweakable block ciphers). On the other hand, when we build a compression function (to be used in the Merkle-Damgård construction)

based on (tweakable) block ciphers, even the known approaches to achieve the same level of security require more complex constructions [Nai11, HK14].

Observe that F_{256} and F_{384} do not give a perfect random function. If we write $F_{256}(x) = Y_1||Y_2$, then $Y_1 = Y_2$ never happens. Similarly, if we write $F_{384}(x) = Y_1||Y_2||Y_3$, then for any $i \neq j$, $Y_i = Y_j$ is impossible. The n-bit security claim comes from the intuition that these are the only events that make them different from a truly random function. However, there is no formal proof for the n-bit security claim. Generally, it is highly favorable that a mode of operation of (tweakable) block ciphers has formal security proofs when a security claim is provided.

1.6.2 Our Contributions

In this paper, we give a formal proof of the indifferentiability of the SKINNY-HASH internal functions F_{256} and F_{384} in the ideal cipher model. In fact, we show a more general theorem: Let E be an n-bit block cipher with ℓn-bit key, where ℓ is a small constant. Define $F^E : \{0,1\}^{\ell n} \to \{0,1\}^{\ell n}$ be the function defined by

$$F^E(x) := E_x(c_1)||\cdots||E_x(c_\ell), \tag{1.4}$$

where $c_1, \ldots, c_\ell$ are fixed distinct n-bit constants. We call F^E the SHI function ("SHI function" is an abbreviation of SKINNY-HASH Internal function). We show the following theorem.

Theorem 4 (Indifferentiability of the SHI function, informal)**.** *If E is an ideal cipher, the SHI function F^E is indifferentiable from a random oracle as long as the total number of queries made to E and its inverse E^{-1} are in $o(2^n)$.*

This theorem shows that the SHI function has n-bit security, as claimed by the designers. Since the structure of SKINNY-HASH internal functions and the generalization F^E is quite simple and the security is very high, we believe that more and more function-based sponge constructions will be developed and used in practical situations relying on the SHI construction and our security proof.

Details of the result on the SHI function are provided in Chapter 7.

Implications in Post-Quantum Cryptography. For the SHI function, this paper provides only a *classical* security proof due to technical limitations. Nevertheless, we still think that the result has some implications in post-quantum cryptography. Though we do not have any post-quantum security proof of the SHI function, it is unlikely to be broken by quantum attacks. Hence we will be able to build post-quantum secure hash functions based on the SHI function. The SHI function is an important example of an internal function for function-based sponge hash because there does not exist many other instances. Thus it will also play an important role when we understand post-quantum security of function-based sponge hash functions. Moreover, when post-quantum security of the SHI function will be proved, the proof will be based on our classical proof. Therefore our result will help future studies on post-quantum security of hash functions.

1.7 Summary of Contributions

In summary, we obtained results on post-quantum security in symmetric-key cryptography from the perspective of both theory and practice. On the theoretical side, this paper provides answers to two theoretically important, unresolved problems. One is whether the r-round Luby-Rackoff construction is a secure qPRP for some $r \geq 4$ (Section 1.2 and Chapter 4). The other is whether we can build a quantum-secure tweakable block cipher from a quantum-secure block cipher (Section 1.3 and Chapter 5). On the practical side, we prove the tight security bound of HMAC and NMAC in the quantum random oracle model (Section 1.4 and Chapter 6), and show a formal security proof of the SKINNY-HASH internal function (Section 1.6 and Chapter 7). Though the result on the SKINNY-HASH internal function is in the classical setting, it has an implication in post-quantum security in the sense that quantum proofs will be based on our classical proof. The results related to the compressed oracle technique (Section 1.5 and Chapter 3) are technical ones that help us prove quantum security.

The relationship between the results (except for the ones on the compressed oracle technique) are as follows. See also Fig. 1.1. The first result on the Luby-Rackoff construction shows how to convert qPRFs into qPRPs (quantum-secure block ciphers) in an efficient manner. The second result shows how to achieve a quantum-secure TBC based on qPRPs. Together with the result on the Luby-Rackoff construction, the second one also guarantees that we can build a quantum-secure TBC if there exists a qPRF. The third result on HMAC and NMAC shows that we can achieve an efficient and highly (quantum-)secure MACs from a hash function, or a compression function of fixed input-output

length. The fourth result on the SKINNY-HASH internal function shows how to make a function of fixed input-output length from a TBC in a provably secure manner.

1.8 Related Works

Other than the ones introduced above, security proofs against quantum query adversaries for symmetric key schemes include a proof for standard modes of operations by Targhi et al. [ATTU16], one for the Carter-Wegman message authentication codes (MACs) by Boneh and Zhandry [BZ13], and one for Davies-Meyer and Merkle-Damgård constructions by Hosoyamada and Yasuda [HY18]. Czajkowski et al. showed quantum security of random sponge, which can be seen as a variant of CBC-MAC [CHS19]. Zhandry showed the PRP-PRF switching lemma in the quantum setting [Zha15]. Czajkowski et al. showed that the sponge construction is *collapsing* (collapsing is a quantum extension of the classical notion of collision-resistance) when round functions are one-way random permutations or functions [CBH+18]. Alagic and Russell proved that polynomial-time attacks against symmetric-key schemes that use Simon's algorithm can be prevented by replacing XOR operations with modular additions on the basis of an algebraic hardness assumption [AR17]. However, Bonnetain and Naya-Plasecia showed that the countermeasure is not practical [BN18]. For standard security proofs (against quantum adversaries that make only classical queries) for symmetric-schemes, Mennink and Szepieniec proved security for XOR of PRPs [MS17]. There are various notions on quantum MAC security such as EUF-qCMA security [BZ13] and blind unforgeability [AMRS20]. There also exists another security notion for one-time MAC security [GYZ17]. MACs built from qPRFs satisfy all these security notions. The SHI function is quite similar to a function proposed in a previous work [CNL+08, Section 4.4]. The difference of the SHI function from the function in [CNL+08] is that, while the domain and the range of the SHI function are the same since it is supposed to be used in the sponge construction, the domain of the function in [CNL+08] is larger than its range since it is supposed to be used as a compression function in the Merkle-Damgård construction. In addition, while the previous work shows collision-resistance, this paper shows the indifferentiability.

1.9 Paper Organization

The rest of the paper is organized as follows. Chapter 2 describes notations, definitions, and some basic lemmas used in later chapters. Chapter 3 duscusses the compressed oracle technique and introduce an alternative formalization, which is used in quantum security proofs in Chapter 4, Chapter 5, and Chapter 6. Chapter 4 proves that the 4-round Luby-Rackoff construction is a qPRP and its tight quantum security bound is $\Theta(2^{n/6})$. Chapter 5 shows the new construction LRWQ that converts BCs into TBCs and proves that it is a quantum-secure TBC. Chapter 6 proves that the tight quantum security bound of HMAC and NMAC is $\Theta(2^{n/3})$ in the QROM. Chapter 7 provides a formal security proof that the SKINNY-HASH internal function is indifferentiable from a random oracle. Chapter 8 concludes the paper. Besides, a summary of important notations, technical terms and their abbreviations is provided in Appendix A and show the publication list in Appendix B. See also Fig. 1.7.

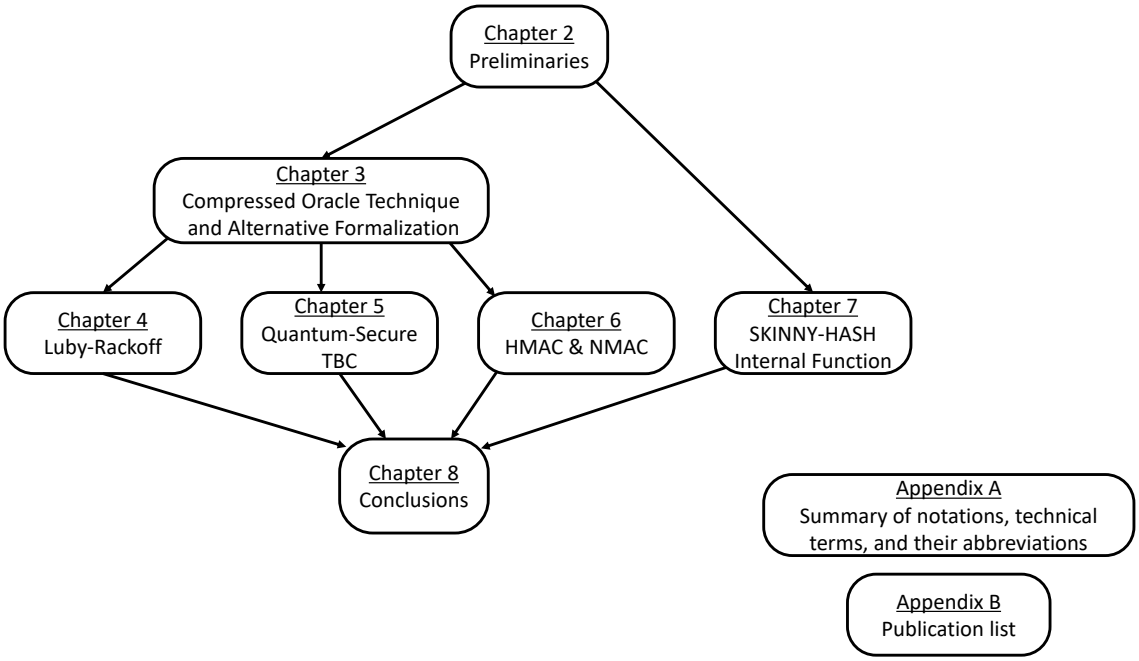


Figure 1.7: Paper organization.

Chapter 2

Preliminaries

This chapter describes notations, definitions, and some basic lemmas used in later chapters. Throughout the paper, algorithms and oracles are quantum algorithms and quantum oracles except for Chapter 7, unless otherwise noted.

2.1 Basic Notations

For any finite sets X and Y, let $\mathsf{Func}(X, Y)$ denote the set of all functions from X to Y, and let $\mathsf{Perm}(X)$ denote the set of all permutations on X. For any n-bit string x, we denote the left-half $n/2$-bits of x by x_L and the right-half $n/2$-bits by x_R, respectively. We identify the set $\{0,1\}^m$ with the set of the integers $\{0, 1, \ldots, 2^m - 1\}$. For bit strings $X \in \{0,1\}^m$ and $Y \in \{0,1\}^n$, let $X||Y \in \{0,1\}^{m+n}$ denote the concatenation of X and Y. For each bit string X of finite length, let $|X|$ denote the length of X in bits. For a positive integer m, $\mathrm{GF}(2^m)$ denotes the finite field of order 2^m. We identify the set of bit strings $\{0,1\}^m$ with the set of integers $\{0, 1, \ldots, 2^m - 1\}$ unless otherwise noted. $\{0,1\}^*$ denotes the set $\coprod_{n=0}^{\infty}\{0,1\}^n$, where $\{0,1\}^0$ denotes the set that includes only the empty string. For a positive integer m, $(\{0,1\}^m)^+$ denotes the set $\coprod_{i=1}^{\infty}\{0,1\}^{im}$. We say that a function $f : \mathbb{Z}_{\geq 0} \to \mathbb{R}$ is negligible if, for arbitrary constant $c > 0$, there exists a sufficiently large integer N such that $|f(n)| \leq 1/n^c$ for all $n \geq N$.

2.2 Primitives

A keyed function F is a function from a product space $\{0,1\}^k \times \{0,1\}^m$ to another space $\{0,1\}^n$, where $\{0,1\}^k$ is called the key space of F. We denote the function $F(K, \cdot) : \{0,1\}^m \to \{0,1\}^n$ by $F_K(\cdot)$ for each key $K \in \{0,1\}^k$.

A block cipher (BC) is a keyed function $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ such that $E_K(\cdot)$ is a permutation for each key K. Let E^{-1} denote the inverse of E defined by $E^{-1}(K, E(K, M)) = M$ for all $M \in \{0,1\}^n$. We often write $E_K(\cdot)$ and $E_K^{-1}(\cdot)$ instead of $E(K, \cdot)$ and $E^{-1}(K, \cdot)$, respectively.

A tweakable block cipher (TBC) is a keyed function $\tilde{E} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ such that $\tilde{E}(K, T, \cdot)$ is a permutation on $\{0,1\}^n$ for each $K \in \{0,1\}^k$ and $T \in \{0,1\}^t$. The space $\{0,1\}^t$ is called the tweak space of $\tilde{E}$. Let $\tilde{E}^{-1}$ denote the inverse of $\tilde{E}$ defined by $\tilde{E}^{-1}(K, T, \tilde{E}(K, T, M)) = M$ for every K, T, and M. We often write $\tilde{E}_K^T(M)$ and $(\tilde{E}^{-1})_K^T$ instead of $\tilde{E}(K, T, M)$ and $\tilde{E^{-1}}(K, T, M)$, respectively.

2.3 Basics of Quantum Computations

This section briefly recalls basics of quantum computations. Note that the explanations in this section are not comprehensive. See textbooks such as [NC10] for complete explanations. How we model (oracle-aided) quantum algorithms is described in the next section.

In the theory of classical computation, information and data such as a state of an algorithm are described by bits, which are represented by elements in $\{0,1\}^n$ for some n. On the other hand, in the theory of quantum computation, information and data are described by *qubits*, which are quantum systems that are represented by unit vectors of a 2^n-dimensional Hilbert space $\mathcal{H}$ for some n. (In fact, this is an explanation for pure states. An explanation for more general mixed states will be given later. Besides, two states $|\phi\rangle$ and $c\,|\phi\rangle$ for $c \in \mathbb{C}^\times$ are identified.) The inner product of two vectors $|\phi\rangle, |\psi\rangle \in \mathcal{H}$ is denoted by $\langle\phi|\psi\rangle$, and the norm of $|\phi\rangle$ is denoted by $\| |\phi\rangle \|$. The function $\langle\phi|\cdot\rangle : \mathcal{H} \to \mathbf{C}$ (i.e., the element in the dual space $\mathcal{H}^*$) is denoted by $\langle\phi|$. In addition, by $|\phi\rangle\langle\psi|$ we denote the operator defined by $|\phi\rangle\langle\psi|\,(|\eta\rangle) = \langle\psi|\eta\rangle\,|\phi\rangle$.

We fix a basis of $\mathcal{H}$ and label the 2^n basis vectors as $|0\cdots00\rangle, |0\cdots01\rangle, \ldots, |1\cdots11\rangle$, and call it the *computational basis*. A classical bit string $x \in \{0,1\}^n$ is identified with the vector $|x\rangle$. By using the computational basis, arbitrary (pure) quantum state $|\phi\rangle$ is described as

$$|\phi\rangle = \sum_{x\in\{0,1\}^n} \alpha_x |x\rangle, \tag{2.1}$$

where $\alpha_0, \alpha_1, \ldots, \alpha_{2^n-1} \in \mathbb{C}$ satisfy $\sum_x |\alpha_x|^2 = 1$. The equation (2.1) implies that the quantum state $|\phi\rangle$ can take a "superposition" of the classical states $0\cdots00, 0\cdots01, \ldots, 1\cdots11 \in \{0,1\}^n$ with the weight function α.

Suppose there exists another quantum system described with a 2^m-dimensional Hilbert space $\mathcal{H}'$. Then the joint system of the two quantum systems is described with the tensor product $\mathcal{H}\otimes\mathcal{H}'$. We assume that its computational basis is $\{|x\rangle|y\rangle\}_{x\in\{0,1\}^n, y\in\{0,1\}^m}$, where the computational basis of $\mathcal{H}'$ is $\{|y\rangle\}_{y\in\{0,1\}^m}$. (We often omit writing the symbol "$\otimes$" and denote $|x\rangle\otimes|y\rangle$ by $|x\rangle|y\rangle$ or $|xy\rangle$, for simplicity.)

Very roughly speaking, arbitrary operation on quantum states is described by a combination of (i) unitary operators, (ii) embedding into a larger system, (iii) measurements, and (iv) partial trace. First, we explain (i)-(iii).

(i) The operation that is described by a unitary operator U changes a state $|\phi\rangle$ to $U|\phi\rangle$. The important characteristic of this operation is *reversibility*. The original state $|\phi\rangle$ can be obtained from $U|\phi\rangle$ by applying the conjugate operator U^* (in practice it may be hard to implement U^*, though).

(ii) An operation of embedding changes a state $|\phi\rangle$ into another state $|\phi\rangle\otimes|\psi\rangle \in \mathcal{H}\otimes\mathcal{H}'$ of a larger system for some $|\psi\rangle \in \mathcal{H}'$.

(iii) Let $S := \{P_i : \mathcal{H} \to \mathcal{H}\}_{1\le i\le s}$ be a set of operators such that (a) $P_i^* = P_i$ for each i, (b) P_iP_j is equal to P_i if $i = j$ and equal to 0 otherwise, and (c) $\sum_{1\le i\le s} P_i = I$ (I is the identity operator). The measurement with S is a operation that changes $|\phi\rangle$ into $P_i|\phi\rangle/\|P_i|\phi\rangle\|$ and outputs the information that we measured i, with probability $p_i := \|P_i|\phi\rangle\|^2$. This operation is irreversible.

Below we give a few examples of (iii).
Example 1: Measurement by the computational basis. Let $S_c := \{P_x := |x\rangle\langle x|\}_{x\in\{0,1\}^n}$. Then it is straightforward to check S_c satisfies the properties (a)-(c). When we measure $|\phi\rangle$ with S_c, we obtain a classical bit string x and the state changes to $|x\rangle$ with probability $p_x = \|(|x\rangle\langle x|)|\phi\rangle\|^2 = \|\alpha_x|x\rangle\|^2 = |\alpha_x|^2$. We call this measurement the measurement with the computational basis.

Example 2: Partial measurement with the computational basis. Suppose $|\psi\rangle$ is in $\mathcal{H}\otimes\mathcal{H}'$, where $\dim(\mathcal{H}) = 2^n$ and $\dim(\mathcal{H}') = 2^m$. The computational basis of $\mathcal{H}$ and $\mathcal{H}'$ is $\{|x\rangle\}_{x\in\{0,1\}^n}$ and $\{|y\rangle\}_{y\in\{0,1\}^m}$, respectively. $|\psi\rangle$ can be described as $|\psi\rangle = \sum_{x,y}\beta_{x,y}|x\rangle|y\rangle$, where $\beta_{x,y}$ satisfies $\sum_{x,y}|\beta_{x,y}|^2 = 1$. Now, let $S_{cp} := \{P'_x := |x\rangle\langle x|\otimes I_m\}_{x\in\{0,1\}^n}$, where I_m is the identity operator on $\mathcal{H}'$. Then S_{cp} satisfies the properties (a)-(c). When we measure $|\psi\rangle$ with S_{cp}, we obtain a classical bit string x with probability $p'_x = \|(|x\rangle\langle x|\otimes I_m)|\psi\rangle\|^2 = \|\sum_y \beta_{x,y}|x\rangle|y\rangle\|^2 = |\sum_y\beta_{x,y}|^2$. Intuitively, the measurement with S_{cp} partially measures the leftmost n-qubits of $|\psi\rangle$ with the computational basis. We call this measurement (and similar measurements that partially measure other qubits) the partial measurement with the computational basis.

Before describing what partial trace is, here we explain *mixed state* and *density operator*. Suppose there are two persons Alice and Bob, and Alice has a 2-qubit state $|\psi\rangle = \frac{1}{\sqrt{2}}|0\rangle|+\rangle + \frac{1}{\sqrt{2}}|1\rangle|-\rangle$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. If Alice partially measures the leftmost qubit of $|\psi\rangle$, she will obtain 0 or 1 with probability 1/2 and the state changes to $|0\rangle|+\rangle$ or $|1\rangle|-\rangle$, respectively. After the measurement, if Alice does not tell the measurement result to Bob, what Bob knows on Alice's state is that it is $|0\rangle|+\rangle$ or $|1\rangle|-\rangle$ with probability 1/2. From Bob's point of view, this state cannot be described as a single vector. Such a state is called a *mixed state* and described by a *density operator*. More generally, suppose that we have a mixed state that is equal to $|\psi_i\rangle$ with probability p_i ($1 \le i \le s$, $\sum_i p_i = 1$). Then this state is described by the operator $\rho = \sum_i p_i|\psi_i\rangle\langle\psi_i|$, which is called the density operator of the mixed state. Two states with the same density operator are considered identical. In general, a density operator is an Hermitian non-negative operator on $\mathcal{H}$ such that $\mathrm{Tr}(\rho) = 1$, where Tr is the trace function (it is easy to check that $\sum_i p_i|\psi_i\rangle\langle\psi_i|$ is indeed Hermitian non-negative and its trace is 1). Mixed states are the most general quantum states, i.e., arbitrary quantum state can be regarded as a mixed state and described by a density operator. A state that can be described by a unit vector $|\phi\rangle$ is called a *pure state*. Note that a pure state $|\phi\rangle$ can also be regarded as the mixed state of the density operator $|\phi\rangle\langle\phi|$. Recall that the trace norm $\|A\|_{\mathrm{tr}}$ of an operator A is defined by $\|A\|_{\mathrm{tr}} := \mathrm{Tr}\left(\sqrt{A\cdot A^*}\right)$. In this paper the distance between two operators ρ and σ is measured by the trace distance $\mathsf{td}(\rho,\sigma) := \frac{1}{2}\|\rho-\sigma\|_{\mathrm{tr}}$ (when it can be defined).

The operations (i)-(iii) are generalized to mixed states as follows. The unitary operator U changes a mixed state ρ to $U\rho U^*$. An embedding changes ρ to $\rho \otimes |\psi\rangle\langle\psi|$ for some $|\psi\rangle$. When we measure a state ρ with the operators $S = \{P_i\}_{1\leq j\leq t}$, we obtain the information that we measured i with probability $\mathrm{Tr}(P_i\rho)$ and the state changes to $P_i\rho/\mathrm{Tr}(P_i\rho)$.

Next, we explain the partial trace operation.

(iv) Let σ be the density operator of a state on the joint system $\mathcal{H}\otimes\mathcal{H}'$. Then there exist $A_1,\ldots,A_s,B_1,\ldots,B_s$, where A_i and B_i are operators on $\mathcal{H}$ and $\mathcal{H}'$, respectively, such that $\sigma = \sum_{1\leq i\leq s} A_i\otimes B_i$. The partial trace of σ on $\mathcal{H}'$ is defined by $\mathrm{tr}_{\mathcal{H}'}(\sigma) := \sum_{1\leq i\leq s}\mathrm{Tr}(B_i)A_i$. ($\mathrm{tr}_{\mathcal{H}'}(\sigma)$ becomes a density operator on $\mathcal{H}$ and this definition does not depend on how we choose $A_1,\ldots,A_s,B_1,\ldots,B_s$.) Intuitively, this operation corresponds to discarding qubits that correspond to $\mathcal{H}'$.

Note that the partial trace of a pure state $|\psi\rangle$ (more precisely, the state $|\psi\rangle\langle\psi|$) is not necessarily a pure state. Conversely, for arbitrary mixed state ρ on $\mathcal{H}$, there exists a quantum system associated with a Hilbert space $\mathcal{H}'$ and a pure state $|\psi\rangle$ in $\mathcal{H}\otimes\mathcal{H}'$ such that $\mathrm{tr}_{\mathcal{H}'}(|\psi\rangle\langle\psi|) = \rho$ holds. Such $|\psi\rangle$ is called a *purification* of ρ.

Throughout the paper, we use the following notations. H denotes the Hadamard transform on 1-qubit states defined by $H|b\rangle = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b|1\rangle)$ for $b\in\{0,1\}$. Note that $H^{\otimes n}|x\rangle = \sum_{y\in\{0,1\}^n}(-1)^{x\cdot y}|y\rangle$ holds for each $x\in\{0,1\}^n$, where $x\cdot y$ denotes the dot product defined by $(x_1\wedge y_1)\oplus\cdots\oplus(x_n\wedge y_n)\in\{0,1\}$ (x_i and y_i are the i-th bits of x and y, respectively). We denote the identity operator for an n-qubit quantum system by I_n or just I. In addition, we denote the vectors $|\phi\rangle\otimes|0^s\rangle$ and $|0^s\rangle\otimes|\phi\rangle$ by the same symbol $|\phi\rangle$, if there will be no confusion. For a unitary operator U, we denote the operators $U\otimes I$ and $I\otimes U$ by the same symbol U.

2.4 (Oracle-Aided) Quantum Algorithms

This section describes how to model quantum oracles and (oracle-aided) quantum algorithms. First, in Section 2.4.1 we consider the case where an adversary has an access to a single quantum oracle and we take only the number of quantum queries into account as adversaries' computational resources, i.e., we consider quantum information-theoretic adversaries. Section 2.4.2 explains how an information theoretic adversary is modeled when it has accesses to multiple quantum oracles. Section 2.4.3 treats the case when we take other computational resources such as time and the number of available qubits.

In what follows, we assume that adversaries and the oracles are modeled as in this section when refer to the "quantum setting", unless otherwise noted. Besides, by "quantum security" we denote various security notions proven in the quantum setting (see Section 2.6 for concrete definitions of security notions in the quantum setting). Similarly, the "classical setting" denotes the setting where all the algorithms including adversaries and oracles are classical ones, and "classical security" denotes security notions proven in the classical setting.

2.4.1 Information-Theoretic Model with a Single Quantum Oracle

When a single quantum oracle is available and we ignore computational resources except for the number of queries, following previous works [BDF+11, SY17, Zha12a] we model an oracle-aided quantum algorithm $\mathcal{A}$ that makes at most q quantum queries as a sequence of unitary operators $(U_0,\ldots,U_q)$ that act on an s-qubit state space (which is the state space of $\mathcal{A}$), where U_0 corresponds to an initialization process and U_i corresponds to $\mathcal{A}$'s offline computation after the i-th query, for $i\geq 1$. Without loss of generality we can assume that $\mathcal{A}$ does not make any intermediate measurements, and $\mathcal{A}$'s state space $\mathcal{H}_{\mathcal{A}}$ (a Hilbert space) is a joint system of an a_{query}-qubit quantum system $\mathcal{H}_{\mathrm{query}}$, an a_{answer}-qubit quantum system $\mathcal{H}_{\mathrm{answer}}$, and an $(s-a_{\mathrm{query}}-a_{\mathrm{answer}})$-qubit quantum system $\mathcal{H}_{\mathrm{work}}$. Here, $\mathcal{H}_{\mathrm{query}}$, $\mathcal{H}_{\mathrm{answer}}$, and $\mathcal{H}_{\mathrm{work}}$ correspond to the register to send queries to oracles, the register to receive answers from oracles, and the register for $\mathcal{A}$'s offline works, respectively. We also model a quantum oracle O as a unitary operator O (to process queries) with its own quantum state space. O may have some (classical) randomness, and the unitary operator O may be chosen randomly according to a distribution at the beginning of each game. If O has s'-qubit quantum states, joint quantum states of $\mathcal{A}$ and O are $(s+s')$-qubit quantum states. We denote O's state space by $\mathcal{H}_O$. When $\mathcal{A}$ makes the i-th query, the unitary operator O_i acts on $\mathcal{H}_{\mathrm{query}}\otimes\mathcal{H}_{\mathrm{answer}}\otimes\mathcal{H}_O$. Let $|\mathsf{init}_{\mathcal{A}}\rangle$ and $|\mathsf{init}_O\rangle$ be the initial states of $\mathcal{A}$ and O, respectively. We assume that $|\mathsf{init}_{\mathcal{A}}\rangle$ is set to be $|x\rangle$ when $\mathcal{A}$ takes a classical bit string x as an input (when $\mathcal{A}$ does not take any initial input, by convention we assume that the initial state of $\mathcal{A}$ is $|0^\alpha\rangle$ for some α). When we run $\mathcal{A}$, the unitary operators $U_0,O,U_1,O,\ldots,U_q$ act on the initial state $|\mathsf{init}_{\mathcal{A}}\rangle\otimes|\mathsf{init}_O\rangle$ in a sequential order (the resulting quantum state is $|\Phi\rangle = U_qO\cdots OU_0(|\mathsf{init}_{\mathcal{A}}\rangle\otimes|\mathsf{init}_O\rangle)$), $\mathcal{A}$ measures the first s-qubit of the state $|\Phi\rangle$ with the computational basis to obtain a classical s-bit string z, and finally outputs (a part of) z. We denote the event that $\mathcal{A}$ outputs a bit string x after it runs relative to O by $x\leftarrow\mathcal{A}^O$.

Examples. The quantum oracle O_f of a (fixed) function $f : \{0,1\}^m \to \{0,1\}^n$ is modeled as the unitary operator

$$O_f : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle . \tag{2.2}$$

O_f does not have its own state. When a quantum algorithm $\mathcal{A}$ runs relative to O_f, $\mathcal{H}_{\text{query}}$ and $\mathcal{H}_{\text{answer}}$ are defined as m-qubit space and n-qubit space, respectively.

Let F be a family of functions from $\{0,1\}^m$ to $\{0,1\}^n$. Suppose that a quantum algorithm $\mathcal{A}$ runs relative to the quantum oracle O_F that first chooses f randomly from F (according to a distribution on F) and gives $\mathcal{A}$ a quantum oracle access to f. In this case we assume that f is chosen randomly from F and $\mathcal{A}$ runs relative to the quantum oracle of f. When f is chosen just uniformly at random from the set of all the functions from $\{0,1\}^m$ to $\{0,1\}^n$, then this is the quantum oracle of a random function.

Remark 6. *Even if a function f admits input messages M and M' of which lengths differ, we assume that the quantum oracle of O_f admits queries of superpositions of M and M'. In such a case, we assume that length $|M|$ of each message M is encoded with M. However, for ease of notation, we just write $|M\rangle$ instead of $|(|M|, M)\rangle$ for each message M.*

2.4.2 Information-Theoretic Model with Multiple Quantum Oracles

Suppose that an adversary $\mathcal{A}$ is given oracle accesses to multiple quantum oracles $O_1, \ldots, O_s$, and $\mathcal{A}$ makes q queries to each oracle $O_1, \ldots, O_s$ in a sequential order. That is, for each $1 \leq j \leq s$, after $\mathcal{A}$ makes the i-th query to O_j, $\mathcal{A}$ performs some offline computations, and them makes the i-th query to O_{j+1}. Similarly, after $\mathcal{A}$ makes the i-th query to O_s, $\mathcal{A}$ performs some offline computations, and then makes the $(i+1)$-th query to O_1. Here we explain how to model the behavior of $\mathcal{A}$ and multiple quantum oracles $O_1, \ldots, O_s$ as sequential applications of unitary operators, in the case that $\mathcal{A}$ makes queries in a sequential order as above.

The adversary $\mathcal{A}$ is modeled as the sequence of unitary operators $(U_0, U_{1,1}, \ldots, U_{s,1}, U_{1,2}, \ldots, U_{s,q})$, where $U_{i,j}$ corresponds to the offline computation by $\mathcal{A}$ after the j-th query to O_i. The state space of $\mathcal{A}$ is modeled in the same way as before. The oracles are assumed to share a state space $\mathcal{H}_O$. For each quantum oracle O_i, let O_i denote the unitary operator to process queries. Let $|\mathsf{init}_{\mathcal{A}}\rangle$ and $|\mathsf{init}_O\rangle$ be the initial states of $\mathcal{A}$ and the oracles, respectively. Then the quantum state of $\mathcal{A}$ and the oracles before the final measurement becomes $\left(\prod_{j=1}^{q} U_{s,j} O_s \cdots U_{1,j} O_1\right) U_0 |\mathsf{init}_{\mathcal{A}}\rangle \otimes |\mathsf{init}\rangle$. By $z \leftarrow \mathcal{A}^{O_1,\ldots,O_s}(x)$, we denote the event that $\mathcal{A}$ finally outputs the classical string z when $\mathcal{A}$ takes x as an input and runs relative to the oracles $O_1, \ldots, O_s$.

2.4.2.1 The Model of Adversaries of Which Queries are not in a Sequential Order

In the above model we considered the special case that the adversary queries to oracles $O_1, \ldots, O_s$ in a sequential order. However, even if an adversary $\mathcal{B}$ (given oracle accesses to $O_1, \ldots, O_s$) does not make queries in such a sequential order, the behavior of $\mathcal{B}$ can be captured with the above model: Suppose that $\mathcal{B}$ makes at most q_i quantum queries to O_i for each i, and s is a constant. Then, we can make another adversary $\mathcal{A}$ such that $\mathcal{A}$'s output distributions are the same as that of $\mathcal{B}$, and $\mathcal{A}$ makes $O(\max\{q_1, \ldots, q_s\})$ queries to each oracle in a sequential order as in the above model, by appropriately increasing the number of queries. Thus all reasonable adversaries are captured by the above model.

2.4.3 Non-Information-Theoretic Model

When we take other computational resources such as time and the number of available qubits into account in addition to the number of quantum queries, we model a quantum algorithm as a combination of classical algorithms and quantum circuits. In this paper we consider the pure quantum circuit model and ignore the costs related to communication complexity and error corrections. We regard that a quantum circuit of depth D runs in time D. We assume that each quantum circuit is composed of (1) the Hadamard gate H, (2) the $\pi/8$-gate T, (3) the phase gate S, (4) the CNOT gate, and (5) the oracle gate (if an oracle is available). We assume that each of basic gates runs in time $O(1)$, in addition that CNOT can act on arbitrary pair of qubits.

Remark 7. *In practice, computational complexity of quantum algorithms would significantly vary depending on error correction costs and quantum hardware architectures, or communication costs. Our model might overestimate quantum algorithms' abilities, but schemes that are proven to be secure in this model will remain secure in other more realistic models.*

2.5 Ideal Primitive Models

The random oracle model is the model where there exists the oracle of a random function RO (either of fixed input-length and variable input-lengths), and adversaries have access to $\mathsf{RO}(\cdot)$. The ideal permutation model is the model where there exists the oracle of a random permutation P and its inverse P^{-1}, and adversaries have access to $P(\cdot)$ and $P^{-1}(\cdot)$ (we sometimes refer to P as an ideal permutation). The ideal cipher model is the model where there exists the oracle of an ideal cipher E (an ideal cipher is a block cipher such that, for each key K, $E(K,\cdot)$ is chosen independently at random) and its inverse E^{-1}, and adversaries have access to $E(\cdot,\cdot)$ and $E^{-1}(\cdot,\cdot)$.

In addition, a quantum random oracle (QRO) is defined to be the quantum oracle such that, $f : \{0,1\}^m \to \{0,1\}^n$ is chosen uniformly at random at the beginning of each game (for some m and n), and quantum oracle access to O_f is given to adversaries. The quantum random oracle model (QROM) is the model where a QRO is available to an adversary.

In what follows, we refer to (i) a (quantum) random oracle (either of fixed input length and variable input lengths), (ii) an ideal permutation, and (iii) an ideal cipher as *ideal primitives*.

2.6 Security Definitions

This section provides security definitions. Definitions for the setting where a quantum adversary has an access to a single quantum oracle is given in Section 2.6.1. Those for multiple quantum oracles (including security definitions in the QROM) are given in Section 2.6.2. Section 2.6.3 gives definitions of indifferentiability in the classical setting.

2.6.1 Quantum Security in Single-Oracle Settings

2.6.1.1 Quantum Distinguishing Advantage

Let $\mathcal{A}$ be a quantum algorithm that makes at most q queries and outputs 0 or 1 as the final output, and let O_1 and O_2 be some oracles. We consider the situation where O_1 and O_2 are chosen randomly in accordance with some distributions. We define the *quantum distinguishing advantage* of $\mathcal{A}$ by

$$\mathbf{Adv}^{\mathrm{dist}}_{O_1,O_2}(\mathcal{A}) := \left| \Pr_{O_1}\left[\mathcal{A}^{O_1}() \to 1\right] - \Pr_{O_2}\left[\mathcal{A}^{O_2}() \to 1\right] \right|. \tag{2.3}$$

When we are interested only in the number of queries and do not consider other complexities such as the number of gates (i.e., we focus on information theoretic adversaries), we use the notation

$$\mathbf{Adv}^{\mathrm{dist}}_{O_1,O_2}(q) := \max_{\mathcal{A}} \left\{ \mathbf{Adv}^{\mathrm{dist}}_{O_1,O_2}(\mathcal{A}) \right\}, \tag{2.4}$$

where the maximum is taken over all quantum algorithms that make at most q quantum queries.

2.6.1.2 Quantum PRF Advantage

Let RF denote the quantum oracle of a random function, i.e., the oracle such that a function $f \in \mathsf{Func}(\{0,1\}^m, \{0,1\}^n)$ is chosen uniformly at random, and adversaries are given oracle access to O_f.

Let $\mathcal{F} = \{F_k : \{0,1\}^m \to \{0,1\}^n\}_{k\in\mathcal{K}}$ be a family of functions (i.e., a keyed function). Let us use the same symbol $\mathcal{F}$ to denote the oracle such that k is chosen uniformly at random, and adversaries are given oracle access to O_{F_k}. In addition, let $\mathcal{A}$ be an oracle query algorithm that outputs 0 or 1. Then we define the quantum pseudorandom function advantage (qPRF advantage) by

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(\mathcal{A}) := \mathbf{Adv}^{\mathrm{dist}}_{\mathcal{F},\mathsf{RF}}(\mathcal{A}).$$

Similarly, we define $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(q)$ by $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(q) := \max_{\mathcal{A}} \left\{ \mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(\mathcal{A}) \right\}$, where the maximum is taken over all quantum algorithms $\mathcal{A}$ that make at most q quantum queries.

2.6.1.3 Quantum PRP Advantage

Let RP denote the quantum oracle of a random permutation, i.e., the oracle such that a permutation $P \in \mathsf{Perm}(\{0,1\}^n)$ is chosen uniformly at random, and adversaries are given oracle access to O_P.

Let $\mathcal{P} = \{P_k : \{0,1\}^n \to \{0,1\}^n\}_{k\in\mathcal{K}}$ be a family of permutations. We use the same symbol $\mathcal{P}$ to denote the oracle such that k is chosen uniformly at random, and adversaries are given oracle access to O_{P_k}. Let $\mathcal{A}$ be an oracle query algorithm that outputs 0 or 1, and we define the quantum pseudorandom permutation advantage (qPRP advantage) by

$$\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(\mathcal{A}) := \mathbf{Adv}^{\mathrm{dist}}_{\mathcal{P},\mathsf{RP}}(\mathcal{A}).$$

Similarly, we define $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(q)$ by $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(q) := \max_{\mathcal{A}}\left\{\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(\mathcal{A})\right\}$, where the maximum is taken over all quantum algorithms $\mathcal{A}$ that make at most q quantum queries.

2.6.1.4 Quantum $\widetilde{\mathrm{PRP}}$ Advantage

Let $\widetilde{\mathsf{RP}}$ be the quantum oracle of a function $\tilde{P} : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ such that $\tilde{P}(T,\cdot)$ is chosen from $\mathsf{Perm}(\{0,1\}^n)$ uniformly at random for each $T \in \{0,1\}^t$ (i.e., $\tilde{P}$ is a tweakable random permutation).

Let $\tilde{E} : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ be a tweakable block cipher, and $\mathcal{A}$ be an oracle-aided quantum algorithm. By abuse of notation, let $\tilde{E}$ also denote the quantum oracle that chooses a key $K \in \{0,1\}^k$ uniformly at random and gives a quantum oracle access to $\tilde{E}(K,\cdot,\cdot)$. Extending the classical security notion [LRW02, LRW11], we define the quantum tweakable pseudorandom permutation advantage (or $\widetilde{\mathrm{qPRP}}$ advantage for short) by

$$\mathbf{Adv}^{\widetilde{\mathrm{qPRP}}}_{\tilde{E}}(\mathcal{A}) := \mathbf{Adv}^{\mathrm{dist}}_{\tilde{E},\widetilde{\mathsf{RP}}}(\mathcal{A}).$$

Similarly, we define $\mathbf{Adv}^{\widetilde{\mathrm{qPRP}}}_{\mathcal{P}}(q)$ by $\mathbf{Adv}^{\widetilde{\mathrm{qPRP}}}_{\tilde{E}}(q) := \max_{\mathcal{A}}\left\{\mathbf{Adv}^{\widetilde{\mathrm{qPRP}}}_{\tilde{E}}(\mathcal{A})\right\}$, where the maximum is taken over all quantum algorithms $\mathcal{A}$ that make at most q quantum queries.

2.6.1.5 Security against Efficient Adversaries

An algorithm $\mathcal{A}$ is called *efficient* if it can be realized as a quantum circuit that has a polynomial number of quantum gates in n. A keyed function $\mathcal{F}$ (resp., a block cipher $\mathcal{P}$, and a tweakable block cipher $\tilde{E}$) is a *quantum-secure PRF* or *qPRF* (resp., a *quantum-secure PRP* or *qPRP*, and a *quantum-secure* $\widetilde{\mathrm{PRP}}$ or $\widetilde{\mathrm{qPRP}}$) if the following properties are satisfied:

1. Evaluation of $\mathcal{F}$ (resp., $\mathcal{P}$, and $\tilde{E}$) can be implemented on a quantum circuit that have a polynomial number of quantum gates in n.
2. $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathcal{F}}(\mathcal{A})$ (resp., $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathcal{P}}(\mathcal{A})$, and $\mathbf{Adv}^{\widetilde{\mathrm{qPRP}}}_{\tilde{E}}(\mathcal{A})$) is negligible for any efficient algorithm $\mathcal{A}$.

2.6.2 Quantum Security in Multiple-Oracle Settings

2.6.2.1 Quantum Distinguishing Advantage

For quantum oracles $O_1,\ldots,O_s$ and $O'_1,\ldots,O'_s$, we define the quantum distinguishing advantage of an adversary $\mathcal{A}$ by

$$\mathbf{Adv}^{\mathrm{dist}}_{(O_1,\ldots,O_s),(O'_1,\ldots,O'_s)}(\mathcal{A}) := \left|\Pr\left[1 \leftarrow \mathcal{A}^{O_1,\ldots,O_s}()\right] - \Pr\left[1 \leftarrow \mathcal{A}^{O'_1,\ldots,O'_s}()\right]\right|.$$

In addition, we define $\mathbf{Adv}^{\mathrm{dist}}_{O_1^h,O_2^h}(q) := \max\left\{\mathbf{Adv}^{\mathrm{dist}}_{(O_1,\ldots,O_s),(O'_1,\ldots,O'_s)}(\mathcal{A})\right\}$, where the maximum is taken over all the adversaries that make at most q queries to each oracle.

2.6.2.2 Quantum PRF Advantage in the QROM

Let h be a QRO and F^h_K be a keyed function that may depend on h. By the same symbol F^h_K we denote the quantum oracle such that the key K is chosen at random, and the quantum oracle access to F^h_K is given to adversaries. In addition, let RF be the quantum oracle of a random function that is independent of h. Then, we define the quantum-secure pseudorandom function advantage (qPRF advantage) of $\mathcal{A}$ on F^h_K by

$$\mathbf{Adv}^{\mathrm{qPRF}}_{F^h_K}(\mathcal{A}) := \mathbf{Adv}^{\mathrm{dist}}_{(F^h_K,h),(\mathsf{RF},h)}(\mathcal{A}).$$

In addition, we define $\mathbf{Adv}^{\mathrm{qPRF}}_{F^h_K}(q) := \max\left\{\mathbf{Adv}^{\mathrm{qPRF}}_{F^h_K}(\mathcal{A})\right\}$, where the maximum is taken over all the adversaries that make at most q quantum queries to each oracle.

2.6.2.3 Quantum PRG Advantage in the QROM

Let h be a QRO and $\rho^h : \{0,1\}^{k_1} \to \{0,1\}^{k_2}$ be a function that may depend on h. Then, we define the quantum PRG advantage $\mathbf{Adv}^{\mathrm{qPRG}}_{\rho^h}(\mathcal{A})$ of $\mathcal{A}$ on ρ^h by

$$\mathbf{Adv}^{\mathrm{qPRG}}_{\rho^h}(\mathcal{A}) := \left|\Pr\left[K_1 \xleftarrow{\$} \{0,1\}^{k_1} : 1 \leftarrow \mathcal{A}^h(\rho^h(K_1))\right] - \Pr\left[K_2 \xleftarrow{\$} \{0,1\}^{k_2} : 1 \leftarrow \mathcal{A}^h(K_2)\right]\right|.$$

2.6.3 Classical Indifferentiability

In this section, all the algorithms and oracles are classical ones. Let $\mathcal{R}$ be a classical ideal primitive. Let H be a function that accesses to the oracle of another ideal primitive O, and suppose that the input and output lengths of H are the same as those of $\mathcal{R}$. Let $\mathcal{S}$ be an algorithm that has the same interface of input and output as O and has an oracle access to $\mathcal{R}$. Let $\mathsf{Real}^{H,O,\mathcal{A}}$ be the game that runs $\mathcal{A}$ relative to (H^O, O), and finally returns what $\mathcal{A}^{H^O,O}$ outputs. In addition, let $\mathsf{Ideal}^{\mathcal{R},\mathcal{A}}_{\mathcal{S}}$ be the game that runs $\mathcal{A}$ relative to $(\mathcal{R}, \mathcal{S}^{\mathcal{R}})$, and finally returns what $\mathcal{A}^{\mathcal{R},\mathcal{S}^{\mathcal{R}}}$ outputs. We define the indifferentiability advantage of an adversary $\mathcal{A}$ against (H^O, O) and $\mathcal{R}$ with respect to the simulator $\mathcal{S}$ by

$$\mathbf{Adv}^{\mathrm{indiff}}_{(H^O,O),\mathcal{R},\mathcal{S}}(\mathcal{A}) := \left|\Pr\left[1 \leftarrow \mathsf{Real}^{H,O,\mathcal{A}}\right] - \Pr\left[1 \leftarrow \mathsf{Ideal}^{\mathcal{R},\mathcal{A}}_{\mathcal{S}}\right]\right|.$$

See also Fig. 2.1.

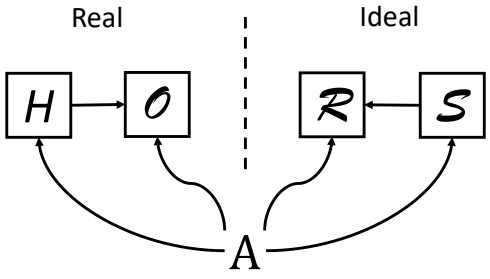


Figure 2.1: Indifferentiability games.

Definition 1 (Indifferentiability [MRH04])**.** *The function H^O is said to be $(t_{\mathcal{S}}, t_{\mathcal{A}}, q_{\mathcal{A}}, Q_{\mathcal{A}}, \epsilon)$-indifferentiable from $\mathcal{R}$ if there exists a simulator $\mathcal{S}$ such that (1) $\mathcal{S}$ runs in time at most $t_{\mathcal{S}}$, and (2) for any adversary $\mathcal{A}$ that runs in time $t_{\mathcal{A}}$, makes at most $q_{\mathcal{A}}$ queries to O (resp., $\mathcal{S}^{\mathcal{R}}$), and $Q_{\mathcal{A}}$ queries to H^O (resp., $\mathcal{R}$),*

$$\mathbf{Adv}^{\mathrm{indiff}}_{(H^O,O),\mathcal{R},\mathcal{S}}(\mathcal{A}) \leq \epsilon$$

holds.

We ambiguously say that H^O is indifferentiable from $\mathcal{R}$ up to x queries if there exists a simulator $\mathcal{S}$ such that, for arbitrary adversary $\mathcal{A}$ such that $q_{\mathcal{A}}, Q_{\mathcal{A}} \ll x$, $\mathbf{Adv}^{\mathrm{indiff}}_{(H^O,O),\mathcal{R},\mathcal{S}}(\mathcal{A})$ is negligible.

The composition theorem [RSS11] assures that, if (i) the security of a primitive Q is defined with a single-stage game, and (ii) H^O is indifferentiable from a random oracle, then it suffice to prove the security of $Q^{\mathcal{R}}$ in the setting that adversaries can access to $\mathcal{R}$ to prove the security of Q^{H^O} in the setting that adversaries can access to (H^O, O).

2.6.4 Useful Proof Tools in the Quantum Setting

This section reviews some useful proof tools in the quantum setting for later use. Note that, in this section we take the running time and the number of available qubits into account, in addition to the number of quantum queries, when we estimate adversaries' computational resources (see Section 2.4.3 for details).

Switching Random Functions and Random Permutations. The following theorem is a quantum version of the RF-RP switching lemma, which was shown by Zhandry [Zha15].

Theorem 5 (Theorem 7 in [Zha15])**.** *Let* RF *and* RP *denote quantum oracles of a random function from* $\{0,1\}^n$ *to* $\{0,1\}^n$ *and an n-bit random permutation, respectively. Let* $\mathcal{A}$ *be an oracle-aided quantum algorithm that makes at most q quantum queries. Then* $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{RF},\mathsf{RP}}(\mathcal{A}) \leq O(q^3/2^n)$ *holds.*

Simulating Random Functions in the Quantum Setting. For a positive integer k, *k-wise independent hash function family* is a family of functions $H = \{h_i : \mathcal{X} \to \mathcal{Y}\}_{i \in I}$ (I is a finite index set) such that $\Pr_{i \leftarrow\$ I}\left[h_i(x_1) = y_1 \wedge \cdots \wedge h_i(x_k) = y_k\right] = 1/|\mathcal{Y}|^k$ holds for arbitrary tuple $(x_1, \ldots, x_k, y_1, \ldots, y_k) \in \mathcal{X}^k \times \mathcal{Y}^k$ such that $x_\alpha \neq x_\beta$ for $\alpha \neq \beta$.

Zhandry showed that a random function can be perfectly simulated with $2q$-wise independent hash function families against quantum algorithms that make at most q queries [Zha12b].

Theorem 6 (Theorem 3.1 in [Zha12b])**.** *Let* $\mathcal{A}$ *be an oracle-aided quantum algorithm that makes at most q quantum queries. Let* $H = \{h_i : \{0,1\}^m \to \{0,1\}^n\}_{i \in I}$ *be a* $2q$*-wise independent hash function family. By abuse of notation, let H also denote the quantum oracle such that* $i \in I$ *is chosen uniformly at random and the quantum oracle access to the function* h_i *is given to* $\mathcal{A}$*. Then* $\mathbf{Adv}^{\mathrm{qPRF}}_{H}(\mathcal{A}) = 0$ *holds.*

The set of polynomials over $\mathrm{GF}(2^n)$ of which degree is at most $2q - 1$ ($\leq 2^n$) becomes a $2q$-wise independent hash function family (domains and ranges are $\mathrm{GF}(2^n) = \{0,1\}^n$). Let $H = \{h_i : \{0,1\}^n \to \{0,1\}^n\}_{i \in I}$ denote this hash function family. Then H can be regarded as a function from $I \times \{0,1\}^n$ to $\{0,1\}^n$. We can built a quantum circuit with depth $\tilde{O}(q)$ and width $\tilde{O}(q)$ ($\tilde{O}$ suppresses factors of polynomials in n) that computes the function $H : (i, x) \mapsto h_i(x)$. Therefore, the following corollary follows from Theorem 6.

Corollary 1. *There exists a function family* $H = \{h_i : \{0,1\}^n \to \{0,1\}^n\}_{i \in I}$ *such that (1) sampling i from I uniformly at random can be done in time* $\tilde{O}(q)$*, (2)* $H : (i, x) \mapsto h_i(x)$ *is implemented on a quantum circuit with depth* $\tilde{O}(q)$ *and width* $\tilde{O}(q)$*, and (3)* $\mathbf{Adv}^{\mathrm{qPRF}}_{h_i}(\mathcal{A}) = 0$ *holds for any quantum algorithm* $\mathcal{A}$ *that makes at most q quantum queries when i is chosen uniformly at random.*

Chapter 3

Compressed Oracle Technique

This chapter provides an alternative formalization for the compressed oracle technique and its properties. All the security proofs in the quantum setting of later chapters rely on the techniques explained in this chapter.

See also Section 1.5 for an overview. Section 3.1 briefly explains the reason that copying and recording queries is important in classical security proofs, and why it becomes hard when adversaries make quantum queries. Section 3.2 gives an overview of the original technique by Zhandry. Then, in Section 3.3 we describe our alternative formalization.

3.1 The Recording Barrier in the Quantum Setting

Lots of classical security proofs rely on the fact that the queries to oracles and the answers can be copied and recorded. For instance, suppose we want to show the hardness of finding a collision of a random function $f : \{0,1\}^n \to \{0,1\}^n$ in the classical setting[1]. Let $\mathcal{A}$ be a (classical) adversary that tries to find a collision of f by making exactly q queries. f is chosen randomly before $\mathcal{A}$ runs. Since we are in the classical setting, we can modify the oracle of f so that it will copy and record $\mathcal{A}$'s queries and the answers (this modification does not change the difficulty of finding a collision and $\mathcal{A}$ cannot notice). Then the record can be represented as a sequence of pairs $((X_1, Y_1), \ldots, (X_q, Y_q))$, where X_i is $\mathcal{A}$'s i-th query and Y_i is the response (i.e., $Y_i = f(X_i)$). $\mathcal{A}$ finds a collision if and only if $Y_i = Y_j$ for some i and j such that $X_i \neq X_j$[2]. Thus we have

$$\begin{aligned}
\Pr[\mathcal{A} \text{ finds a collision}] &= \Pr\left[Y_i = Y_j \text{ for some } i \neq j \text{ such that } X_i \neq X_j\right] \\
&\leq \sum_{1 \leq i < j \leq q, Y \in \{0,1\}^n} \Pr\left[Y_i = Y \text{ and } Y_j = Y \text{ and } X_i \neq X_j\right] \\
&= \sum_{1 \leq i < j \leq q, Y \in \{0,1\}^n} \Pr[Y_j = Y \text{ and } X_i \neq X_j | Y_i = Y] \cdot \Pr[Y_i = Y]
\end{aligned}$$

Since f is a random function, $\Pr[Y_i = Y] = 1/2^n$ and $\Pr[Y_j = Y \text{ and } X_i \neq X_j | Y_i = Y] \leq 1/2^n$ hold for all $i < j$ and all $Y \in \{0,1\}^n$. Hence

$$\Pr[\mathcal{A} \text{ finds a collision}] \leq \sum_{1 \leq i < j \leq q, Y \in \{0,1\}^n} \frac{1}{2^{2n}} \leq \frac{q^2}{2^n}$$

holds, which implies that the probability that $\mathcal{A}$ finds a collision is extremely small when $q \ll 2^{n/2}$.

The above classical proof fully relies on the fact that we can record the sequence of queries and answers $((X_1, Y_1), \ldots, (X_q, Y_q))$ without being noticed by $\mathcal{A}$. However, in the quantum setting, we cannot copy and record X_i and Y_i in general because this may perturb the adversary's quantum states significantly, which may be detected by the adversary. Below we explain why this is the case.

Recall that the quantum oracle of f is represented as the unitary operator $O_f : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus f(x)\rangle$. Let $\mathcal{B}$ be the quantum adversary that tries to find a collision of the random function f by making $O(2^{n/3})$ *quantum* queries to f as follows.

[1] Recall that a collision of f is a pair of distinct inputs (X, X') such that $f(X) = f(X')$.

[2] To be precise there is a possibility that $\mathcal{A}$ finds and outputs a collision by chance even if $Y_i \neq Y_j$ holds for all i and j such that $X_i \neq X_j$. However, here we assume that $\mathcal{A}$ gives up and abort (which means that $\mathcal{A}$ failed to find a collision) in such a situation, for simplicity.

1. $\mathcal{B}$ queries the state $\sum_{X\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |X\rangle |0^n\rangle$ to the quantum oracle *twice in a row*. Now $\mathcal{B}$ has a $2n$-qubit state $|\phi\rangle$. Then, $\mathcal{B}$ applies the Hadamard operator $H^{\otimes n}$ on the leftmost n-qubit of $|\phi\rangle$.

2. $\mathcal{B}$ measures the leftmost n-qubit and checks whether it is $|0^n\rangle$. If it is $|0^n\rangle$, proceed to the next step. If not, $\mathcal{B}$ aborts (in this case $\mathcal{B}$ fails to find a collision).

3. $\mathcal{B}$ runs the quantum collision-finding algorithm by Brassard et al. [BHT98, BHT97], which finds a collision of a random function with high probability by making $O(2^{n/3})$ quantum queries ($\mathcal{B}$ succeeds to find a collision).

Suppose that the oracle given to $\mathcal{B}$ is indeed the original O_f without any modification. Then, the transition of the quantum state of $\mathcal{B}$ in the first step is as follows.

$$\sum_{X\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |X\rangle |0^n\rangle \xrightarrow{O_f} \sum_{X\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |X\rangle |f(X)\rangle \xrightarrow{O_f} \sum_{X\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |X\rangle |0^n\rangle \xrightarrow{H^{\otimes n}\otimes I_n} |0^n\rangle |0^n\rangle (= |\phi\rangle)$$

Hence the leftmost n-qubit of $|\phi\rangle$ is always $|0^n\rangle$ in the second step, and $\mathcal{B}$ successfully finds a collision in the third step.

Next, suppose O_f is modified in such a way that it copies and records queries and answers. Formally, the modified oracle is represented by the operator

$$O'_f : |X\rangle |Y\rangle \mapsto |X\rangle |Y \oplus f(X)\rangle \otimes |X\rangle |f(X)\rangle .$$

(The number of qubits stored in the oracle increases by $2n$ per each query. Note that this operator can be realized by a combination of the embedding $|X\rangle |0^n\rangle \mapsto |X\rangle |0^n\rangle \otimes |0^n\rangle |0^n\rangle$, a query to O_f, and some other unitary operations.) If the oracle given to $\mathcal{B}$ is O'_f, the transition of the entire quantum state in the first step becomes as follows.

$$\begin{aligned}
\sum_{X\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |X\rangle |0^n\rangle &\xrightarrow{O'_f} \sum_{X\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |X\rangle |f(X)\rangle \otimes |X\rangle |f(X)\rangle \\
&\xrightarrow{O'_f} \sum_{X\in\{0,1\}^n} \frac{1}{\sqrt{2^n}} |X\rangle |0^n\rangle \otimes |X\rangle |f(X)\rangle |X\rangle |f(X)\rangle \\
&\xrightarrow{H^{\otimes n}\otimes I_n\otimes I_{4n}} \sum_{X,Y\in\{0,1\}^n} \frac{1}{2^n} |Y\rangle |0^n\rangle \otimes |X\rangle |f(X)\rangle |X\rangle |f(X)\rangle (= |\phi\rangle)
\end{aligned}$$

When $\mathcal{B}$ measures the leftmost n-qubits of $|\phi\rangle$ in the second step, the probability that $\mathcal{B}$ obtains $|0^n\rangle$ is $1/2^n$. Thus $\mathcal{B}$ aborts and fails to find a collision with an overwhelming probability.

The above example demonstrates that the quantum state is perturbed and $\mathcal{B}$ can detect it if we copy and record queries and answers in the quantum setting. In particular, the classical security proof we mentioned before does not work in the quantum setting because there exist quantum adversaries such as $\mathcal{B}$ that can distinguish O_f and O'_f (in other words, the classical proof works because O_f and O'_f are indistinguishable for classical adversaries.). What Zhandry showed in [Zha19] is that this recording barrier in the quantum setting can be overcome to some extent, for the quantum oracle of random functions.

3.2 An Overview of the Original Technique

First, Zhandry observed that the quantum oracle of a (fixed) function $f : \{0,1\}^m \to \{0,1\}^n$, which is described as the unitary operator $O_f : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle$, can be implemented with an encoding of f and an operator stO that is independent of f. In this section, we assume that each function $f : \{0,1\}^m \to \{0,1\}^n$ is encoded into the $(n2^m)$-qubit state $|f\rangle = |f(0)\|f(1)\|\cdots\|f(2^m-1)\rangle$. The operator stO is the unitary operator that acts on $(n+m+n2^m)$-qubit states defined as

$$\mathsf{stO} : |x\rangle |y\rangle \otimes |\alpha_0\rangle \cdots |\alpha_{2^m-1}\rangle \mapsto |x\rangle |y \oplus \alpha_x\rangle \otimes |\alpha_0\rangle \cdots |\alpha_{2^m-1}\rangle, \tag{3.1}$$

where $\alpha_x \in \{0,1\}^n$ for each $0 \le x \le 2^m - 1$. [3] We can easily confirm that $\mathsf{stO} |x\rangle |y\rangle |f\rangle = |x\rangle |y \oplus f(x)\rangle |f\rangle$ holds. Here, $|x\rangle |y\rangle$ corresponds to the first $(m+n)$-qubits of adversaries' registers.

[3] "stO" is an abbreviation of "standard oracle".

When f is chosen uniformly at random and $\mathcal{A}$ runs relative to stO and $|f\rangle$ (i.e., $\mathcal{A}$ runs relative to the quantum oracle of a random function), the whole quantum state before $\mathcal{A}$ makes the $(i+1)$-st quantum query becomes

$$|\phi_{f,i+1}\rangle = (U_i \otimes I)\mathsf{stO}(U_{i-1} \otimes I)\mathsf{stO} \cdots \mathsf{stO}(U_0 \otimes I)\,|0^\ell\rangle\,|f\rangle \tag{3.2}$$

with probability $1/2^{n2^m}$. Here, we assume that $\mathcal{A}$ has ℓ-qubit quantum states.

The random choice of f can be implemented by first making the uniform superposition of functions $\sum_f \frac{1}{\sqrt{2^{n2^m}}}|f\rangle = H^{\otimes n2^m}|0^{n2^m}\rangle$ and then measuring the state with the computational basis. So far we have considered the case that a random function f is chosen at the beginning of games, but the output distribution of $\mathcal{A}$ will not be changed even if we measure the $|f\rangle$ register at the same time as we measure $\mathcal{A}$'s register. Thus, below we assume that all quantum registers including those of functions are measured only once at the end of each game.

Then the whole quantum state before $\mathcal{A}$ makes the $(i+1)$-st quantum query becomes

$$|\phi_{i+1}\rangle = \sum_f |\phi_{f,i+1}\rangle = (U_i \otimes I)\mathsf{stO} \cdots \mathsf{stO}(U_0 \otimes I)\left(|0^\ell\rangle \otimes \sum_f \frac{1}{\sqrt{2^{n2^m}}}|f\rangle\right). \tag{3.3}$$

Next, we change the basis of the y register and α_i registers in (3.1) from the standard computational basis $\{|u\rangle\}_{u\in\{0,1\}^n}$ to the one called the *Fourier basis* $\{H^{\otimes n}|u\rangle\}_{u\in\{0,1\}^n}$[4] by Zhandry [Zha19]. In what follows, we use the symbol "$\widehat{\ }$" to denote the encoding of classical bit strings into quantum states by using the Fourier basis instead of the computational basis, and we ambiguously denote $H^{\otimes n}|u\rangle$ by $|\widehat{u}\rangle$ for each $u \in \{0,1\}^n$. Then, it can be easily confirmed that

$$\mathsf{stO}\,|x\rangle\,|\widehat{y}\rangle \otimes |\widehat{\alpha_0}\rangle \cdots |\widehat{\alpha_{2^m-1}}\rangle = |x\rangle\,|\widehat{y}\rangle \otimes |\widehat{\alpha_0}\rangle \cdots |\widehat{\alpha_x \oplus y}\rangle \cdots |\widehat{\alpha_{2^m-1}}\rangle \tag{3.4}$$

holds. Intuitively, the direction of data writing changes after changing the basis: When we use the standard computational basis, data is written from the function registers to adversaries' registers as in (3.1). On the other hand, when we use the Fourier basis, data is written in the opposite direction as in (3.4). With the Fourier basis, $|\phi_{i+1}\rangle$ can be written as

$$|\phi_{i+1}\rangle = (U_i \otimes I)\mathsf{stO}(U_{i-1} \otimes I)\mathsf{stO} \cdots \mathsf{stO}(U_0 \otimes I)\left(|0^\ell\rangle \otimes |\widehat{0^{n2^m}}\rangle\right). \tag{3.5}$$

Here, note that $\sum_f |f\rangle = H^{\otimes n2^m}|0^{n2^m}\rangle = |\widehat{0^{n2^m}}\rangle$ holds. Thus

$$|\phi_{i+1}\rangle = \sum_{xyz\widehat{D}} a'_{xyz\widehat{D}}\,|xyz\rangle \otimes |\widehat{D}\rangle \tag{3.6}$$

holds for some complex numbers $a'_{xyz\widehat{D}}$ such that $\sum_{xyz\widehat{D}} |a'_{xyz\widehat{D}}|^2 = 1$, where each x is an m-bit string that corresponds to $\mathcal{A}$'s register to send queries to oracles, y is an n-bit string that corresponds to $\mathcal{A}$'s register to receive answers from oracles, z corresponds to $\mathcal{A}$'s remaining register to perform offline computations, and $\widehat{D} = \widehat{\alpha_0}\|\cdots\|\widehat{\alpha_{2^m-1}}$ is a concatenation of 2^m strings of n bits.

Zhandry's key observation is that, since stO adds at most one data to the $\widehat{D}$-register in each query, $\widehat{\alpha}_x \neq 0^n$ holds for at most i indices x, and thus $\widehat{D}$ can be regarded as a database with at most i non-zero entries. (Note that $\widehat{D}$ may contain fewer than i non-zero entries. For example, if a state $|x\rangle\,|\widehat{y}\rangle$ is successively queried to stO twice, then the database will remain unchanged since $\mathsf{stO}\cdot\mathsf{stO} = I$.) We use the same notation $\widehat{D}$ to denote the database and call it the *Fourier database* since now we are using the Fourier basis for $\widehat{D}$. Each entry of the database $\widehat{D}$ has the form $(x, \widehat{\alpha}_x)$, where $x \in \{0,1\}^m$, $\widehat{\alpha}_x \in \{0,1\}^n$, and $\widehat{\alpha}_x \neq 0^n$.

Intuitively, if the Fourier database $\widehat{D}$ contains an entry $(x, \widehat{\alpha}_x)$, it means that $\mathcal{A}$ has queried x to a random function f and holds some information about the value $f(x)$. Hence $\widehat{D}$ can be seen as a record of transcripts for queries and answers. However, it is still not clear what kind of information $\mathcal{A}$ has about the value $f(x)$, since we are now using the Fourier basis. To clarify this information, let the Hadamard operator $H^{\otimes n}$ act on each $\widehat{\alpha}_x$ in $\widehat{D}$ and obtain another (superposition of) database D. Then, intuitively, D satisfies the condition in which "$(x, \alpha_x) \in D$ corresponds to the condition that $\mathcal{A}$ has queried x to the oracle and received the value α_x in response." We call D a *standard database*.

In summary, Zhandry observed that the quantum random oracle can be described as a stateful quantum oracle CstO. The whole quantum state of an adversary $\mathcal{A}$ and the oracle just before the $(i+1)$-st query is

$$|\phi_{i+1}\rangle = \sum_{xyzD} a_{xyzD}\,|xyz\rangle \otimes |D\rangle, \tag{3.7}$$

[4]Note that the Hadamard operator $H^{\otimes n}$ corresponds to the Fourier transformation over the group $(\mathbb{Z}/2\mathbb{Z})^{\oplus n}$.

where each D is a standard database that contains at most i entries. Initially, the database D is empty. Intuitively, when $\mathcal{A}$ makes a query $|x, y\rangle$ to the oracle, CstO does the following three-step procedure[5].

The Three-Step Procedure of CstO.

1. Look for a tuple $(x, \alpha_x) \in D$. If one is found, respond with $|x, y \oplus \alpha_x\rangle$.
2. If no tuple is found, create new registers initialized to the state $\frac{1}{\sqrt{2^n}} \sum_{\alpha_x} |\alpha_x\rangle$. Add the registers (x, α_x) to D. Then respond with $|x, y \oplus \alpha_x\rangle$.
3. Finally, regardless of whether the tuple was found or added, there is now a tuple (x, α_x) in D, which may have to be removed. To do so, test whether the registers containing α_x contain 0^n in the Fourier basis. If so, remove the tuple from D. Otherwise, leave the tuple in D.

Intuitively, the first and second steps correspond to the classical *lazy sampling*, which do the following procedure: When an adversary makes a query x to the oracle, look for a tuple (x, α_x) in the database. If one is found, respond with α_x (this part corresponds to the first procedure of CstO). If no tuple is found, *choose α_x uniformly at random from* $\{0,1\}^n$ (this part corresponds to creating the superposition $\frac{1}{\sqrt{2^n}} \sum_{\alpha_x} |\alpha_x\rangle$ in the second step of CstO), respond with α_x, and add (x, α_x) to the database.

The third "test and forget" step is crucial and specific to the quantum setting. Intuitively, the third step forgets data that is no longer used by the adversary from the database. By appropriately forgetting information, we can record transcripts of queries and answers without perturbing quantum states.

3.2.1 Formalization with Compression

On the basis of above clever intuitions, Zhandry gave a formalized description of the compressed standard oracle CstO (although we do not give the explicit description here). Note that, since each database D has at most i entries before the $(i+1)$-st query, D can be encoded in a compressed manner by using only $O(i(m+n))$ qubits. With this observation, CstO is formalized in such a way that it has $O(i(m+n))$-qubit states before the $(i+1)$-st query for each i, which enables us to simulate a random oracle very efficiently on the fly, without an a priori bound on the number of queries (which required computational assumption before Zhandry's work).

3.3 Our Alternative Formalization

Next we give our alternative formalization. From now on, we represent each function $f : \{0,1\}^m \to \{0,1\}^n$ as an $(n+1)2^m$-bit string $(0\|f(0))\|(0\|f(1))\|\cdots\|(0\|f(2^m-1))$. Remember that the whole quantum state after $\mathcal{A}$ makes the i-th query is described as

$$|\tilde{\phi}_i\rangle = \mathsf{stO}(U_{i-1} \otimes I)\mathsf{stO} \cdots \mathsf{stO}(U_0 \otimes I)\left(|0^\ell\rangle \otimes \sum_f \frac{1}{\sqrt{2^{n2^m}}} |f\rangle\right). \tag{3.8}$$

At each query, we first "decode" superpositions of databases to superpositions of functions when an adversary makes a query, then respond to the adversary, and finally "encode" again superpositions of functions to superpositions of databases. Below we describe our encoding.

3.3.0.1 Encoding Functions to Databases: Intuitive Descriptions

Modifying the idea of Zhandry, we apply the following operations to the $|f\rangle$-register of $|\tilde{\phi}_i\rangle$ (i.e., just after the i-th query).

1. First, for each x, we change the basis of the registers for the output value $f(x)$ from the computational basis to the Fourier basis. That is, we let the Hadamard operator $H^{\otimes n}$ act on the $f(x)$ register for all x. Now the state becomes
$$\sum_{xyz\widetilde{D}} a'_{xyz\widetilde{D}} |xyz\rangle \otimes |\widetilde{D}\rangle \tag{3.9}$$

[5] Note that this three-step procedure is a quoted verbatim from a preliminary full version of the original paper [Zha18] on IACR Cryptology ePrint archive, except that the symbol y' and 0 are used instead of α_x and 0^n, respectively, in the original procedure.

for some complex numbers $a'_{xyz\widetilde{D}}$, where each $\widetilde{D} = (0\|\widehat{\alpha}_0)\|\cdots\|(0\|\widehat{\alpha}_{2^m-1})$ is a concatenation of 2^m strings of $(n+1)$ bits, and $\widehat{\alpha}_x \neq 0^n$ at most i indices x.

2. Next, we check and mark which x has been previously queried by $\mathcal{A}$. Intuitively, $\widehat{\alpha}_x \neq 0^n$ means that $\mathcal{A}$ has queried x before. Thus, for each x, we flip the bit just before $\widehat{\alpha}_x$ if $\widehat{\alpha}_x \neq 0^n$. Then each $\widetilde{D}$ changes to the bit string $(b_0\|\widehat{\alpha}_0)\|\cdots\|(b_{2^m-1}\|\widehat{\alpha}_{2^m-1})$, where $b_x \in \{0,1\}$, and $b_x = 1$ if and only if $\widehat{\alpha}_x \neq 0^n$.

3. Now the information on which x has been previously queried by $\mathcal{A}$ is recorded in $\tilde{D}$. However, it is still not clear what kind of information $\mathcal{A}$ has about the response value $f(x)$, since we are now using the Fourier basis. To clarify this information, for x that $\mathcal{A}$ has previously queried, we change the basis of the register $\widehat{\alpha}_x$ back to the computational basis. That is, for each x, we let the n-bit Hadamard transformation $H^{\otimes n}$ act on $|\widehat{\alpha}_x\rangle$ if and only if $b_x = 1$. Then the quantum state becomes

$$|\tilde{\psi}_i\rangle := \sum_{xyzD} a_{xyzD} |xyz\rangle \otimes |D\rangle \tag{3.10}$$

for some complex numbers a_{xyzD}, where each D is a concatenation of 2^m strings of $(n+1)$ bits, $(b_0\|\alpha_0)\|\cdots\|(b_{2^m-1}\|\alpha_{2^m-1})$, such that $b_x \neq 0$ holds for at most i indices x. Intuitively, $b_x \neq 0$ means that $\mathcal{A}$ has queried x to a random function f and has information that $f(x) = \alpha_x$. If $b_x = 0$, then $\alpha_x = 0^n$ holds.

3.3.0.2 Encoding Functions to Databases: Formal Descriptions

The above three operations can be formally realized as actions of unitary operators on $|f\rangle$-registers. The first one is realized as $\mathsf{IH} := (I_1 \otimes H^{\otimes n})^{\otimes 2^m}$. The second one is realized as $U_{\text{toggle}} := (I_1 \otimes |0^n\rangle\langle 0^n| + X \otimes (I_n - |0^n\rangle\langle 0^n|))^{\otimes 2^m}$, where X is the 1-qubit operator such that $X|0\rangle = |1\rangle$ and $X|1\rangle = |0\rangle$. The third one is realized by the operator $\mathsf{CH} := (CH^{\otimes n})^{\otimes 2^m}$, where $CH := |0\rangle\langle 0| \otimes I_n + |1\rangle\langle 1| \otimes H^{\otimes n}$.

We call the action of the unitary operator $U_{\text{enc}} := \mathsf{CH} \cdot U_{\text{toggle}} \cdot \mathsf{IH}$ and its conjugate U^*_{enc} *encoding* and *decoding*, respectively.

Remark 8. *In Zhandry's paper [Zha19], U_{enc} and U^*_{enc} correspond to a single unitary operator* StdDecomp′ *that is defined in a theoretically concise and sophisticated way. We use the encoding as the composition of three unitary operators like above so that the intuition behind the encoding and decoding is clear as much as possible.*

By using our encoding and decoding, the recording standard oracle with errors is defined as follows.

Definition 2 (Recording standard oracle with errors)**.** *The* recording standard oracle with errors *is the quantum oracle such that queries are processed with the unitary operator* RstOE *defined by* $\mathsf{RstOE} := (I \otimes U_{\text{enc}}) \cdot \mathsf{stO} \cdot (I \otimes U^*_{\text{enc}})$ *and the initial state is* $|0^{(n+1)2^m}\rangle$*. (See also Fig. 3.1.)*

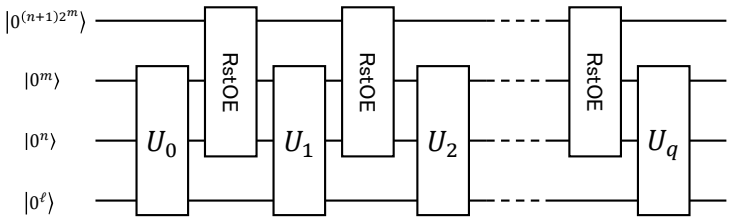


Figure 3.1: A quantum circuit that illustrates an adversary $\mathcal{A}$ that runs relative to RstOE. The register $|0^{(n+1)2^m}\rangle$ at the top corresponds to the oracle's state. The second and third registers ($|0^m\rangle$ and $|0^n\rangle$) are used to send queries and receive answers, respectively. The register $|0^\ell\rangle$ at the bottom corresponds to $\mathcal{A}$'s private working space for offline computations.

The original compressed oracle maintains only an $O(i(m+n))$-qubit state by compressing databases. On the other hand, our oracle always has $(n+1)2^m$-qubit states since we do not consider any compression.

3.3.1 Core Properties of RstOE

This subsection describes some useful properties of RstOE.

Note that $|\tilde{\psi}_i\rangle = \mathsf{RstOE}(U_{i-1} \otimes I)\mathsf{RstOE} \cdots \mathsf{RstOE}(U_0 \otimes I)(|0^\ell\rangle \otimes |0^{(n+1)2^m}\rangle)$ and $|\tilde{\phi}_i\rangle = (I \otimes U_{\mathrm{enc}}^*)\,|\tilde{\psi}_i\rangle$ hold for each i. Therefore, the following proposition holds.

Proposition 1. *The recording standard oracle with errors is perfectly indistinguishable from the quantum oracle of a random function.*

The following proposition guarantees that each database contains at most i entries after i quantum queries.

Proposition 2. *Let $i \geq 1$. Suppose that we measure the oracle states' register of $|\psi_{i+1}\rangle$ and obtained a database D. Then D is valid, and contains at most i entries.*

Proof. Let I_A and I_D denote the identity operators on the adversary's states and databases, respectively ($I_A \otimes I_D$ becomes the identity operator on the entire state space). Recall that U_j denotes the unitary operator for the adversary's offline computation after the j-th query.

First,

$$|\tilde{\psi}_i\rangle = ((U_{i-1} \otimes I_D) \cdot \mathsf{RstOE}) \cdots ((U_1 \otimes I_D) \cdot \mathsf{RstOE})\,|\tilde{\psi}_1\rangle$$

holds for $i \geq 2$.

Second, recall that

$$\mathsf{RstOE} = (I_A \otimes U_{\mathrm{enc}}) \cdot \mathsf{stO} \cdot (I_A \otimes U_{\mathrm{enc}})^*$$

holds. Since U_{enc} does not act on the adversary's registers, and "$U_{\mathrm{toggle}} \cdot \mathsf{CH}$" in

$$(U_{\mathrm{enc}})^* = \mathsf{IH} \cdot U_{\mathrm{toggle}} \cdot \mathsf{CH}$$

does not change the state $|\tilde{\psi}_1\rangle$ (because the database register of $|\tilde{\psi}_1\rangle$ is all 0), we have

$$|\tilde{\psi}_i\rangle = (I_A \otimes U_{\mathrm{enc}}) \cdot ((U_{i-1} \otimes I_D) \cdot \mathsf{stO}) \cdots ((U_1 \otimes I_D) \cdot \mathsf{stO}) \cdot \mathsf{IH}\,|\tilde{\psi}_1\rangle$$

for $i \geq 2$.

Next, define

$$\begin{aligned}
\mathsf{stO}' &:= (H^{\otimes m} \otimes \mathsf{IH})\mathsf{stO}(H^{\otimes m} \otimes \mathsf{IH}),\\
U'_j &:= H^{\otimes m} \cdot U_j \cdot H^{\otimes m} \text{ for } j = 1, \ldots, i-2, \text{ and}\\
U'_{i-1} &:= U_{i-1} \cdot H^{\otimes m},\\
U'_{\mathrm{enc}} &:= (\mathsf{CH} \cdot U_{\mathrm{toggle}}),
\end{aligned}$$

where $H^{\otimes m}$ acts on the adversary's register to receive answers from the oracle. Then

$$|\tilde{\psi}_i\rangle = (I_A \otimes U'_{\mathrm{enc}}) \cdot ((U'_{i-1} \otimes I_D) \cdot \mathsf{stO}') \cdots ((U'_1 \otimes I_D) \cdot \mathsf{stO}') \cdot (H^{\otimes m} \otimes I_D)\,|\tilde{\psi}_1\rangle \tag{3.11}$$

follows.

Recall that

$$\mathsf{stO}\,|x\rangle\,|y\rangle\,|S\rangle = |x\rangle\,|y \oplus s_x\rangle\,|S\rangle$$

holds, where $x \in \{0,1\}^m$, $y \in \{0,1\}^n$, and $S = (b_0\|s_0)\|(b_1\|s_1)\|\cdots\|(b_{2^m-1}\|s_{2^m-1})$, where $b_i \in \{0,1\}$ and $s_i \in \{0,1\}^n$ for each $i \in \{0,1\}^m$. On the other hand, straightforward calculations show that

$$\mathsf{stO}'\,|x\rangle\,|y\rangle\,|S\rangle = |x\rangle\,|y \oplus s_x\rangle\,|S \oplus (y)_x\rangle$$

holds, where $S \oplus (y)_x := (b_0\|s_0)\|\cdots\|(b_x\|s_x \oplus y)\|\cdots\|(b_{2^m-1}\|s_{2^m-1})$.

Since the database register of $|\tilde{\psi}_1\rangle$ is all 0, when we measure the state

$$((U'_{i-1} \otimes I_D) \cdot \mathsf{stO}') \cdots ((U'_1 \otimes I_D) \cdot \mathsf{stO}') \cdot (H^{\otimes m} \otimes I_D)\,|\tilde{\psi}_1\rangle,$$

we always obtain a bit string S of the form

$$S = (0||s_0)||(0||s_1)||...||(0||s_{2^m-1}),$$

where the number of j such that $s_j \neq 0$ is at most $(i-1)$. When $U'_{\mathrm{enc}} = \mathsf{CH} \cdot U_{\mathrm{toggle}}$ acts on such a state $|S\rangle$, we always obtain a (superposition of) valid database D with $|D| \leq (i-1)$. Since (3.11) holds, this means that the claim of Proposition 2 holds. □

Next, we introduce notations that are required to describe important properties of RstOE. We call a bit string $D = (b_0\|\alpha_0)\|\cdots\|(b_{2^m-1}\|\alpha_{2^m-1})$, where $b_x \in \{0,1\}$ and $\alpha_x \in \{0,1\}^n$ for each $x \in \{0,1\}^m$, is a *valid database* if $\alpha_x \neq 0^n$ holds only if $b_x = 1$. We call D an *invalid database* if it is not a valid database. Note that, in a valid database, b_x can be 0 or 1 if $\alpha_x = 0^n$. We identify a valid database D with the partially defined function from $\{0,1\}^m$ to $\{0,1\}^n$ of which the value on $x \in \{0,1\}^m$ is defined to be y if and only if $b_x = 1$ and $\alpha_x = y$. We use the same notation D for this function. If x is in the domain of D, we write $D(x) \neq \perp$, and otherwise write $D(x) = \perp$. Moreover, we identify D with the set $\{(x, D(x))\}_{x\in\mathrm{dom}(D)} \subset \{0,1\}^m \times \{0,1\}^n$, and we use the notations $D \cup (x,\alpha)$ and $D \setminus (x',\alpha')$ to denote the insertion of (x,α) into D and the deletion of (x',α') from D. For a valid database D that corresponds to the bit string $(b_0||\alpha_0)||\cdots||(b_{2^m-1}||\alpha_{2^m-1})$ such that $D(x) = \perp$ (i.e., $b_x = 0$ and $\alpha_x = 0^n$) and $\gamma \neq 0^n$, we denote the invalid database that corresponds to the bit string $(b_0||\alpha_0)||\cdots||(b_{x-1}||\alpha_{x-1})||(0||\gamma)||(b_{x+1}||\alpha_{x+1})||\cdots||(b_{2^m-1}||\alpha_{2^m-1})$ by $D \cup [\![x,\gamma]\!]$. Unless otherwise noted, we always assume that D is valid.

The following proposition describes the core properties of RstOE.

Proposition 3 (Core Properties)**.** *Let D be a valid database and suppose that n is sufficiently large ($n \geq 6$ suffices). Then, the following properties hold.*

1. *Suppose that $D(x) = \perp$. Then, for any y and α, there exists a vector $|\epsilon\rangle$ such that*

$$\mathsf{RstOE}\,|x\rangle\,|y\rangle \otimes |D \cup (x,\alpha)\rangle = |x\rangle\,|y \oplus \alpha\rangle \otimes |D \cup (x,\alpha)\rangle + |\epsilon\rangle$$

and $\| |\epsilon\rangle \| \leq 5/\sqrt{2^n}$. More precisely,

$$\mathsf{RstOE}\,|x,y\rangle \otimes |D \cup (x,\alpha)\rangle = |x, y \oplus \alpha\rangle \otimes |D \cup (x,\alpha)\rangle \tag{3.12}$$

$$+ \frac{1}{\sqrt{2^n}}\,|x, y \oplus \alpha\rangle \left(|D\rangle - \left(\sum_{\gamma\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|D \cup (x,\gamma)\rangle \right) \right) \tag{3.13}$$

$$- \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}}\,|x, y \oplus \gamma\rangle \otimes \left(|D \cup (x,\gamma)\rangle - |D^{\mathsf{invalid}}_{\gamma}\rangle \right) \tag{3.14}$$

$$+ \frac{1}{2^n}\,|x\rangle\,|\widehat{0^n}\rangle \otimes \left(2 \sum_{\delta\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|D \cup (x,\delta)\rangle - |D\rangle \right) \tag{3.15}$$

holds, where $|D^{\mathsf{invalid}}_{\gamma}\rangle$ is a superposition of invalid databases defined by

$$|D^{\mathsf{invalid}}_{\gamma}\rangle := \sum_{\delta\neq 0^n} \frac{(-1)^{\gamma\cdot\delta}}{\sqrt{2^n}}\,|D \cup [\![x,\delta]\!]\rangle$$

for each γ, and $|\widehat{0^n}\rangle = H^{\otimes n}\,|0^n\rangle$.

2. *Suppose that $D(x) = \perp$. Then, for any y, there exists a vector $|\epsilon'\rangle$ such that*

$$\mathsf{RstOE}\,|x\rangle\,|y\rangle \otimes |D\rangle = \sum_{\alpha\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|x\rangle\,|y \oplus \alpha\rangle \otimes |D \cup (x,\alpha)\rangle + |\epsilon'\rangle \tag{3.16}$$

and $\| |\epsilon'\rangle \| \leq 2/\sqrt{2^n}$. To be more precise,

$$|\epsilon'\rangle = \frac{1}{\sqrt{2^n}}\,|x\rangle\,|\widehat{0^n}\rangle \otimes \left(|D\rangle - \sum_{\gamma\in\{0,1\}^n} \frac{1}{\sqrt{2^n}}\,|D \cup (x,\gamma)\rangle \right) \tag{3.17}$$

holds, where $|\widehat{0^n}\rangle = H^{\otimes n}\,|0^n\rangle$.

An intuitive interpretation of Proposition 3. The proposition shows that, when the adversary's state is not superposed, we can intuitively capture time evolutions of databases with only the (classical) lazy-sampling-like arguments by ignoring the error terms $|\epsilon\rangle$ and $|\epsilon'\rangle$: When an adversary makes a query x to the oracle, RstOE looks for a tuple (x,α) in the database. If one is found, respond with α (the first property in the above proposition). If no tuple is found, create the superposition $\frac{1}{\sqrt{2^n}} \sum_{\alpha_x} |\alpha_x\rangle$, respond with α_x, and add (x,α_x) to the database (the second property in the above proposition).

Note that this intuition for the classical lazy-sampling does not necessarily work when the adversary's state is superposed. This means that, intuitively, a record (x, α) in a database may be deleted or overwritten by another record (x, γ) when a quantum query is made.

For example, suppose that the database is empty, the adversary's state is $|x\rangle|0^n\rangle$,[6] and the adversary makes the same query twice. At the first query, the adversary's state is not superposed and the classical intuition works: Due to the second property of the proposition, the state changes to $\sum_\alpha |x\rangle|\alpha\rangle \otimes |(x,\alpha)\rangle$ up to a small error term $|\epsilon'\rangle$. This intuitively means that α is randomly sampled and the data (x, α) is added to the database. At the second query, classical intuition says that the data (x, α) will be kept in the database. However, now the adversary's state is superposed and the classical intuition does not work: Since $\mathsf{RstOE} \cdot \mathsf{RstOE} = I$ holds and the second query cancels the first query, the database gets back to empty. This means that the sum of the error terms (in the first property of the proposition) must be large at the second query.

Therefore, sometimes we can ignore the error terms and use the classical intuition, but sometimes we cannot.

Remark 9. *For invalid databases, basically we can ignore them in security proofs since, when we measure the database register while an adversary runs relative to the recording standard oracle with errors, we always obtain a valid database.*

Proof of Proposition 3. Recall that RstOE is decomposed as

$$\mathsf{RstOE} = (I \otimes \mathsf{CH}) \cdot (I \otimes U_{\mathrm{toggle}}) \cdot (I \otimes \mathsf{IH})\mathsf{stO}(I \otimes \mathsf{IH}^*) \cdot (I \otimes U^*_{\mathrm{toggle}}) \cdot (I \otimes \mathsf{CH}^*), \tag{3.18}$$

and that each D is described as a bit string $(b_0\|\alpha_0)\|\cdots\|(b_{2^m-1}\|\alpha_{2^m-1})$, where $b_x \in \{0,1\}$ and $\alpha_x \in \{0,1\}^n$ for each $x \in \{0,1\}^m$.

We begin with showing the first property. Since now the operator RstOE does not affect the registers of entry of x' in D for $x' \neq x$, it suffices to show that the claim holds when D is empty. In addition, without loss of generality, we can assume that $x = 0^m$. Now $D \cup (x, \alpha)$ corresponds to the bit string $(1\|\alpha)\|(0\|0^n)\|\cdots\|(0\|0^n)$. We have that $U^*_{\mathrm{enc}} = \mathsf{IH}^* U^*_{\mathrm{toggle}} \mathsf{CH}^* = \mathsf{IH} U_{\mathrm{toggle}} \mathsf{CH}$ and

$$\begin{aligned}
U^*_{\mathrm{enc}} |D \cup (x,\alpha)\rangle &= \mathsf{IH} U_{\mathrm{toggle}} \left(\sum_{u\in\{0,1\}^n} \frac{(-1)^{\alpha\cdot u}}{\sqrt{2^n}} |1\|u\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\|0^n\rangle \right) \\
&= \mathsf{IH} \left(\sum_{u\in\{0,1\}^n} \frac{(-1)^{\alpha\cdot u}}{\sqrt{2^n}} |0\|u\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\|0^n\rangle \right) + \mathsf{IH} \left(\frac{1}{\sqrt{2^n}} (|1\|0^n\rangle - |0\|0^n\rangle) \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\|0^n\rangle \right) \\
&= |0\|\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle |\widehat{0^n}\rangle \right) + |\epsilon_1\rangle,
\end{aligned} \tag{3.19}$$

where $|\widehat{0^n}\rangle := H^{\otimes n}|0^n\rangle$ and $|\epsilon_1\rangle = \frac{1}{\sqrt{2^n}}(|1\rangle - |0\rangle)|\widehat{0^n}\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle|\widehat{0^n}\rangle\right)$. Thus, we have that

$$\mathsf{stO}\,(I \otimes U^*_{\mathrm{enc}})\,|x,y\rangle \otimes |D \cup (x,\alpha)\rangle = |x, y\oplus\alpha\rangle \otimes |0\|\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle|\widehat{0^n}\rangle \right) + \mathsf{stO}(|x,y\rangle \otimes |\epsilon_1\rangle). \tag{3.20}$$

Note that, from (3.19), it follows that

$$U_{\mathrm{enc}} \left(|0\|\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle|\widehat{0^n}\rangle \right) + |\epsilon_1\rangle \right) = |D \cup (x,\alpha)\rangle\,. \tag{3.21}$$

Therefore,

$$\begin{aligned}
&(I \otimes U_{\mathrm{enc}})\,\mathsf{stO}\,(I \otimes U^*_{\mathrm{enc}})\,|x,y\rangle \otimes |D \cup (x,\alpha)\rangle \\
&= (I \otimes U_{\mathrm{enc}}) \left(|x, y\oplus\alpha\rangle \otimes |0\|\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle|\widehat{0^n}\rangle \right) + \mathsf{stO}(|x,y\rangle \otimes |\epsilon_1\rangle) \right) \\
&= (I \otimes U_{\mathrm{enc}}) \left(|x, y\oplus\alpha\rangle \otimes |0\|\alpha\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle|\widehat{0^n}\rangle \right) + |x, y\oplus\alpha\rangle \otimes |\epsilon_1\rangle \right) \\
&\qquad - (I \otimes U_{\mathrm{enc}})\,(|x, y\oplus\alpha\rangle \otimes |\epsilon_1\rangle) + (I \otimes U_{\mathrm{enc}})\mathsf{stO}(|x,y\rangle \otimes |\epsilon_1\rangle) \\
&= |x, y\oplus\alpha\rangle \otimes |D \cup (x,\alpha)\rangle + |\epsilon_2\rangle
\end{aligned} \tag{3.22}$$

[6] $|x\rangle$ corresponds to the register to send queries to the oracle and $|0^n\rangle$ corresponds to the register to receive answers from the oracle.

holds, where $|\epsilon_2\rangle = -(I \otimes U_{\mathrm{enc}})(|x, y \oplus \alpha\rangle \otimes |\epsilon_1\rangle) + (I \otimes U_{\mathrm{enc}})\mathsf{stO}(|x, y\rangle \otimes |\epsilon_1\rangle)$. Now we have that

$$
\begin{aligned}
&(I \otimes U_{\mathrm{enc}})\mathsf{stO}(|x, y\rangle \otimes |\epsilon_1\rangle) \\
&= (I \otimes \mathsf{CH} \cdot U_{\mathrm{toggle}} \cdot \mathsf{IH}) \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes (|1\rangle - |0\rangle) \otimes |\gamma\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |\widehat{0^n}\rangle \right) \\
&= (I \otimes \mathsf{CH} \cdot U_{\mathrm{toggle}}) \frac{1}{\sqrt{2^n}} \sum_{\gamma,\delta} \frac{(-1)^{\gamma\cdot\delta}}{2^n} |x, y \oplus \gamma\rangle \otimes (|1\rangle - |0\rangle) \otimes |\delta\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&= (I \otimes \mathsf{CH}) \frac{1}{\sqrt{2^n}} \sum_{\gamma,\delta} \frac{(-1)^{\gamma\cdot\delta}}{2^n} |x, y \oplus \gamma\rangle \otimes (|0\rangle - |1\rangle) \otimes |\delta\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&\quad + (I \otimes \mathsf{CH}) \frac{2}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{2^n} |x, y \oplus \gamma\rangle \otimes (|1\rangle - |0\rangle) \otimes |0^n\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes \left(|0\rangle \otimes \left(H^{\otimes n} |\gamma\rangle \right) - |1\rangle \otimes |\gamma\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&\quad + \frac{2}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{2^n} |x, y \oplus \gamma\rangle \otimes \left(|1\rangle \otimes \left(H^{\otimes n} |0^n\rangle \right) - |0\rangle \otimes |0^n\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |0\rangle \otimes \left(H^{\otimes n} |\gamma\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&\quad - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |1\rangle \otimes |\gamma\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&\quad + \frac{2}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{2^n} |x, y \oplus \gamma\rangle \otimes \left(\sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |0\rangle \otimes \left(\sum_{\delta} \frac{(-1)^{\gamma\cdot\delta}}{\sqrt{2^n}} |\delta\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&\quad - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |1\rangle \otimes |\gamma\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&\quad + \frac{2}{2^n} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes \left(\sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |0\rangle \otimes \left(\sum_{\delta \neq 0^n} \frac{(-1)^{\gamma\cdot\delta}}{\sqrt{2^n}} |\delta\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&\quad + \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |0\rangle \otimes \left(\frac{1}{\sqrt{2^n}} |0^n\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&\quad - \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |1\rangle \otimes |\gamma\rangle \otimes \left(\bigotimes_{i=1}^{2^m-1} |0\rangle\, |0^n\rangle \right) \\
&\quad + \frac{2}{2^n} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes \left(\sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |D_{\gamma}^{\mathsf{invalid}}\rangle \\
&\quad + \frac{1}{2^n} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |D\rangle
\end{aligned}
$$

$$
\begin{aligned}
&- \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes |D \cup (x, \gamma)\rangle \\
&+ \frac{2}{2^n} |x\rangle |\widehat{0^n}\rangle \otimes \left(\sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right) \\
&= -\frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes \left(|D \cup (x, \gamma)\rangle - |D_{\gamma}^{\mathsf{invalid}}\rangle \right) \\
&+ \frac{1}{2^n} |x\rangle |\widehat{0^n}\rangle \otimes \left(2 \sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right), \qquad (3.23)
\end{aligned}
$$

where

$$
|D_{\gamma}^{\mathsf{invalid}}\rangle = \left(\sum_{\delta \neq 0^n} \frac{(-1)^{\gamma \cdot \delta}}{\sqrt{2^n}} |0\rangle |\delta\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m - 1} |0\rangle |0^n\rangle \right) = \sum_{\delta \neq 0^n} \frac{(-1)^{\gamma \cdot \delta}}{\sqrt{2^n}} |D \cup [\![x, \delta]\!]\rangle
$$

for each γ.

In addition, we have that

$$
\begin{aligned}
U_{\mathrm{enc}} |\epsilon_1\rangle &= (\mathsf{CH} U_{\mathrm{toggle}} \mathsf{IH}) \frac{1}{\sqrt{2^n}} (|1\rangle - |0\rangle) |\widehat{0^n}\rangle \otimes \left(\bigotimes_{i=1}^{2^m - 1} |0\rangle |\widehat{0^n}\rangle \right) \\
&= \mathsf{CH} \frac{1}{\sqrt{2^n}} (|1\rangle - |0\rangle) |0^n\rangle \otimes \left(\bigotimes_{i=1}^{2^m - 1} |0\rangle |0^n\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} (|1\rangle |\widehat{0^n}\rangle - |0\rangle |0^n\rangle) \otimes \left(\bigotimes_{i=1}^{2^m - 1} |0\rangle |0^n\rangle \right) \\
&= \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle - \frac{1}{\sqrt{2^n}} |D\rangle \qquad (3.24)
\end{aligned}
$$

holds. Thus,

$$
(I \otimes U_{\mathrm{enc}}) |x, y \oplus \alpha\rangle \otimes |\epsilon_1\rangle = \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \left(\left(\sum_{\gamma} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) - |D\rangle \right) \qquad (3.25)
$$

holds. Therefore,

$$
\begin{aligned}
\mathsf{RstOE} |x, y\rangle \otimes |D \cup (x, \alpha)\rangle &= |x, y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle \\
&+ \frac{1}{\sqrt{2^n}} |x, y \oplus \alpha\rangle \left(|D\rangle - \left(\sum_{\gamma} \frac{1}{\sqrt{2^n}} |D \cup (x, \gamma)\rangle \right) \right) \\
&- \frac{1}{\sqrt{2^n}} \sum_{\gamma} \frac{1}{\sqrt{2^n}} |x, y \oplus \gamma\rangle \otimes \left(|D \cup (x, \gamma)\rangle - |D_{\gamma}^{\mathsf{invalid}}\rangle \right) \\
&+ \frac{1}{2^n} |x\rangle |\widehat{0^n}\rangle \otimes \left(2 \sum_{\delta} \frac{1}{\sqrt{2^n}} |D \cup (x, \delta)\rangle - |D\rangle \right) \qquad (3.26)
\end{aligned}
$$

holds, and this proves the first property.

Next, we show the second property. Since now the operator RstOE does not affect the registers of entry of x' in D for $x' \neq x$, it suffices to show that the claim holds when D has no entry. In addition, we can without loss of generality assume that $x = 0^m$. Now D corresponds to the bit string $(0\|0^n)\|(0\|0^n)\|\cdots\|(0\|0^n)$, and we have that

$$
\begin{aligned}
U_{\mathrm{enc}}^{*} |D\rangle &= \mathsf{IH} U_{\mathrm{toggle}} \mathsf{CH} |D\rangle \\
&= \left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} |0\rangle |\alpha\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m - 1} |0\rangle |\widehat{0^n}\rangle \right). \qquad (3.27)
\end{aligned}
$$

Hence, it holds that

$$\mathsf{stO}(I \otimes U_{\mathrm{enc}}^{*}) \left|x, y\right\rangle \otimes \left|D\right\rangle = \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \alpha\right\rangle \otimes \left|0\right\rangle \left|\alpha\right\rangle \otimes \left(\bigotimes_{i=1}^{2^m - 1} \left|0\right\rangle \left|\widehat{0^n}\right\rangle \right). \tag{3.28}$$

In addition, we have that

$$\begin{aligned}
&(I \otimes U_{\mathrm{enc}})\mathsf{stO}(I \otimes U_{\mathrm{enc}}^{*}) \left|x, y\right\rangle \otimes \left|D\right\rangle \\
&= (I \otimes (\mathsf{CH} U_{\mathrm{toggle}} \mathsf{IH})) \left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \alpha\right\rangle \otimes \left|0\right\rangle \left|\alpha\right\rangle \otimes \left(\bigotimes_{i=1}^{2^m - 1} \left|0\right\rangle \left|\widehat{0^n}\right\rangle \right) \right) \\
&= (I \otimes (\mathsf{CH} U_{\mathrm{toggle}})) \left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \alpha\right\rangle \otimes \left(\sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} \left|0\right\rangle \left|u\right\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m - 1} \left|0\right\rangle \left|0^n\right\rangle \right) \right) \\
&= (I \otimes \mathsf{CH}) \left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \alpha\right\rangle \otimes \left(\sum_{u \in \{0,1\}^n} \frac{(-1)^{\alpha \cdot u}}{\sqrt{2^n}} \left|1\right\rangle \left|u\right\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m - 1} \left|0\right\rangle \left|0^n\right\rangle \right) \right) \\
&\quad + (I \otimes \mathsf{CH}) \left(\sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \alpha\right\rangle \otimes \left(\frac{1}{\sqrt{2^n}} (\left|0\right\rangle - \left|1\right\rangle) \otimes \left|0^n\right\rangle \right) \otimes \left(\bigotimes_{i=1}^{2^m - 1} \left|0\right\rangle \left|0^n\right\rangle \right) \right) \\
&= \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \alpha\right\rangle \otimes \left|1\right\rangle \left|\alpha\right\rangle \otimes \left(\bigotimes_{i=1}^{2^m - 1} \left|0\right\rangle \left|0^n\right\rangle \right) \\
&\quad + \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \alpha\right\rangle \otimes \left(\frac{1}{\sqrt{2^n}} (\left|0\right\rangle \left|0^n\right\rangle - \left|1\right\rangle \left|\widehat{0^n}\right\rangle) \right) \otimes \left(\bigotimes_{i=1}^{2^m - 1} \left|0\right\rangle \left|0^n\right\rangle \right) \\
&= \sum_{\alpha \in \{0,1\}^n} \frac{1}{\sqrt{2^n}} \left|x, y \oplus \alpha\right\rangle \otimes \left|D \cup (x, \alpha)\right\rangle \\
&\quad + \frac{1}{\sqrt{2^n}} \left|x\right\rangle \left|\widehat{0^n}\right\rangle \otimes \left(\left|D\right\rangle - \sum_{\gamma} \frac{1}{\sqrt{2^n}} \left|D \cup (x, \gamma)\right\rangle \right)
\end{aligned} \tag{3.29}$$

holds. Therefore, the second property also holds. □

Let RstOE be the recording oracle with errors for a random function $f : \{0,1\}^m \to \{0,1\}^n$. We also show the following proposition for later use.

Proposition 4. *Let y be a fixed n-bit string, and*

$$\begin{aligned}
\left|\psi\right\rangle = &\sum_{\substack{x \in \{0,1\}^m, \alpha \in \{0,1\}^n, D \\ D(x) = \perp}} c_{x,\alpha,D} \left|x, y\right\rangle \otimes \left|D \cup (x, \alpha)\right\rangle \otimes \left|\psi_{x,\alpha,D}\right\rangle \\
&+ \sum_{\substack{x \in \{0,1\}^m, D \\ D(x) = \perp}} c'_{x,D} \left|x, y\right\rangle \otimes \left|D\right\rangle \otimes \left|\psi'_{x,D}\right\rangle
\end{aligned}$$

be a vector such that $\| \left|\psi\right\rangle \| \leq 1$, $\| \left|\psi_{x,D}\right\rangle \| \leq 1$, and $\| \left|\psi'_{x,\alpha,D}\right\rangle \| \leq 1$ for each x, α, and D. Here, $\left|x\right\rangle$ and $\left|y\right\rangle$ are the registers to send queries to f and receive the responses, respectively, and $\left|\psi_{x,\alpha,D}\right\rangle, \left|\psi'_{x,D}\right\rangle$ correspond to an additional quantum system on which RstOE does not affect. In addition, $c_{x,\alpha,D}$ and $c'_{x,D}$ are complex numbers such that

$$\sum_{\substack{x \in \{0,1\}^m, \alpha \in \{0,1\}^n, D \\ D(x) = \perp}} |c_{x,\alpha,D}|^2 \leq 1$$

and

$$\sum_{\substack{x \in \{0,1\}^m, D \\ D(x) = \perp}} |c'_{x,D}|^2 \leq 1.$$

Let Π_{valid} *be the orthogonal projection onto the vector space spanned by valid databases. Then there exists a vector* $|\epsilon\rangle$ *such that* $\| |\epsilon\rangle \| \leq 10/\sqrt{2^n}$ *and*

$$\begin{aligned}\Pi_{\mathsf{valid}}\mathsf{RstOE}\,|\psi\rangle = &\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\bot}} c_{x,\alpha,D}\,|x,y\oplus\alpha\rangle\otimes|D\cup(x,\alpha)\rangle\otimes|\psi_{x,\alpha,D}\rangle\\ &-\sum_{\substack{x\in\{0,1\}^m,\alpha,\gamma\in\{0,1\}^n,D\\ D(x)=\bot}} \frac{1}{2^n}c_{x,\alpha,D}\,|x,y\oplus\gamma\rangle\otimes|D\cup(x,\gamma)\rangle\otimes|\psi_{x,\alpha,D}\rangle\\ &+\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\bot}} c'_{x,D}\frac{1}{\sqrt{2^n}}\,|x,y\oplus\alpha\rangle\otimes|D\cup(x,\alpha)\rangle\otimes|\psi'_{x,D}\rangle\\ &+|\epsilon\rangle\end{aligned}$$

hold.

An intuitive interpretation of Proposition 4. Intuitively, this proposition shows that, when an adversary's register to receive responses from the oracle (i.e., the $|y\rangle$ register) is not superposed, we can ignore the effect that an existing record (x,α) will be deleted from a database. (Nevertheless, we cannot ignore the effect that an existing record (x,α) will be overwritten with another record (x,γ).)

Proof of Proposition 4. Let

$$|\phi_0\rangle := \sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\bot}} c_{x,\alpha,D}\,|x,y\oplus\alpha\rangle\otimes|D\cup(x,\alpha)\rangle\otimes|\psi_{x,\alpha,D}\rangle,$$

$$|\phi_1\rangle := \sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\bot}} c_{x,\alpha,D}\frac{1}{\sqrt{2^n}}\,|x,y\oplus\alpha\rangle\otimes\left(|D\rangle-\left(\sum_{\gamma\in\{0,1\}^n}\frac{1}{\sqrt{2^n}}\,|D\cup(x,\gamma)\rangle\right)\right)\otimes|\psi_{x,\alpha,D}\rangle,$$

$$|\phi_2\rangle := -\sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\bot}} c_{x,\alpha,D}\frac{1}{\sqrt{2^n}}\sum_{\gamma}\frac{1}{\sqrt{2^n}}\,|x,y\oplus\gamma\rangle\otimes\left(|D\cup(x,\gamma)\rangle-|D^{\mathsf{invalid}}_{\gamma}\rangle\right)\otimes|\psi_{x,\alpha,D}\rangle,$$

$$|\phi_3\rangle := \sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\bot}} c_{x,\alpha,D}\frac{1}{2^n}\,|x\rangle|\widehat{0^n}\rangle\otimes\left(2\sum_{\delta\in\{0,1\}^n}\frac{1}{\sqrt{2^n}}\,|D\cup(x,\delta)\rangle-|D\rangle\right)\otimes|\psi_{x,\alpha,D}\rangle,$$

$$|\phi'_0\rangle := \sum_{\substack{x\in\{0,1\}^m,\alpha\in\{0,1\}^n,D\\ D(x)=\bot}} c'_{x,D}\frac{1}{\sqrt{2^n}}\,|x,y\oplus\alpha\rangle\otimes|D\cup(x,\alpha)\rangle\otimes|\psi'_{x,D}\rangle,$$

$$|\phi'_1\rangle := \sum_{\substack{x\in\{0,1\}^m,D\\ D(x)=\bot}} c'_{x,D}\frac{1}{\sqrt{2^n}}\,|x\rangle|\widehat{0^n}\rangle\otimes\left(|D\rangle-\sum_{\gamma\in\{0,1\}^n}\frac{1}{\sqrt{2^n}}\,|D\cup(x,\gamma)\rangle\right)\otimes|\psi'_{x,D}\rangle\,.$$

Then

$$\mathsf{RstOE}\,|\psi\rangle = \sum_{0\leq i\leq 3}|\phi_i\rangle+\sum_{0\leq i\leq 1}|\phi'_i\rangle$$

follows from Proposition 3.

Upper bounding $\| |\phi_1\rangle \|$.
First, for distinct tuples $(x,\alpha,D)\neq(x',\alpha',D')$ such that $D(x)=\bot$ and $D(x')=\bot$,

$$|x,y\oplus\alpha\rangle\otimes\left(|D\rangle-\left(\sum_{\gamma\in\{0,1\}^n}\frac{1}{\sqrt{2^n}}\,|D\cup(x,\gamma)\rangle\right)\right)$$

is orthogonal to

$$|x',y\oplus\alpha'\rangle\otimes\left(|D'\rangle-\left(\sum_{\gamma\in\{0,1\}^n}\frac{1}{\sqrt{2^n}}\,|D'\cup(x',\gamma)\rangle\right)\right).$$

Thus

$$\| |\phi_1\rangle \|^2 \leq (2/2^n) \cdot \sum_{\substack{x\in\{0,1\}^m, \alpha\in\{0,1\}^n, D \\ D(x)=\perp}} |c_{x,\alpha,D}|^2 \leq 2/2^n \tag{3.30}$$

holds.

Upper bounding $\| |\phi_3\rangle \|$.
We have that

$$\| |\phi_3\rangle \|^2 \leq 5 \cdot \sum_{\substack{x\in\{0,1\}^m, D \\ D(x)=\perp}} \left(\sum_{\alpha} \frac{|c_{x,\alpha,D}|}{2^n} \right)^2 \leq 5 \cdot \sum_{\substack{x\in\{0,1\}^m, D \\ D(x)=\perp}} \frac{\sum_{\alpha} |c_{x,\alpha,D}|^2}{2^n} \leq \frac{5}{2^n} \tag{3.31}$$

holds, where we used the convexity of the function $X \mapsto X^2$ for the second inequality.

Upper bounding $\| |\phi'_1\rangle \|$.
We have that

$$\left\| |\phi'_1\rangle \right\|^2 \leq \frac{2}{2^n} \sum_{\substack{x\in\{0,1\}^m, D \\ D(x)=\perp}} |c'_{x,D}|^2 \leq \frac{2}{2^n} \tag{3.32}$$

holds.

Now the claim of the proposition holds by setting $|\epsilon\rangle := |\phi_1\rangle + |\phi_3\rangle + |\phi'_1\rangle$. □

Chapter 4

Quantum Security of the 4-Round Luby-Rackoff Construction

This chapter provides technical details of our results on the 4-round Luby-Rackoff construction. The result of this chapter contributes to understanding (post-)quantum security of symmetric-key schemes mainly from the theoretical perspective. The Luby-Rackoff construction is the most important scheme to convert PRFs to PRPs. Thus the problem of whether the r-round Luby-Rackoff construction is a secure qPRP for some r is theoretically significant. However, the problem has been unresolved since Kuwakado and Morii showed the 3-round quantum distinguisher [KM10]. We solve it by proving that the 4-round construction is indeed a secure qPRP. See also Section 1.2 for an overview, and Section 1.7 for the relationship of the results in this chapter with those in other chapters.

First, we briefly recall the definition of the Luby-Rackoff constructions. Fix $r \geq 1$, and for $1 \leq i \leq r$, let $f_i := \{f_{i,k} : \{0,1\}^{n/2} \to \{0,1\}^{n/2}\}_{k \in \mathcal{K}}$ be a family of functions parameterized by key k in a key space $\mathcal{K}$. Then, the Luby-Rackoff construction for $f_1, \ldots, f_r$ is defined as a family of n-bit permutations $\mathsf{LR}_r(f_1, \ldots, f_r) := \{\mathsf{LR}_r(f_{1,k_1}, \ldots, f_{r,k_r})\}_{k_1,\ldots,k_r \in \mathcal{K}}$ with the key space $(\mathcal{K})^r$. For each fixed key $(k_1, \ldots, k_r)$, $\mathsf{LR}_r(f_{1,k_1}, \ldots, f_{r,k_r})$ is defined by the following procedure: First, given an input $x_0 \in \{0,1\}^n$, divide it into $n/2$-bit strings x_{0L} and x_{0R}. Second, iteratively update n-bit states as

$$(x_{(i-1)L}, x_{(i-1)R}) \mapsto (x_{iL}, x_{iR}) := (x_{(i-1)R} \oplus f_{i,k_i}(x_{(i-1)L}), x_{(i-1)L}) \tag{4.1}$$

for $1 \leq i \leq r$. Finally, return the final state $x_r := x_{rL} \| x_{rR}$ as the output.

The resulting function $\mathsf{LR}_r(f_{1,k_1}, \ldots, f_{r,k_r}) : x_0 \mapsto x_r$ becomes an n-bit permutation owing to the property of the Feistel network. Each f_{i,k_i} is called the i-th round function. When we say that an adversary is given oracle access to $\mathsf{LR}_r(f_1, \ldots, f_r)$, we consider the situation in which keys $k_1, \ldots, k_r$ are first chosen independently and uniformly at random, and then the adversary runs relative to the stateless oracle $O_{\mathsf{LR}_r(f_{1,k_1},\ldots,f_{r,k_r})} : |x\rangle|y\rangle \mapsto |x\rangle|y \oplus \mathsf{LR}_r(f_{1,k_1}, \ldots, f_{r,k_r})(x)\rangle$. When each round function is chosen from $\mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$ uniformly at random (i.e., each f_i is the set of all functions $\mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$ for all i), we use the notation LR_r for short.

The goal of this chapter is to show Theorem 1 and Theorem 2, which are restated below.

Theorem 7 (Lower bound and upper bound, informal (Restatement of Theorem 1))**.** *If $f_1, \ldots, f_4$ are truly random functions, then the following claims hold.*

1. LR_4 *cannot be distinguished from a truly random permutation by qCPAs up to $O(2^{n/6})$ quantum queries.*
2. *A quantum algorithm exists that distinguishes LR_4 from a truly random permutation with a constant probability by making $O(2^{n/6})$ quantum chosen-plaintext queries.*

Theorem 8 (Construction of qPRP from qPRF, informal (Restatement of Theorem 2))**.** *Suppose that each f_i is a secure PRF against efficient quantum query attacks, for $1 \leq i \leq 4$. Then $\mathsf{LR}_4(f_1, f_2, f_3, f_4)$ is a secure PRP against efficient qCPAs.*

The current chapter is organized as follows. Section 4.1 provides an informal technical overview. Section 4.2 gives formal security proofs. Section 4.3 shows the matching upper bound.

4.1 Technical Overview

It is straightforward to show that Theorem 8 follows from the second claim of Theorem 7. In addition, the second claim of Theorem 7 can be achieved by a simple quantum polynomial speed-up of existing classical attacks. In what follows, we present a rough overview on how we show the first claim of Theorem 7.

We assume that all round functions in the Luby-Rackoff constructions are truly random functions, and we focus on the number of queries when we consider computational resources of adversaries.

To have a good intuition on our proof in the quantum setting, it would be better to intuitively capture how LR_3 is proven to be secure against classical CPAs, how the quantum attack on LR_3 works, and what problem will be hard even for quantum adversaries. Thus, we first give some observations about these questions, and then provide a high-level overview on the quantum security proof of LR_4.

4.1.1 An Overview of a Classical Security Proof for LR_3.

Here we give an overview of a *classical* proof for the security of LR_3 against chosen plaintext attacks in the classical setting. For simplicity, we consider a proof for PRF security of LR_3.

Let bad_2 be the event that an adversary makes two distinct plaintext queries $(x_{0L}, x_{0R}) \neq (x'_{0L}, x'_{0R})$ to the real oracle LR_3 such that the corresponding inputs x_{1L} and x'_{1L} to the second round function f_2 are equal, i.e., inputs to f_2 collide. In addition, let bad_3 be the event that inputs to f_3 collide, and define $\mathsf{bad} := \mathsf{bad}_2 \vee \mathsf{bad}_3$.

If bad_2 (resp., bad_3) does not occur, then the right-half (resp., left-half) $n/2$ bits of LR_3's outputs cannot be distinguished from truly random $n/2$-bit strings. Thus, unless the event bad occurs, adversaries cannot distinguish LR_3 from random functions.

If the number of queries of an adversary $\mathcal{A}$ is at most q, we can show that the probability that the event bad occurs when $\mathcal{A}$ runs relative to the oracle LR_3 is in $O(q^2/2^{n/2})$. Thus we can deduce that LR_3 is indistinguishable from a random function up to $O(2^{n/4})$ queries.

4.1.2 Quantum Chosen Plaintext Attack on LR_3.

Next, we give an overview of the quantum chosen plaintext attack on LR_3 by Kuwakado and Morii [KM10]. Note that we consider the setting in which adversaries can make quantum queries. The attack distinguishes LR_3 from a random permutation with only $O(n)$ queries.

Fix $\alpha_0 \neq \alpha_1 \in \{0,1\}^{n/2}$ and for $i = 0, 1$, define $g_i : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ by $g_i(x) = (\mathsf{LR}_3(\alpha_i, x))_R \oplus \alpha_i$, where $(\mathsf{LR}_3(\alpha_i, x))_R$ denote the right half $n/2$-bits of $\mathsf{LR}_3(\alpha_i, x)$. In addition, define $G : \{0,1\} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ by $G(b, x) = g_b(x)$. Then, $g_0(x) = g_1(x \oplus s)$ can be easily confirmed to hold for any $x \in \{0,1\}^{n/2}$, where $s = f_1(\alpha_0) \oplus f_1(\alpha_1)$. Thus $G(b, x) = G((b, x) \oplus (1, s))$ holds for any b and x, i.e., the function G has the period $(1, s)$.

If we can make quantum queries to G, then we can find the period $(1, s)$ by using Simon's period finding algorithm [Sim94, Sim97], making $O(n)$ queries to G. In fact G can be implemented on an oracle-aided quantum circuit C^{LR_3} by making $O(1)$ queries to LR_3.[1]

Roughly speaking, Simon's algorithm outputs the periods with a high probability by making $O(n)$ queries if applied to periodic functions, and outputs the result that "this function is not periodic" if applied to functions without periods.

If we are given the oracle of a random permutation RP, the circuit C^{RP} will implement an almost random function, which does not have any period with a high probability. Thus, if we run Simon's algorithm on C^{RP}, with a high probability, it does not output any period. Therefore, we can distinguish LR_3 from RP by checking if Simon's period finding algorithm outputs a period.

4.1.3 Observation: Why the Classical Proof Does not Work?

Here we give an observation about why quantum adversaries can distinguish LR_3 from random permutations even though LR_3 is proven to be indistinguishable from a random permutation in the classical setting.

We observe that quantum adversaries can make the event bad_2 occur: Once we find the period $1\|s = 1\|f_1(\alpha_0) \oplus f_2(\alpha_1)$ given the real oracle LR_3, we can force collisions on the input of f_2. Concretely, take $x \in \{0,1\}^{n/2}$ arbitrarily and set $(x_{0L}, x_{0R}) := (\alpha_0, x)$, $(x'_{0L}, x'_{0R}) := (\alpha_1, x \oplus s)$. Then the corresponding inputs to f_2 become $f_1(\alpha_0) \oplus x$ for both plaintexts. Thus the classical proof idea does not work in the quantum setting.

[1] Here we have to truncate outputs of O without destroying quantum states, which is pointed out to be non-trivial in the quantum setting [KLLN16a]. However, this "truncation" issue can be overcome by using a technique described in [HS18].

4.1.4 Quantum Security Proof for LR_4: The Basic Strategy

As we explained above, the essence of the quantum attack on LR_3 is finding collisions for inputs to the second round function f_2. On the other hand, finding collisions for inputs to the third round function f_3 seems difficult even for quantum (chosen-plaintext) query adversaries. This implies that the left part of the output of LR_3, which is $x_{3L} = x_{2R} \oplus f_3(x_{2L})$, always looks completely random for adversaries. (Recall that x_{iL} and x_{iR} denote the left-half and right-half $n/2$ bits of the internal state after the i-th round, respectively.)

Having these observations, our idea is that even quantum adversaries would have difficulty in noticing that the third state update $(x_{2L}, x_{2R}) \mapsto (x_{2R} \oplus f_3(x_{2L}), x_{2L})$ of LR_3 is modified as $(x_{2L}, x_{2R}) \mapsto (F(x_{2L}, x_{2R}), x_{2L})$, where $F : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ is a random function. We denote this modified function by LR'_3 (see Fig. 4.1) and will show that it is hard to distinguish LR'_3 from LR_3.

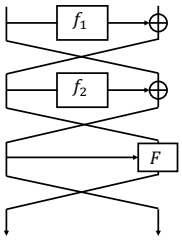


Figure 4.1: LR'_3

Next, let LR''_2 denote a modified version of the 2-round Luby-Rackoff construction such that the first and second state update operations are modified as $(x_{0L}, x_{0R}) \mapsto (F_1(x_{0L}, x_{0R}), x_{0L})$ and $(x_{1L}, x_{1R}) \mapsto (F_2(x_{1L}, x_{1R}), x_{1L})$, respectively, where $F_1, F_2 : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ are independent random functions (see Fig. 4.2). Then, we intuitively see that LR''_2 is hard to distinguish from a random function RF from $\{0,1\}^n$ to $\{0,1\}^n$.

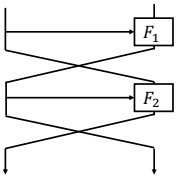


Figure 4.2: LR''_2

Once we show the above two properties, i.e.,

1. LR'_3 is hard to distinguish from LR_3, and
2. LR''_2 is hard to distinguish from RF,

we can prove Theorem 8 with simple and easy arguments: Define functions LR''_4 and LR'''_4 as in Fig. 4.3. Then, by applying the first property twice we can show that LR_4 and LR''_4 are indistinguishable. In addition, LR''_4 and LR'''_4 are indistinguishable from the second property. Since the distribution of the function LR'''_4 is equal to that of a random function, indistinguishability of LR_4 and a random function follows.

In other words, those two properties are technically the most difficult parts to show in our proof for Theorem 8.

4.1.5 Adversary and Oracle's States

We show the two properties by heavily using (our alternative formalization of) the compressed oracle technique. See Chapter 3 for the details of the compressed oracle technique.

As in Chapter 2, We assume that an oracle-aided quantum algorithm $\mathcal{A}$ has three quantum registers and its state is described as a superposition

$$\sum_{x,y,z} \alpha_{x,y,z} \left|x, y, z\right\rangle .$$

$|x\rangle$ and $|y\rangle$ corresponds to the registers to send queries to the oracle and receive the answers, respectively, and $|z\rangle$ corresponds to the register for $\mathcal{A}$'s offline computation. Recall that the quantum oracle of a (fixed) function f is modeled by the unitary operator $O_f : |x\rangle |y\rangle \mapsto |x\rangle |y \oplus f(x)\rangle$.

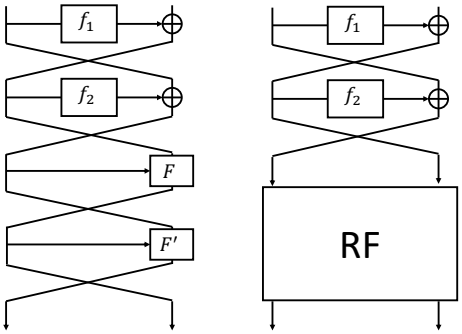


Figure 4.3: The functions LR_4'' (illustrated on the left side) and LR_4''' (illustrated on the right side). $F, F' : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ and $\mathsf{RF} : \{0,1\}^n \to \{0,1\}^n$ are independent random functions.

When $\mathcal{A}$ runs relative to the quantum oracle of a random function, we can use the compressed oracle technique. Recall that the compressed oracle maintains a state called *database*, which corresponds to the record of queries and answers in the classical lazy sampling. Before making any queries, the database is empty. When $\mathcal{A}$ queries a value x and x is not found in the database (i.e., x has not been queried before), the oracle makes the uniform superposition $\sum_y |y\rangle$, responds with y, and adds the data (x, y) into the database. (Making the uniform superposition corresponds sampling y uniformly at random in the classical lazy sampling.) When $\mathcal{A}$ queries a value x and a pair (x, y) is found in the database (i.e., x has been queried before and the previous answer was y), the oracle responds with y. The entire state of $\mathcal{A}$ and the oracle is described as

$$\sum_{x,y,z,D} \alpha_{x,y,z,D} |x, y, z\rangle \otimes |D\rangle,$$

where each D is a database that keeps some pairs $(x_1, y_1), \ldots, (x_i, y_i)$.

Remark 10. *The compressed oracle technique looks close to the classical lazy sampling. However, there is actually a large difference between them. In the compressed oracle technique, records in a database are sometimes removed or overwritten when $\mathcal{A}$ makes queries, unlike the classical lazy sampling. If the oracle does not remove the records in databases appropriately, the quantum state may be perturbed and $\mathcal{A}$ may notice that the oracle is recording queries and answers. We do not explain the details on when records are deleted in this section, but this difference is crucial for recording queries in the quantum setting.*

4.1.6 How to Prove the Two Properties

Next, we explain how we show the first property, i.e., the indistinguishability of RF_3 and RF_3'. Since RF_3 (resp., RF_3') depends on three random functions f_1, f_2, and f_3 (resp., f_1, f_2, and F), the oracle keeps three databases D_1, D_2, and D_3 (resp., D_1, D_2, and D_F). As we mentioned before, we expect that the two oracles are indistinguishable unless a collision occurs for inputs to f_3. We define that a database (D_1, D_2, D_3) for RF_3 is "bad" when the database contains the information that there is a collision for inputs to f_3. Similarly, we define that a database (D_1, D_2, D_F) for RF_3' is "bad" when the database contains the information that there is a collisions at left-half inputs to F. We define a database is "good" if it is not bad.

Let $|\psi_j\rangle$ (resp., $|\psi_j'\rangle$) be the entire state of $\mathcal{A}$ and the oracle LR_3 (resp., LR_3') just before the j-th query. Then, roughly speaking, $|\psi_j\rangle$ can be decomposed as $|\psi_j\rangle = |\psi_j^{\mathsf{good}}\rangle + |\psi_j^{\mathsf{bad}}\rangle$, where $|\psi_j^{\mathsf{good}}\rangle$ contains good databases and $|\psi_j^{\mathsf{bad}}\rangle$ contains (mainly) bad databases. $|\psi_j'\rangle$ can be decomposed in the same way.

Roughly speaking, we have the following observations:

(a) There is a natural one-to-one correspondence between the good databases for LR_3 and those for LR_3'. More precisely, for a good database (D_1, D_2, D_3) for LR_3, there exists D_F such that (D_1, D_2, D_F) is a good database for LR_3', which we denote by $[(D_1, D_2, D_3)]_F$. Similarly, for a good database (D_1, D_2, D_F) for LR_3', there exists D_3 such that (D_1, D_2, D_3) is a good database for LR_3.

(b) The behavior of the oracle LR_3 on a good database (D_1, D_2, D_3) is the same as that of LR_3' on $[(D_1, D_2, D_3)]_F$ unless they change to bad.

(c) The chance that a good database change to bad is very small.

Intuitively, (a) and (b) guarantee that $|\psi_j^{\mathsf{good}}\rangle$ and $|\psi_j'^{\mathsf{good}}\rangle$ are always the same for each j when we ignore the state of databases, which implies that $\mathcal{A}$ cannot distinguish LR_3 and LR_3' as long as databases are good. In addition, (c) shows that the "bad" components $\| |\psi_j^{\mathsf{bad}}\rangle \|$ and $\| |\psi_j'^{\mathsf{bad}}\rangle \|$ are always small, which implies that LR_3 and LR_3' are indeed indistinguishable.

For the indistinguishability of LR_2'' and RF are shown in the similar way except that we define "bad" databases as, roughly speaking, the ones that contain "collisions at left-half inputs to F_2".

Our proof is much more complex than the classical one, though, we give rigorous and careful analyses.

Remark 11. *If we try to show the quantum security of the* 3-round *Luby-Rackoff construction with similar ideas (e.g., try to show that quantum adversaries cannot notice when we replace the second and third round of* LR_3 *with* LR_2''*), we will be able to show that adversaries cannot distinguish as long as databases are good, but will not be able to prove the claim that the chance that good databases change to bad is small.*

The next section provides formal security proofs based on the intuition explained above.

4.2 Security Proofs

The goal of this section is to show the following theorem, which gives the quantum query lower bound for the problem of distinguishing the 4-round Luby-Rackoff construction LR_4 from a random permutation RP, when all round functions are truly random functions. This theorem is the formal version of the first half of Theorem 7.

Theorem 9. $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathsf{LR}_4}(q)$ *is in* $O\left(\sqrt{q^3/2^{n/2}}\right)$.

Before showing the theorem, we prove the following corollary, which is the formal version of Theorem 8.

Corollary 2. *Let* f_i *be a quantumly secure PRF for each* $1 \le i \le 4$*. Then, the* 4*-round Luby-Rackoff construction* $\mathsf{LR}_4(f_1, f_2, f_3, f_4)$ *is a quantumly secure PRP.*

Proof. Let $\mathsf{RF}_1, \ldots, \mathsf{RF}_4$ be independent random functions from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$. For $i = 0, \ldots, 4$, let $G_i := \mathsf{LR}_4\left(g_1^{(i)}, g_2^{(i)}, g_3^{(i)}, g_4^{(i)}\right)$, where $g_j^{(i)} = f_j$ if $j > i$ and $g_j^{(i)} = \mathsf{RF}_j$ if $j \le i$. Then $G_0 = \mathsf{LR}_4(f_1, f_2, f_3, f_4)$ and $G_4 = \mathsf{LR}_4$ hold.

For each $1 \le i \le 4$ and any efficient adversary $\mathcal{A}$, we can construct an efficient adversary $\mathcal{B}_i$ such that $\mathbf{Adv}^{\mathrm{dist}}_{G_{i-1},G_i}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{qPRF}}_{f_i}(\mathcal{B}_i)$. Below, we explain how we construct $\mathcal{B}_i$ when $i = 2$. Suppose that $\mathcal{B}_2$ is given an oracle $\tilde{g}$, which is either f_2 or RF_2. First, $\mathcal{B}_2$ runs $\mathcal{A}$. $\mathcal{B}_2$ simulates the oracle of $\tilde{G} := \mathsf{LR}_4(\mathsf{RF}_1, \tilde{g}, f_3, f_4)$ by simulating RF_1, f_3, and f_4 by itself and making queries to $\tilde{g}$. When $\mathcal{A}$ makes queries, $\mathcal{B}_2$ responds with $\tilde{G}$. Finally, $\mathcal{B}_2$ returns $\mathcal{A}$'s final output as its own output. Because truly random functions can be efficiently simulated against efficient quantum adversaries [Zha12b], we can make $\mathcal{B}_2$ efficient. We have $\mathbf{Adv}^{\mathrm{dist}}_{G_1,G_2}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{qPRF}}_{f_2}(\mathcal{B}_2)$ because $\tilde{G} = G_1$ if $\tilde{g} = f_2$, and $\tilde{G} = G_2$ if $\tilde{g} = \mathsf{RF}_2$. $\mathcal{B}_i$ for other i can be constructed in the same way[2].

Now we have

$$\begin{aligned}\mathbf{Adv}^{\mathrm{qPRP}}_{\mathsf{LR}_4(f_1,f_2,f_3,f_4)}(\mathcal{A}) &\le \sum_{1\le i\le 4} \mathbf{Adv}^{\mathrm{dist}}_{G_{i-1},G_i}(\mathcal{A}) + \mathbf{Adv}^{\mathrm{qPRP}}_{\mathsf{LR}_4}(\mathcal{A}) \\ &= \sum_{1\le i\le 4} \mathbf{Adv}^{\mathrm{qPRF}}_{f_i}(\mathcal{B}_i) + \mathbf{Adv}^{\mathrm{qPRP}}_{\mathsf{LR}_4}(\mathcal{A}).\end{aligned}$$

The first term of the right hand side of the above inequality is negligible since f_i is a quantumly secure PRF for each i. The second term is also negligible by Theorem 9. Hence the corollary follows. □

In the rest of this section, we assume that all round functions in the Luby-Rackoff constructions are truly random functions, and we focus on the number of queries when we consider computational resources of adversaries.

As we explained in Section 4.1, technically the most hardest parts to show the quantum security of LR_4 is to show the indistinguishability of LR_3 and LR_3', and the indistinguishability of LR_2'' and a random function.

Recall that LR_3' is defined in the same way as LR_3 except that the third state update $(x_{2L}, x_{2R}) \mapsto (x_{2R} \oplus f_3(x_{2L}), x_{2L})$ of LR_3 is modified as $(x_{2L}, x_{2R}) \mapsto (F(x_{2L}, x_{2R}), x_{2L})$, where $F : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ is a random function. LR_2'' denote a modified version of the 2-round Luby-Rackoff construction such that the first and second state update operations are modified as $(x_{0L}, x_{0R}) \mapsto (F_1(x_{0L}, x_{0R}), x_{0L})$ and $(x_{1L}, x_{1R}) \mapsto (F_2(x_{1L}, x_{1R}), x_{1L})$, respectively, where $F_1, F_2 : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ are independent random functions.

[2]When $i = 1$, we do not need efficient simulation of a random function.

4.2.0.1 Organization of the Rest of Section 4.2

Section 4.2.1 shows that LR_3' is hard to distinguish from LR_3. Section 4.2.2 shows that LR_2'' is hard to distinguish from RF. Section 4.2.3 proves Theorem 9 by combining the results in Section 4.2.1 and Section 4.2.2.

4.2.1 Hardness of Distinguishing LR_3' from LR_3

Here we show the following proposition.

Proposition 5. $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_3,\mathsf{LR}_3'}(q)$ *is in* $O\left(\sqrt{q^3/2^{n/2}}\right)$.

First, let us discuss the behavior of the quantum oracles of LR_3 and LR_3'. Let $\mathcal{A}$ be an adversary that makes at most q quantum queries.

4.2.1.1 Quantum Oracle of LR_3

Let us define the unitary operator $O_{\mathrm{UP}.i}$ that computes the state update of the i-th round by

$$O_{\mathrm{UP}.i} : |x_{(i-1)L}, x_{(i-1)R}\rangle\,|y_L, y_R\rangle \mapsto |x_{(i-1)L}, x_{(i-1)R}\rangle\,|(y_L, y_R) \oplus (f_i(x_{(i-1)L}) \oplus x_{(i-1)R}, x_{(i-1)L})\rangle\,.$$

$O_{\mathrm{UP}.i}$ can be implemented by making one query to f_i (see Fig. 4.4).

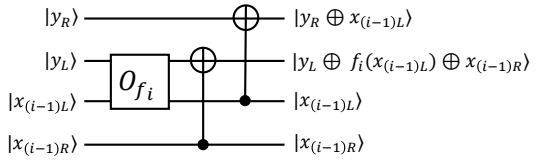


Figure 4.4: Implementation of $O_{\mathrm{UP}.i}$. In the security proof, O_{f_i} is replaced with the recording standard oracle with errors for f_i.

Now O_{LR_3} can be implemented as follows by using $\{O_{\mathrm{UP}.i}\}_{1\le i\le 3}$:

1. Take $|x\rangle\,|y\rangle = |x_{0L}, x_{0R}\rangle\,|y_L, y_R\rangle$ as an input.
2. Compute the state (x_{1L}, x_{1R}) by querying $|x_{0L}, x_{0R}\rangle\,|0^n\rangle$ to $O_{\mathrm{Up}.1}$, and obtain
$$|x_{0L}, x_{0R}\rangle\,|y_L, y_R\rangle \otimes |x_{1L}, x_{1R}\rangle\,. \tag{4.2}$$
3. Compute the state (x_{2L}, x_{2R}) by querying $|x_{1L}, x_{1R}\rangle\,|0^n\rangle$ to $O_{\mathrm{Up}.2}$, and obtain
$$|x_{0L}, x_{0R}\rangle\,|y_L, y_R\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle\,. \tag{4.3}$$
4. Query $|x_{2L}, x_{2R}\rangle\,|y_L, y_R\rangle$ to $O_{\mathrm{Up}.3}$, and obtain
$$|x\rangle\,|y \oplus \mathsf{LR}_3(x)\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle\,. \tag{4.4}$$
5. Uncompute Steps 2 and 3 to obtain
$$|x\rangle\,|y \oplus \mathsf{LR}_3(x)\rangle\,. \tag{4.5}$$
6. Return $|x\rangle\,|y \oplus \mathsf{LR}_3(x)\rangle$.

The above implementation is illustrated in Fig. 4.5.

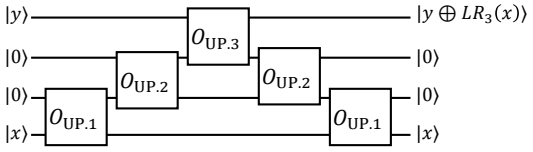


Figure 4.5: Implementation of LR_3.

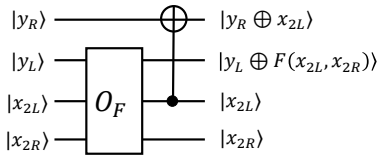


Figure 4.6: Implementation of $O'_{\mathrm{UP}.3}$. In the security proof, O_F is replaced with the recording standard oracle with errors for F.

4.2.1.2 Quantum Oracle of LR'_3

The quantum oracle of LR'_3 is implemented in the same way as LR_3, except that the third round state update oracle $O_{\mathrm{UP}.3}$ is replaced with another oracle $O'_{\mathrm{UP}.3}$ defined as

$$O'_{\mathrm{UP}.3} : |x_{2L}, x_{2R}\rangle\,|y_L, y_R\rangle \mapsto |x_{2L}, x_{2R}\rangle\,|(y_L, y_R) \oplus (F(x_{2L}, x_{2R}), x_{2L})\rangle\,.$$

$O'_{\mathrm{UP}.3}$ is implemented by making one query to O_F, i.e., the quantum oracle of F (see Fig. 4.6).

In what follows, we assume that the oracles of the functions f_i and F are implemented as the recording standard oracle with errors, and we use D_1, D_2, D_3, and D_F to denote (valid) databases for f_1, f_2, f_3, and F, respectively. In particular, after the i-th query of an adversary to LR_3, the joint quantum states of the adversary and functions can be described as

$$\sum_{x,y,z,D_1,D_2,D_3} a_{x,y,z,D_1,D_2,D_3}\,|x, y, z\rangle \otimes |D_1\rangle\,|D_2\rangle\,|D_3\rangle \tag{4.6}$$

for some complex numbers a_{x,y,z,D_1,D_2,D_3} such that $\sum_{x,y,z,D_1,D_2,D_3} |a_{x,y,z,D_1,D_2,D_3}|^2 = 1$. Here, x, y, and z correspond to the adversary's register to send queries to oracles, receive answers from oracles, and perform offline computations, respectively. (If the oracle is LR'_3, then the register $|D_3\rangle$, which corresponds to f_3, is replaced with $|D_F\rangle$, which corresponds to F.)

Next, we define good and bad databases for LR_3 and LR'_3. Intuitively, we say that a tuple (D_1, D_2, D_3) (resp., (D_1, D_2, D_F)) for LR_3 (resp., LR'_3) is bad if and only if it contains the information that some inputs to f_3 (resp., the left halves of some inputs to F) collide. Roughly speaking, we define good and bad databases in such a way that a one-to-one correspondence exists between good databases for LR_3 and those for LR'_3, so that adversaries will not be able to distinguish LR'_3 from LR_3 as long as databases are good.

4.2.1.3 Good and Bad Databases for LR_3

Here we introduce the notion of *good* and *bad* for each tuple (D_1, D_2, D_3) of valid database for LR_3. We say that (D_1, D_2, D_3) is good if, for each entry $(x_{2L}, \gamma) \in D_3$, there exists exactly one pair $((x_{0L}, \alpha), (x_{1L}, \beta)) \in D_1 \times D_2$ such that $\beta \oplus x_{0L} = x_{2L}$. We say that (D_1, D_2, D_3) is bad if it is not good.

4.2.1.4 Good and Bad Databases for LR'_3

Next we introduce the notion of *good* and *bad* for each tuple (D_1, D_2, D_F) of valid database for LR'_3. We say that a valid database D_F is *without overlap* if each pair of distinct entries (x_{2L}, x_{2R}, γ) and $(x'_{2L}, x'_{2R}, \gamma')$ in D_F satisfies $x_{2L} \neq x'_{2L}$. We say that (D_1, D_2, D_F) is good if D_F is without overlap, and for each entry $(x_{2L}, x_{2R}, \gamma) \in D_F$, there exists exactly one pair $((x_{0L}, \alpha), (x_{1L}, \beta)) \in D_1 \times D_2$ such that $\beta \oplus x_{0L} = x_{2L}$ and $x_{2R} = x_{1L}$. We say that (D_1, D_2, D_F) is bad if it is not good.

4.2.1.5 Compatibility of D_F with D_3

For a valid database D_F for F without overlap, let $[D_F]_3$ be the valid database for f_3 such that $(x_{2L}, x_{2R}, \gamma) \in D_F$ if and only if $(x_{2L}, x_{2R} \oplus \gamma) \in [D_F]_3$. We say that a valid database D_3 for f_3 is compatible with D_F if $D_3 = [D_F]_3$.

Remark 12. *For each good database (D_1, D_2, D_3) for LR_3, a unique D_F without overlap exists such that $[D_F]_3 = D_3$ and (D_1, D_2, D_F) is a good database for LR'_3, by the definition of good databases. Similarly, for each good database (D_1, D_2, D_F) for LR'_3, $(D_1, D_2, [D_F]_3)$ becomes a good database for LR_3. That is, there exists a one-to-one correspondence between good databases for LR_3 and those for LR'_3.*

Here we prove the following lemma for later use, which shows that the behavior of $O'_{\mathrm{UP}.3}$ for D_F without overlap is the same as that of $O_{\mathrm{UP}.3}$ for $[D_F]_3$.

Lemma 1. *It holds that*

$$\begin{aligned}&\langle x'_{2L}, x'_{2R}, y'_L, y'_R| \otimes \langle D'_F|\, O'_{\mathrm{UP}.3}\, |x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |D_F\rangle \\ &= \langle x'_{2L}, x'_{2R}, y'_L, y'_R| \otimes \langle [D'_F]_3|\, O_{\mathrm{UP}.3}\, |x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |[D_F]_3\rangle \end{aligned} \tag{4.7}$$

for any $x_{2L}, x_{2R}, y_L, y_R, x'_{2L}, x'_{2R}, y'_L, y'_R \in \{0,1\}^{n/2}$ and any valid databases D_F and D'_F without overlap.

Proof. It suffices to consider the case that $x'_{2L} = x_{2L}$, $x'_{2R} = x_{2R}$, and $y'_R = y_R$ because the both sides of (4.7) become zero if these three equations do not hold. Since the database $O'_{\mathrm{UP}.3}$ affects only the entry of (x_{2L}, x_{2R}) in D_F when it acts on $|x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |D_F\rangle$, it suffices to show the claim for the cases that (1) D_F has only a single entry (x_{2L}, x_{2R}, α), or (2) D_F has no entry (i.e., $D_F = \emptyset$).

First, we show the claim for the first case where $D_F = \{(x_{2L}, x_{2R}, \alpha)\}$. In this case, by the first property of Proposition 3 we have that

$$\begin{aligned} O'_{\mathrm{UP}.3}\, |x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |D_F\rangle &= |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, x_{2R}, \alpha)\rangle \\ &+ \frac{1}{\sqrt{2^{n/2}}}\, |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left(|\emptyset\rangle - \left(\sum_\gamma \frac{1}{\sqrt{2^{n/2}}}\, |(x_{2L}, x_{2R}, \gamma)\rangle \right) \right) \\ &- \frac{1}{\sqrt{2^{n/2}}} \sum_\gamma \frac{1}{\sqrt{2^{n/2}}}\, |x_{2L}, x_{2R}, y_L \oplus \gamma, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, x_{2R}, \gamma)\rangle \\ &+ \frac{1}{2^{n/2}}\, |x_{2L}, x_{2R}\rangle\, |\widehat{0^n}\rangle\, |y_R \oplus x_{2L}\rangle \otimes \left(2 \sum_\delta \frac{1}{\sqrt{2^{n/2}}}\, |(x_{2L}, x_{2R}, \delta)\rangle - |\emptyset\rangle \right) \\ &+ |\mathsf{invalid}\rangle \end{aligned} \tag{4.8}$$

holds, where $\emptyset$ is the empty database and $|\mathsf{invalid}\rangle$ is a vector containing invalid databases. In addition, we have that $[D_F]_3 = \{(x_{2L}, \alpha \oplus x_{2R})\}$, and

$$\begin{aligned} O_{\mathrm{UP}.3}\, |x_{2L}, x_{2R}, y_L, y_R\rangle \otimes |[D_F]_3\rangle &= |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, \alpha \oplus x_{2R})\rangle \\ &+ \frac{1}{\sqrt{2^{n/2}}}\, |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left(|\emptyset\rangle - \left(\sum_\gamma \frac{1}{\sqrt{2^{n/2}}}\, |(x_{2L}, \gamma)\rangle \right) \right) \\ &- \frac{1}{\sqrt{2^{n/2}}} \sum_\gamma \frac{1}{\sqrt{2^{n/2}}}\, |x_{2L}, x_{2R}, y_L \oplus \gamma \oplus x_{2R}, y_R \oplus x_{2L}\rangle \otimes |(x_{2L}, \gamma)\rangle \\ &+ \frac{1}{2^{n/2}}\, |x_{2L}, x_{2R}\rangle\, |\widehat{0^n}\rangle\, |y_R \oplus x_{2L}\rangle \otimes \left(2 \sum_\delta \frac{1}{\sqrt{2^{n/2}}}\, |(x_{2L}, \delta)\rangle - |\emptyset\rangle \right) \\ &+ |\mathsf{invalid}'\rangle \end{aligned}$$

$$
\begin{aligned}
&= |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \alpha)]_3\rangle \\
&\quad + \frac{1}{\sqrt{2^{n/2}}} |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left(|\emptyset\rangle - \left(\sum_\gamma \frac{1}{\sqrt{2^{n/2}}} |[(x_{2L}, x_{2R}, \gamma \oplus x_{2R})]_3\rangle \right) \right) \\
&\quad - \frac{1}{\sqrt{2^{n/2}}} \sum_\gamma \frac{1}{\sqrt{2^n}} |x_{2L}, x_{2R}, y_L \oplus \gamma \oplus x_{2R}, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \gamma \oplus x_{2R})]_3\rangle \\
&\quad + \frac{1}{2^{n/2}} |x_{2L}, x_{2R}\rangle |\widehat{0^n}\rangle |y_R \oplus x_{2L}\rangle \otimes \left(2 \sum_\delta \frac{1}{\sqrt{2^{n/2}}} |[(x_{2L}, x_{2R}, \delta \oplus x_{2R})]\rangle - |\emptyset\rangle \right) \\
&\quad + |\mathsf{invalid}'\rangle \\
&= |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \alpha)]_3\rangle \\
&+ \frac{1}{\sqrt{2^{n/2}}} |x_{2L}, x_{2R}, y_L \oplus \alpha, y_R \oplus x_{2L}\rangle \left(|\emptyset\rangle - \left(\sum_\gamma \frac{1}{\sqrt{2^{n/2}}} |[(x_{2L}, x_{2R}, \gamma)]_3\rangle \right) \right) \\
&- \frac{1}{\sqrt{2^{n/2}}} \sum_\gamma \frac{1}{\sqrt{2^{n/2}}} |x_{2L}, x_{2R}, y_L \oplus \gamma, y_R \oplus x_{2L}\rangle \otimes |[(x_{2L}, x_{2R}, \gamma)]_3\rangle \\
&\quad + \frac{1}{2^{n/2}} |x_{2L}, x_{2R}\rangle |\widehat{0^n}\rangle |y_R \oplus x_{2L}\rangle \otimes \left(2 \sum_\delta \frac{1}{\sqrt{2^{n/2}}} |[(x_{2L}, x_{2R}, \delta)]_3\rangle - |\emptyset\rangle \right) \\
&+ |\mathsf{invalid}'\rangle, \qquad (4.9)
\end{aligned}
$$

where $|\mathsf{invalid}'\rangle$ is a vector containing invalid databases. From (4.8) and (4.9), the claim immediately follows for the first case that $D_F = \{(x_{2L}, x_{2R}, \alpha)\}$.

We can similarly show that the claim holds for the second case where D_F is empty by straightforward calculations using the second property of Proposition 3. □

4.2.1.6 Technical Core to Prove the Indistinguishability of LR_3 and LR'_3

Let $|\psi_i\rangle$ and $|\psi'_i\rangle$ be the joint quantum states of the adversary $\mathcal{A}$ and the oracle just before making the i-th query when $\mathcal{A}$ runs relative to LR_3 and LR'_3, respectively. In addition, by $|\psi_{q+1}\rangle$ and $|\psi'_{q+1}\rangle$ we similarly denote the states just before the final measurement, by abuse of notation. Then

$$
|\psi_j\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_3 \\ (D_1,D_2,D_3)\,:\,\text{valid database}}} c_{x,y,z,D_1,D_2,D_3} |x, y, z\rangle \otimes |D_1\rangle |D_2\rangle |D_3\rangle
$$

holds for some complex number c_{x,y,z,D_1,D_2,D_3} such that

$$
\sum_{\substack{x,y,z,D_1,D_2,D_3 \\ (D_1,D_2,D_3)\,:\,\text{valid database}}} |c_{x,y,z,D_1,D_2,D_3}|^2 = 1.
$$

Here, $x = x_{0L} \| x_{0R}$, $y = y_L \| y_R$, and z correspond to $\mathcal{A}$'s registers to send queries, receive answers, and perform offline computations, respectively ($x_{0L}, x_{0R}, y_L, y_R \in \{0,1\}^{n/2}$). Note that $|D_1|, |D_2| \leq 2(j-1)$, and $|D_3| \leq j-1$ hold for each summand of $|\psi_j\rangle$, since each query to the recording standard oracle with errors RstOE affects only the qubits that correspond to a single entry of each database. $|\psi'_j\rangle$ can be decomposed on the computational basis in the same way.

Showing the following proposition is the technical core to prove Proposition 5.

Proposition 6. *For each $j = 1, \ldots, q+1$, there exist vectors $|\psi_j^{\mathsf{good}}\rangle$, $|\psi_j^{\mathsf{bad}}\rangle$, $|\psi_j^{'\mathsf{good}}\rangle$, $|\psi_j^{'\mathsf{bad}}\rangle$, and complex number $a^{(j)}_{x,y,z,D_1,D_2,D_F}$ such that*

$$
\begin{aligned}
|\psi_j\rangle &= |\psi_j^{\mathsf{good}}\rangle + |\psi_j^{\mathsf{bad}}\rangle, \quad |\psi'_j\rangle = |\psi_j^{'\mathsf{good}}\rangle + |\psi_j^{'\mathsf{bad}}\rangle, \\
|\psi_j^{\mathsf{good}}\rangle &= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,good}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x, y, z\rangle \otimes |D_1, D_2, [D_F]_3\rangle, \qquad (4.10) \\
|\psi_j^{'\mathsf{good}}\rangle &= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,good}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x, y, z\rangle \otimes |D_1, D_2, D_F\rangle, \qquad (4.11)
\end{aligned}
$$

the vector $|D_1, D_2, D_F\rangle$ *in* $|\psi_j^{'\mathsf{good}}\rangle$ *(resp.,* $|D_1, D_2, [D_F]_3\rangle$ *in* $|\psi_j^{\mathsf{good}}\rangle$*) has non-zero quantum amplitude only if* $|D_1| \leq 2(j-1)$*,* $|D_2| \leq 2(j-1)$*, and* $|D_F| \leq j-1$*, and*

$$\| \, |\psi_j^{\mathsf{bad}}\rangle \, \| \leq \left\| |\psi_{j-1}^{\mathsf{bad}}\rangle \right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \quad \| \, |\psi_j^{'\mathsf{bad}}\rangle \, \| \leq \left\| |\psi_{j-1}^{'\mathsf{bad}}\rangle \right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{4.12}$$

hold (we set $|\psi_0^{\mathsf{bad}}\rangle = 0$ *and* $|\psi_0^{'\mathsf{bad}}\rangle = 0$*).*

Intuition on the claim of the proposition. Intuitively, equations (4.10) and (4.11) show that the adversary $\mathcal{A}$ cannot distinguish the oracles as long as databases are good: Roughly speaking, the vectors $|\psi_j^{\mathsf{good}}\rangle$ and $|\psi_j^{'\mathsf{good}}\rangle$ are the components of $|\psi_j\rangle$ and $|\psi'_j\rangle$ with good databases. Due to (4.10) and (4.11), the coefficient of each basis vector $|x, y, z\rangle \otimes |D_1, D_2, [D_F]_3\rangle$ in $|\psi_j^{\mathsf{good}}\rangle$ is exactly equal to that of $|x, y, z\rangle \otimes |D_1, D_2, D_F\rangle$ in $|\psi_j^{'\mathsf{good}}\rangle$, where $(D_1, D_2, [D_F]_3)$ is the good database for LR_3 that corresponds to (D_1, D_2, D_3) for LR'_3. This implies that we have $\mathsf{td}\left(\mathrm{tr}_{\mathcal{D}_{123}}\left(|\psi_j^{\mathsf{good}}\rangle\langle\psi_j^{\mathsf{good}}|\right), \mathrm{tr}_{\mathcal{D}_{12F}}\left(|\psi_j^{'\mathsf{good}}\rangle\langle\psi_j^{'\mathsf{good}}|\right)\right) = 0$, which intuitively means that LR_3 and LR'_3 are indistinguishable for $\mathcal{A}$ as long as databases are good. (Here, $\mathrm{tr}_{\mathcal{D}_{123}}$ and $\mathrm{tr}_{\mathcal{D}_{12F}}$ denote the partial trace operations over the databases for LR_3 and LR'_3, respectively.)

Equation (4.12) shows that, at each query, the chance that good databases change to bad is exponentially small. This means that the trace distance $\mathsf{td}\left(\mathrm{tr}_{\mathcal{D}_{123}}\left(|\psi_{q+1}\rangle\langle\psi_{q+1}|\right), \mathrm{tr}_{\mathcal{D}_{12F}}\left(|\psi'_{q+1}\rangle\langle\psi'_{q+1}|\right)\right)$, which is an upper bound of $\mathcal{A}$'s distinguishing advantage, is quite close to $\mathsf{td}\left(\mathrm{tr}_{\mathcal{D}_{123}}\left(|\psi_{q+1}^{\mathsf{good}}\rangle\langle\psi_{q+1}^{\mathsf{good}}|\right), \mathrm{tr}_{\mathcal{D}_{12F}}\left(|\psi_{q+1}^{'\mathsf{good}}\rangle\langle\psi_{q+1}^{'\mathsf{good}}|\right)\right) = 0$.

Therefore, it suffices to prove the above proposition to show the indistinguishability of LR_3 and LR'_3.

Proof intuition for Proposition 6. Recall that a database (D_1, D_2, D_3) for LR_3 (resp., (D_1, D_2, D_F) for LR'_3) is defined to be bad if and only if inputs to D_3 collide (resp., the left halves of inputs to D_F collide). Roughly speaking, "good" and "bad" vectors correspond to the states with good and bad databases, respectively.

If we were in the classical setting, databases would correspond to transcripts, and we would define the "good" and "bad" vectors to be the (classical) states with good and bad transcripts, respectively. As long as transcripts are good, the behaviors of the oracles LR_3 and LR'_3 are the same and they are indistinguishable. Basically we can also use a similar intuition in the quantum setting for "good" states, and thus there exists complex number $a^{(j)}_{x,y,z,D_1,D_2,D_F}$ that satisfies (4.10) and (4.11).

For the inequalities (4.12) on "bad" states, when a classical adversary $\mathcal{A}$ makes the j-th query to LR_3 (resp., LR'_3), a good classical state (good transcript) changes to a bad state (bad transcript) only if a new query is made to f_1 or f_2, and the input to f_3 (resp., the left half of the input to F) collides with a previous input to f_3 (resp., the left half of a previous input to F). Such a "bad" event happens with a probability p in $O(j/2^n)$. In the quantum setting, roughly speaking, the difference between the norms of the j-th bad vector $|\psi_j^{\mathsf{bad}}\rangle$ (resp., $|\psi_j^{'\mathsf{bad}}\rangle$) and the $(j-1)$-th bad vector $|\psi_{j-1}^{\mathsf{bad}}\rangle$ (resp., $|\psi_{j-1}^{'\mathsf{bad}}\rangle$) corresponds to $\sqrt{p}$, which is in $O(\sqrt{j/2^n})$. Thus we obtain (4.12).

A very rough proof intuitions is as stated. However, to be more precise, an existing record (x, α) in a database may later be deleted or overwritten with a different record in the quantum setting, and the effect of such deletion and overwriting is too large to be ignored. Therefore, we have to perform more careful and quantum-specific analysis.

4.2.1.7 Technical Lemmas for Bounding "bad" Norms

Before describing the formal proof of Proposition 6, we provide some technical lemmas to bound the norms of "bad" vectors.

Intuitively, when a value x is queried to RstOE_{f_1} (RstOE_{f_i} denotes the recording standard oracle with errors for f_i), a good database (D_1, D_2, D_3) for LR_3 changes to bad when some of the following events happen.

1. x is not recorded in D_1. A new record (x, α) is added to D_1 for some α, and $(D_1 \cup (x, \alpha), D_2, D_3)$ becomes bad.
2. There exists a record (x, α) in D_1, but it is deleted at the query, and $(D_1 \setminus (x, \alpha), D_2, D_3)$ becomes bad.
3. There exists a record (x, α) in D_1, but it is overwritten with a new record (x, γ) for some γ at the query, and $((D_1 \setminus (x, \alpha)) \cup (x, \gamma), D_2, D_3)$ becomes bad.

The events that good databases change to bad at queries to other functions can be classified similarly[3]. The same arguments also hold for LR'_3.

[3]In fact, a good database does not change to bad at queries to RstOE_{f_3} in our proof due to the definition of good databases.

Below, we show four lemmas to bound the norms of "bad" vectors that correspond to the above three events. Lemma 2 and Lemma 3 correspond to the first and second events. For the third event, we further divide it into two different cases.

(a) For each $(\tilde{D}_1, D_2, D_3)$ and α such that $\tilde{D}_1(x) = \perp$ and $(\tilde{D}_1 \cup (x, \alpha), D_2, D_3)$ is good, the number of γ such that $(\tilde{D}_1 \cup (x, \gamma), D_2, D_3)$ becomes bad is small. (Here, $\tilde{D}_1 \cup (x, \alpha)$ corresponds to D_1 in the above discussions.)

(b) For each $(\tilde{D}_1, D_2, D_3)$ and α such that $\tilde{D}_1(x) = \perp$ and $(\tilde{D}_1 \cup (x, \alpha), D_2, D_3)$ is good, $(\tilde{D}_1 \cup (x, \gamma), D_2, D_3)$ becomes bad for almost all $\gamma \neq \alpha$. However, for each $(\tilde{D}_1, D_2, D_3)$ and γ such that $\tilde{D}_1(x) = \perp$ and $(\tilde{D}_1 \cup (x, \alpha), D_2, D_3)$ is bad, the number of α such that $(\tilde{D}_1 \cup (x, \alpha), D_2, D_3)$ becomes good is small.

The cases (a) and (b) correspond to Lemma 5 and Lemma 4, respectively. We describe the lemmas in the most general way as possible so that they can be used for other future applications.

In what follows, S denotes a bit string that corresponds to a database, the adversary's state, and the oracle's state. The bit strings α and γ are in $\{0,1\}^{n/2}$. R_{good} and R_{bad} are some relations. In security proofs, R_{good} (resp., R_{bad}) will be relations such that databases are good (resp., bad) *and* some additional conditions are satisfied.

Lemma 2. *Let a_S be a complex number such that $\sum_S |a_S|^2 \leq O(1)$. Let*

$$|\phi\rangle := \sum_{\substack{S,\alpha \\ S \in R_{\mathsf{good}} \wedge (S,\alpha) \in R_{\mathsf{bad}}}} a_S \frac{1}{\sqrt{2^{n/2}}} |S\rangle |\alpha\rangle .$$

Suppose that the number of α such that $(S, \alpha) \in R_{\mathsf{bad}}$ is at most X for each $S \in R_{\mathsf{good}}$. Then

$$\| |\phi\rangle \| \leq O\left(\sqrt{\frac{X}{2^{n/2}}}\right)$$

holds.

Proof. The claim holds since

$$\| |\phi\rangle \|^2 = \sum_{\substack{S,\alpha \\ S \in R_{\mathsf{good}} \wedge (S,\alpha) \in R_{\mathsf{bad}}}} \frac{|a_S|^2}{2^{n/2}} = \sum_{S \in R_{\mathsf{good}}} |a_S|^2 \cdot \frac{|\{\alpha | (S,\alpha) \in R_{\mathsf{bad}}\}|}{2^{n/2}} \leq O\left(\frac{X}{2^n}\right).$$

□

Lemma 3. *Let $a_{S,\alpha}$ be a complex number such that $\sum_{S,\alpha} |a_{S,\alpha}|^2 \leq O(1)$. Let*

$$|\phi\rangle := \sum_{\substack{S,\alpha \\ (S,\alpha) \in R_{\mathsf{good}} \wedge S \in R_{\mathsf{bad}}}} a_{S,\alpha} \frac{1}{\sqrt{2^{n/2}}} |S\rangle .$$

If the number of α such that $(S, \alpha) \in R_{\mathsf{good}}$ is at most X for each tuple $S \in R_{\mathsf{bad}}$, then

$$\||\phi\rangle\| \leq \sqrt{\frac{X}{2^{n/2}}}$$

holds.

Proof. The claim holds since we have

$$\| |\phi\rangle \|^2 = \sum_{S \in R_{\mathsf{bad}}} \left| \frac{\sum_{\alpha:(S,\alpha) \in R_{\mathsf{good}}} a_{S,\alpha}}{\sqrt{2^n}} \right|^2 \leq \sum_{S \in R_{\mathsf{bad}}} \frac{X \cdot \sum_{\alpha:(S,\alpha) \in R_{\mathsf{good}}} |a_{S,\alpha}|^2}{2^{n/2}} = \frac{X}{2^{n/2}} \sum_{\substack{S,\alpha \\ (S,\alpha) \in R_{\mathsf{good}} \wedge S \in R_{\mathsf{bad}}}} |a_{S,\alpha}|^2 \leq O\left(\frac{X}{2^{n/2}}\right),$$

where we used the convexity of the square function for the first inequality. □

Lemma 4. *Let $a_{S,\alpha}$ be a complex number such that $\sum_{S,\alpha} |a_{S,\alpha}|^2 \leq O(1)$. Let*

$$|\phi\rangle := \sum_{\substack{S,\alpha,\gamma \\ (S,\alpha)\in R_{\mathsf{good}} \wedge (S,\gamma)\in R_{\mathsf{bad}}}} a_{S,\alpha} \frac{1}{2^{n/2}} |S\rangle |\gamma\rangle .$$

If the number of γ such that $(S,\gamma) \in R_{\mathsf{bad}}$ is at most X for each tuple $(S,\alpha) \in R_{\mathsf{good}}$, then

$$\||\phi\rangle\| \leq \sqrt{\frac{X}{2^{n/2}}}$$

holds.

Proof. The claim holds since

$$\begin{aligned} \| |\phi\rangle \|^2 &= \sum_{\substack{S,\gamma \\ (S,\gamma)\in R_{\mathsf{bad}}}} \left| \frac{\sum_{\alpha:(S,\alpha)\in R_{\mathsf{good}}} a_{S,\alpha}}{2^{n/2}} \right|^2 \leq \sum_{\substack{S,\gamma \\ (S,\gamma)\in R_{\mathsf{bad}}}} \frac{\sum_{\alpha:(S,\alpha)\in R_{\mathsf{good}}} |a_{S,\alpha}|^2}{2^{n/2}} \\ &= \sum_{(S,\alpha)\in R_{\mathsf{good}}} \frac{|a_{S,\alpha}|^2 \cdot |\{\gamma | (S,\gamma) \in R_{\mathsf{bad}}\}|}{2^{n/2}} \leq \sum_{(S,\alpha)\in R_{\mathsf{good}}} \frac{|a_{S,\alpha}|^2 \cdot X}{2^{n/2}} \leq O\left(\frac{X}{2^{n/2}}\right) \end{aligned}$$

holds. □

Lemma 5. *Let $a_{S,\alpha}$ be a complex number such that $\sum_{S,\alpha} |a_{S,\alpha}|^2 \leq O(1)$. Let*

$$|\phi\rangle := \sum_{\substack{S,\alpha,\gamma \\ (S,\alpha)\in R_{\mathsf{good}} \wedge (S,\gamma)\in R_{\mathsf{bad}}}} a_{S,\alpha} \frac{1}{2^{n/2}} |S\rangle |\gamma\rangle .$$

If the number of α such that $(S,\alpha) \in R_{\mathsf{good}}$ is at most X for each tuple $(S,\gamma) \in R_{\mathsf{bad}}$, then

$$\||\phi\rangle\| \leq O\left(\sqrt{\frac{X}{2^{n/2}}}\right)$$

holds.

Proof. The claim holds since we have

$$\begin{aligned} \| |\phi\rangle \|^2 &= \sum_{\substack{S,\gamma \\ (S,\gamma)\in R_{\mathsf{bad}}}} \left| \frac{\sum_{\alpha:(S,\alpha)\in R_{\mathsf{good}}} a_{S,\alpha}}{2^{n/2}} \right|^2 \leq \sum_{\substack{S,\gamma \\ (S,\gamma)\in R_{\mathsf{bad}}}} \frac{X \cdot \sum_{\alpha:(S,\alpha)\in R_{\mathsf{good}}} |a_{S,\alpha}|^2}{(2^{n/2})^2} \\ &= \frac{X}{2^{n/2}} \cdot \sum_{\gamma} \frac{1}{2^{n/2}} \sum_{\substack{S,\alpha \\ (S,\alpha)\in R_{\mathsf{good}} \wedge (S,\gamma)\in R_{\mathsf{bad}}}} |a_{S,\alpha}|^2 \leq \frac{X}{2^{n/2}} \cdot \sum_{\gamma} \frac{1}{2^{n/2}} \sum_{S,\alpha} |a_{S,\alpha}|^2 \\ &\leq \frac{X}{2^{n/2}} \cdot 1 \cdot O(1) \leq O\left(\frac{X}{2^{n/2}}\right), \end{aligned}$$

where we used the convexity of the square function for the first inequality. □

4.2.1.8 Proof of Proposition 6

We show the proposition by induction on j. Remember that the oracles of LR_3 and LR'_3 are decomposed as $O_{\mathsf{LR}_3} = O_{\mathrm{UP}.1} \cdot O_{\mathrm{UP}.2} \cdot O_{\mathrm{UP}.3} \cdot O_{\mathrm{UP}.2} \cdot O_{\mathrm{UP}.1}$ and $O_{\mathsf{LR}'_3} = O_{\mathrm{UP}.1} \cdot O_{\mathrm{UP}.2} \cdot O'_{\mathrm{UP}.3} \cdot O_{\mathrm{UP}.2} \cdot O_{\mathrm{UP}.1}$. We check how the quantum states change when $O_{\mathrm{UP}.1}$, $O_{\mathrm{UP}.2}$, $O_{\mathrm{UP}.3}$ (resp., $O'_{\mathrm{UP}.3}$), $O_{\mathrm{UP}.2}$, and $O_{\mathrm{UP}.1}$ act on $|\psi_j\rangle$ (resp., $|\psi'_j\rangle$) in a sequential order. The claim obviously holds for $j = 1$ by setting $|\psi_1^{\mathsf{good}}\rangle := |\psi_1\rangle$ and $|\psi_1'^{\mathsf{good}}\rangle := |\psi'_1\rangle$. Below we show the claim on $|\psi_{j+1}\rangle$ and $|\psi'_{j+1}\rangle$ holds if the claim on $|\psi_k\rangle$ and $|\psi'_k\rangle$ holds for $k = 1, \ldots, j$.

Recall that, in addition to database registers, the quantum oracle O_{LR_3} uses ancillary $2n$-qubit registers to compute the intermediate state after the first and second rounds (see (4.3) and (4.4)). We say that a state vector $|D_1\rangle |D_2\rangle |D_3\rangle \otimes$

$|x_1\rangle \otimes |x_2\rangle$ for O_{LR_3}, where $|x_1\rangle \otimes |x_2\rangle$ is the ancillary $2n$ qubits, is *regular* if $x_1 = 0^n$, $x_2 = 0^n$, and the database is valid. We define regular states for $O_{\mathsf{LR}'_3}$ similarly. Since the encoding operator U_{enc} of RstOE for f_i $(1 \le i \le 3)$ and F does not act on the ancillary $2n$-qubit registers, we always obtain regular vectors when we measure $|\psi_j\rangle$ and $|\psi'_j\rangle$. Similarly, we say that a state vector $|D_1\rangle |D_2\rangle |D_3\rangle \otimes |x_1\rangle \otimes |x_2\rangle$ for O_{LR_3} is *preregular* if $x_2 = 0^n$ and the database is valid, and define preregular states for $O_{\mathsf{LR}'_3}$ similarly. When we measure the states just before the first action of $O_{\mathrm{UP.2}}$ or just after the second action of $O_{\mathrm{UP.2}}$, we always measure preregular vectors. In this proof, for the sake of brevity, we do not write (a part of) the ancillary qubits that are used to compute the intermediate states, as long as they are $|0^m\rangle$ for some m.

Let Π_{good} and Π_{bad} denote the projections onto the vector space spanned by the vectors that correspond to good databases and bad databases, respectively. Let Π_{reg} and Π_{prereg} be the projections onto the spaces spanned by the vectors that correspond to regular and preregular states, respectively.

Action of the first $O_{\mathrm{UP.1}}$.
Here we show the following claim.

Claim 1 (Action of the first $O_{\mathrm{UP.1}}$)**.** *There exist vectors $|\psi_j^{\mathsf{good},1}\rangle$, $|\psi_j^{\mathsf{bad},1}\rangle$, $|\psi_j'^{\mathsf{good},1}\rangle$, $|\psi_j'^{\mathsf{bad},1}\rangle$ that satisfy the following properties.*

1. $O_{\mathrm{UP.1}} |\psi_j\rangle = |\psi_j^{\mathsf{good},1}\rangle + |\psi_j^{\mathsf{bad},1}\rangle$ *and* $O_{\mathrm{UP.1}} |\psi'_j\rangle = |\psi_j'^{\mathsf{good},1}\rangle + |\psi_j'^{\mathsf{bad},1}\rangle$.
2. *There exists complex number $a^{(j),1}_{x,y,z,D_1,D_2,D_F}$ such that*

$$|\psi_j^{\mathsf{good},1}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,good \\ D_1(x_L)\neq\perp}} a^{(j),1}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1,D_2,[D_F]_3\rangle \otimes |x_{1L},x_{1R}\rangle,$$

$$|\psi_j'^{\mathsf{good},1}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,good \\ D_1(x_L)\neq\perp}} a^{(j),1}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1,D_2,D_F\rangle \otimes |x_{1L},x_{1R}\rangle.$$

3. *The vector $|D_1,D_2,D_F\rangle$ in $|\psi_j'^{\mathsf{good},1}\rangle$ (resp., $|D_1,D_2,[D_F]_3\rangle$ in $|\psi_j^{\mathsf{good},1}\rangle$) has non-zero quantum amplitude only if $|D_1| \le 2(j-1)+1$, $|D_2| \le 2(j-1)$, and $|D_F| \le j-1$.*
4. $\| |\psi_j^{\mathsf{bad},1}\rangle \|$ *and* $\| |\psi_j'^{\mathsf{bad},1}\rangle \|$ *are upper bounded as*

$$\| |\psi_j^{\mathsf{bad},1}\rangle \| \le \| |\psi_j^{\mathsf{bad}}\rangle \| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \quad \| |\psi_j'^{\mathsf{bad},1}\rangle \| \le \| |\psi_j'^{\mathsf{bad}}\rangle \| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right).$$

Here, $x_{1L} = D_1(x_L) \oplus x_R$ and $x_{1R} = x_L$ for each summand of $|\psi_j^{\mathsf{good},1}\rangle$ and $|\psi_j'^{\mathsf{good},1}\rangle$.

Proof. Since the response of the first $O_{\mathrm{UP.1}}$ is written into an auxiliary register that is initially set to be $|0^{n/2},0^{n/2}\rangle$, by applying Proposition 4 to RstOE of f_1 there exist vectors $|\epsilon\rangle$, $|\epsilon'\rangle$ such that $\| |\epsilon\rangle \|, \| |\epsilon'\rangle \| \le O(\sqrt{1/2^{n/2}})$, and

$$\begin{aligned}
&\Pi_{\mathsf{valid}} O_{\mathrm{UP.1}} |\psi_j^{\mathsf{good}}\rangle \\
&= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)\neq\perp}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1,D_2,[D_F]_3\rangle \otimes |x_R \oplus D_1(x_L), x_L\rangle \\
&- \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1 \setminus (x_L,D_1(x_L)) \cup (x_L,\gamma), D_2, [D_F]_3\rangle \otimes |x_R \oplus \gamma, x_L\rangle \\
&+ \sum_{\substack{x,y,z,D_1,D_2,D_F,\alpha \\ (D_1,D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)=\perp}} \sqrt{\frac{1}{2^{n/2}}} a^{(j)}_{x,y,z,D_1,D_2,D_F} |x,y,z\rangle \otimes |D_1 \cup (x_L,\alpha), D_2, [D_F]_3\rangle \otimes |x_R \oplus \alpha, x_L\rangle \\
&+ |\epsilon\rangle
\end{aligned} \tag{4.13}$$

and

$$
\begin{aligned}
&\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1} \, |\psi_j^{'\mathsf{good}}\rangle \\
&\quad = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)\neq\perp}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x,y,z\rangle \otimes |D_1,D_2,D_F\rangle \otimes |x_R \oplus D(x_L), x_L\rangle \\
&\quad - \sum_{\substack{x,y,z,\gamma,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x,y,z\rangle \otimes |D_1 \setminus (x_L, D_1(x_L)) \cup (x_L,\gamma), D_2, D_F\rangle \otimes |x_R \oplus \gamma, x_L\rangle \\
&\quad + \sum_{\substack{x,y,z,D_1,D_2,D_F,\alpha \\ (D_1,D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)=\perp}} \sqrt{\frac{1}{2^{n/2}}} a^{(j)}_{x,y,z,D_1,D_2,D_F} \, |x,y,z\rangle \otimes |D_1 \cup (x_L,\alpha), D_2, D_F\rangle \otimes |x_R \oplus \alpha, x_L\rangle \\
&\quad + |\epsilon'\rangle
\end{aligned}
\tag{4.14}
$$

hold.

Now, let

$$
\begin{aligned}
|\psi_j^{\mathsf{good},1}\rangle &:= \Pi_{\mathsf{good}} \left(\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1} \, |\psi_j^{\mathsf{good}}\rangle - |\epsilon\rangle \right), \quad |\psi_j^{\mathsf{bad},1}\rangle := O_{\mathrm{UP}.1} \, |\psi_j\rangle - |\psi_j^{\mathsf{good},1}\rangle, \\
|\psi_j^{'\mathsf{good},1}\rangle &:= \Pi_{\mathsf{good}} \left(\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1} \, |\psi_j^{'\mathsf{good}}\rangle - |\epsilon'\rangle \right), \quad |\psi_j^{'\mathsf{bad},1}\rangle := O_{\mathrm{UP}.1} \, |\psi'_j\rangle - |\psi_j^{'\mathsf{good},1}\rangle .
\end{aligned}
$$

Then the first property of the claim holds by definition, and the second and third properties immediately follow from (4.13) and (4.14) and the assumption on $|\psi_j\rangle$ and $|\psi'_j\rangle$. Below we bound the norms of the bad vectors.

On the first term of the right hand side of (4.14), we have

$$
\Pi_{\mathsf{bad}} \Big(\text{the first term of the right hand side of (4.14)} \Big) = 0 \tag{4.15}
$$

since all the databases are good.

On the second term of the right hand side of (4.14), we have

$$
\begin{aligned}
&- \Pi_{\mathsf{bad}} \Big(\text{the second term of the right hand side of (4.14)} \Big) \\
&\quad = \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1\cup(x_L,\alpha),D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)=\perp \\ (D_1\cup(x_L,\gamma),D_2,D_F)\,:\,\mathrm{bad}}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x_L,\alpha),D_2,D_F} \, |x,y,z\rangle \otimes |D_1 \cup (x_L,\gamma), D_2, D_F\rangle \otimes |x_R \oplus \gamma, x_L\rangle \\
&\quad = \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1\cup(x_L,\alpha),D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)=\perp \\ (D_1\cup(x_L,\gamma),D_2,D_F)\,:\,\mathrm{bad} \\ D_2(x_{1L})\neq\perp\wedge[D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x_L,\alpha),D_2,D_F} \, |x,y,z\rangle \otimes |D_1 \cup (x_L,\gamma), D_2, D_F\rangle \otimes |x_R \oplus \gamma, x_L\rangle \qquad (4.16) \\
&\qquad + \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ (D_1\cup(x_L,\alpha),D_2,D_F)\,:\,\mathrm{good} \\ D_1(x_L)=\perp \\ (D_1\cup(x_L,\gamma),D_2,D_F)\,:\,\mathrm{bad} \\ D_2(x_{1L})=\perp\vee(D_2(x_{1L})\neq\perp\wedge[D_F]_3(x_{2L})=\perp)}} \frac{1}{2^{n/2}} a^{(j)}_{x,y,z,D_1\cup(x_L,\alpha),D_2,D_F} \, |x,y,z\rangle \otimes |D_1 \cup (x_L,\gamma), D_2, D_F\rangle \otimes |x_R \oplus \gamma, x_L\rangle , \qquad (4.17)
\end{aligned}
$$

where $x_{1L} := \alpha \oplus x_R$, and $x_{2L} := D_2(x_{1L}) \oplus x_L$ when $D_2(x_{1L}) \neq \perp$.

Here we give an upper bound of the norm of the term (4.16). If a tuple $(x, (D_1 \cup (x_L,\gamma), D_2, D_F))$ satisfies the conditions

1. $D_1(x_L) = \perp$,
2. $(D_1 \cup (x_L,\gamma), D_2, D_F)$ is bad,

then the number of α such that

1. $(D_1 \cup (x_L, \alpha), D_2, D_F)$ becomes good,
2. $D_2(x_{1L}) \neq \perp$ (here, $x_{1L} := \alpha \oplus x_R$), and
3. $[D_F]_3(x_{2L}) \neq \perp$ (here, $x_{2L} := D_2(x_{1L}) \oplus x_L$),

is at most $|D_2| \leq 2(j-1)$. Hence, by applying Lemma 5, we have

$$\|(4.16)\| \leq O\left(\sqrt{\frac{2(j-1)}{2^{n/2}}}\right) \tag{4.18}$$

Next, we give an upper bound of the norm of the term (4.17). For each tuple $(x, \alpha, (D_1, D_2, D_F))$ that satisfies

1. $D_1(x_L) = \perp$,
2. $(D_1 \cup (x_L, \alpha), D_2, D_F)$ is good, and
3. $D_2(x_{1L}) = \perp$ or $D_2(x_{1L}) \neq \perp \wedge [D_F]_3(x_{2L}) = \perp$ (here, $x_{1L} := \alpha \oplus x_R$ and $x_{2L} := D_2(x_{1L}) \oplus x_L$),

the number of γ such that $(D_1 \cup (x_L, \gamma), D_2, D_F)$ becomes bad is at most $|D_F| \leq j-1$. Thus, by applying Lemma 4, we have

$$\|(4.17)\| \leq O\left(\sqrt{\frac{j-1}{2^{n/2}}}\right). \tag{4.19}$$

From (4.16)–(4.19),

$$\left\|\Big(\text{the second term of the right hand side of (4.14)}\Big)\right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{4.20}$$

follows.

In addition, on the third term of the right hand side of (4.14), for each (x, D_1, D_2, D_F) such that (D_1, D_2, D_F) is good and $D_1(x_L) = \perp$, the number of α such that $(D_1 \cup (x_L, \alpha), D_2, D_F)$ becomes bad is at most $O(j)$. Hence, by applying Lemma 2 we have

$$\left\|\Big(\text{the third term of the right hand side of (4.14)}\Big)\right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right). \tag{4.21}$$

From (4.15), (4.20), and (4.21),

$$\left\|\Pi_{\mathsf{bad}}\left(\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\,|\psi_j'^{\mathsf{good}}\rangle - |\epsilon'\rangle\right)\right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{4.22}$$

follows. Since $\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\,|\psi_j'\rangle = O_{\mathrm{UP}.1}\,|\psi_j'\rangle$, we have

$$\begin{aligned}
\left\||\psi_j'^{\mathsf{bad},1}\rangle\right\| &= \left\|O_{\mathrm{UP}.1}\,|\psi_j'\rangle - |\psi_1'^{\mathsf{good},1}\rangle\right\| \\
&= \left\|\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\left(|\psi_j'^{\mathsf{good}}\rangle + |\psi_j'^{\mathsf{bad}}\rangle\right) - |\psi_1'^{\mathsf{good},1}\rangle\right\| \\
&\leq \left\|\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\,|\psi_j'^{\mathsf{good}}\rangle - |\psi_1'^{\mathsf{good},1}\rangle\right\| + \left\|\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\,|\psi_j'^{\mathsf{bad}}\rangle\right\| \\
&= \left\|\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\,|\psi_j'^{\mathsf{good}}\rangle - \Pi_{\mathsf{good}}\left(\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\,|\psi_j'^{\mathsf{good}}\rangle - |\epsilon'\rangle\right)\right\| + \left\||\psi_j'^{\mathsf{bad}}\rangle\right\| \\
&= \left\|\Pi_{\mathsf{bad}}\left(\Pi_{\mathsf{valid}} O_{\mathrm{UP}.1}\,|\psi_j'^{\mathsf{good}}\rangle - |\epsilon'\rangle\right)\right\| + \left\||\psi_j'^{\mathsf{bad}}\rangle\right\| \\
&\leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) + \left\||\psi_j'^{\mathsf{bad}}\rangle\right\|.
\end{aligned}$$

Similarly, we can also show $\left\||\psi_j^{\mathsf{bad},1}\rangle\right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) + \left\||\psi_j^{\mathsf{bad}}\rangle\right\|$. Therefore, the fourth property of the claim also holds. □

Action of the first $O_{\mathrm{UP}.2}$.
The following claim can be shown by applying Proposition 4 on f_2 in the same way as we showed the claim for the action of the first $O_{\mathrm{UP}.1}$ by applying Proposition 4 on f_1.

Claim 2 (Action of the first $O_{\mathrm{UP}.2}$)**.** *There exist vectors $|\psi_j^{\mathsf{good},2}\rangle$, $|\psi_j^{\mathsf{bad},2}\rangle$, $|\psi_j^{'\mathsf{good},2}\rangle$, $|\psi_j^{'\mathsf{bad},2}\rangle$ that satisfy the following properties.*

1. $O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}|\psi_j\rangle = |\psi_j^{\mathsf{good},2}\rangle + |\psi_j^{\mathsf{bad},2}\rangle$ *and* $O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}|\psi'_j\rangle = |\psi_j^{'\mathsf{good},2}\rangle + |\psi_j^{'\mathsf{bad},2}\rangle$.
2. *There exists complex number $a^{(j),2}_{x,y,z,D_1,D_2,D_F}$ such that*

$$|\psi_j^{\mathsf{good},2}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x_L)\neq\perp, D_2(x_{1L})\neq\perp}} a^{(j),2}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\otimes|D_1,D_2,[D_F]_3\rangle\otimes|x_{1L},x_{1R}\rangle\otimes|x_{2L},x_{2R}\rangle,$$

$$|\psi_j^{'\mathsf{good},2}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x_L)\neq\perp, D_2(x_{1L})\neq\perp}} a^{(j),2}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\otimes|D_1,D_2,D_F\rangle\otimes|x_{1L},x_{1R}\rangle\otimes|x_{2L},x_{2R}\rangle\,.$$

3. *The vector $|D_1,D_2,D_F\rangle$ in $|\psi_j^{'\mathsf{good},2}\rangle$ (resp., $|D_1,D_2,[D_F]_3\rangle$ in $|\psi_j^{\mathsf{good},2}\rangle$) has non-zero quantum amplitude only if $|D_1|\le 2(j-1)+1$, $|D_2|\le 2(j-1)+1$, and $|D_F|\le j-1$.*
4. $\||\psi_j^{\mathsf{bad},2}\rangle\|$ *and* $\||\psi_j^{'\mathsf{bad},2}\rangle\|$ *are upper bounded as*

$$\||\psi_j^{\mathsf{bad},2}\rangle\| \le \||\psi_j^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right),\quad \||\psi_j^{'\mathsf{bad},2}\rangle\| \le \||\psi_j^{'\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right).$$

Here, $x_{1L}=D_1(x_L)\oplus x_R$, $x_{1R}=x_L$, $x_{2L}=D_2(x_{1L})\oplus x_{1R}$, and $x_{2R}=x_{1L}$ for each summand of $|\psi_j^{\mathsf{good},2}\rangle$ and $|\psi_j^{'\mathsf{good},2}\rangle$.

Action of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$.
Here we show the following claim.

Claim 3 (Action of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$)**.** *Let $|\psi_j^{\mathsf{good},3}\rangle := \Pi_{\mathsf{valid}}O_{\mathrm{UP}.3}|\psi_j^{\mathsf{good},2}\rangle$, $|\psi_j^{\mathsf{bad},3}\rangle := O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}|\psi_j\rangle - |\psi_j^{\mathsf{good},3}\rangle$, $|\psi_j^{'\mathsf{good},3}\rangle := \Pi_{\mathsf{valid}}O_{\mathrm{UP}.3}|\psi_j^{'\mathsf{good},2}\rangle$, and $|\psi_j^{'\mathsf{bad},3}\rangle := O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}|\psi'_j\rangle - |\psi_j^{'\mathsf{good},3}\rangle$. Then the following properties hold.*

1. *There exists complex number $a^{(j),3}_{x,y,z,D_1,D_2,D_F}$ such that*

$$|\psi_j^{\mathsf{good},3}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x_L)\neq\perp, D_2(x_{1L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\otimes|D_1,D_2,[D_F]_3\rangle\otimes|x_{1L},x_{1R}\rangle\otimes|x_{2L},x_{2R}\rangle,$$

$$|\psi_j^{'\mathsf{good},3}\rangle = \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\ good \\ D_1(x_L)\neq\perp, D_2(x_{1L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\otimes|D_1,D_2,D_F\rangle\otimes|x_{1L},x_{1R}\rangle\otimes|x_{2L},x_{2R}\rangle\,.$$

2. *The vector $|D_1,D_2,D_F\rangle$ in $|\psi_j^{'\mathsf{good},3}\rangle$ (resp., $|D_1,D_2,[D_F]_3\rangle$ in $|\psi_j^{\mathsf{good},3}\rangle$) has non-zero quantum amplitude only if $|D_1|\le 2(j-1)+1$, $|D_2|\le 2(j-1)+1$, and $|D_F|\le j$.*
3. $\||\psi_j^{\mathsf{bad},3}\rangle\|$ *and* $\||\psi_j^{'\mathsf{bad},3}\rangle\|$ *are upper bounded as*

$$\||\psi_j^{\mathsf{bad},3}\rangle\| \le \||\psi_j^{\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right),\quad \||\psi_j^{'\mathsf{bad},3}\rangle\| \le \||\psi_j^{'\mathsf{bad}}\rangle\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right).$$

Here, $x_{1L}=D_1(x_L)\oplus x_R$, $x_{1R}=x_L$, $x_{2L}=D_2(x_{1L})\oplus x_{1R}$, and $x_{2R}=x_{1L}$ for each summand of $|\psi_j^{\mathsf{good},3}\rangle$ and $|\psi_j^{'\mathsf{good},3}\rangle$.

Remark 13. *Intuitively, a good database does not change to bad as long as it does not change to an invalid database when x_{2L} is queried to f_3 (or (x_{2L}, x_{2R}) is queried to F), due to the definition of good databases. This is the reason why $|\psi_j^{\mathsf{good},3}\rangle$ and $|\psi_j^{'\mathsf{good},3}\rangle$ are defined as above.*

Proof. First, for each summand $|x, y, z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle$ of $|\psi_j^{'\mathsf{good},2}\rangle$, we have that

$$\Pi_{\mathsf{bad}}\Pi_{\mathsf{valid}}O'_{\mathrm{UP}.3}\,|x, y, z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle = 0$$

by definition of good databases. Therefore, we have

$$\Pi_{\mathsf{bad}}\,|\psi_j^{'\mathsf{good},3}\rangle = \Pi_{\mathsf{bad}}\Pi_{\mathsf{valid}}O'_{\mathrm{UP}.3}\,|\psi_j^{'\mathsf{good},2}\rangle = 0,$$

which implies

$$|\psi_j^{'\mathsf{good},3}\rangle = \Pi_{\mathsf{good}}\,|\psi_j^{'\mathsf{good},3}\rangle\,.$$

Similarly,

$$|\psi_j^{\mathsf{good},3}\rangle = \Pi_{\mathsf{good}}\,|\psi_j^{\mathsf{good},3}\rangle$$

holds. Now the first property of the claim follows from the second property in the claim for the first action of $O_{\mathrm{UP}.2}$ and Lemma 1. The second property of the claim follows from the third property in the claim for the first action of $O_{\mathrm{UP}.2}$.

Moreover, we have

$$\begin{aligned}
\left\||\psi_j^{\mathsf{bad},3}\rangle\right\| &= \left\|O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\,|\psi_j\rangle - |\psi_j^{\mathsf{good},3}\rangle\right\| \\
&= \left\|\Pi_{\mathsf{valid}}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\,|\psi_j\rangle - \Pi_{\mathsf{valid}}O_{\mathrm{UP}.3}\,|\psi_j^{\mathsf{good},2}\rangle\right\| \\
&= \left\|\Pi_{\mathsf{valid}}O_{\mathrm{UP}.3}\,|\psi_j^{\mathsf{bad},2}\rangle\right\| \\
&\leq \left\||\psi_j^{\mathsf{bad},2}\rangle\right\| \\
&\leq \|\,|\psi_j^{\mathsf{bad}}\rangle\,\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \qquad (4.23)
\end{aligned}$$

where we used the fourth property in the claim for the first action of $O_{\mathrm{UP}.2}$ in the last inequality. Similarly, $\left\||\psi_j^{'\mathsf{bad},3}\rangle\right\| \leq \|\,|\psi_j^{'\mathsf{bad}}\rangle\,\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right)$ follows. Therefore, the third property of the claim holds. □

Action of the second $O_{\mathrm{UP}.2}$.
Next, we show the following claim.

Claim 4 (Action of the second $O_{\mathrm{UP}.2}$)**.** *Let $|\psi_j^{\mathsf{good},4}\rangle := \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\,|\psi_j^{\mathsf{good},3}\rangle$, $|\psi_j^{\mathsf{bad},4}\rangle := O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\,|\psi_j\rangle - |\psi_j^{\mathsf{good},4}\rangle$, $|\psi_j^{'\mathsf{good},4}\rangle := \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\,|\psi_j^{'\mathsf{good},3}\rangle$, and $|\psi_j^{'\mathsf{bad},4}\rangle := O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\,|\psi'_j\rangle - |\psi_j^{'\mathsf{good},4}\rangle$. Then the following properties hold.*

1. *There exists complex number $a^{(j),4}_{x,y,z,D_1,D_2,D_F}$ such that*

$$\begin{aligned}
|\psi_j^{\mathsf{good},4}\rangle &= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,good \\ D_1(x_L)\neq\perp}} a^{(j),4}_{x,y,z,D_1,D_2,D_F}\,|x, y, z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle, \\
|\psi_j^{'\mathsf{good},4}\rangle &= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F)\,:\,good \\ D_1(x_L)\neq\perp}} a^{(j),4}_{x,y,z,D_1,D_2,D_F}\,|x, y, z\rangle \otimes |D_1, D_2, D_F\rangle \otimes |x_{1L}, x_{1R}\rangle\,.
\end{aligned}$$

2. *The vector $|D_1, D_2, D_F\rangle$ in $|\psi_j^{'\mathsf{good},4}\rangle$ (resp., $|D_1, D_2, [D_F]_3\rangle$ in $|\psi_j^{\mathsf{good},4}\rangle$)) has non-zero quantum amplitude only if $|D_1| \leq 2(j-1)+1$, $|D_2| \leq 2j$, and $|D_F| \leq j$.*

3. *$\|\,|\psi_j^{\mathsf{bad},4}\rangle\,\|$ and $\|\,|\psi_j^{'\mathsf{bad},4}\rangle\,\|$ are upper bounded as*

$$\|\,|\psi_j^{\mathsf{bad},4}\rangle\,\| \leq \|\,|\psi_j^{\mathsf{bad}}\rangle\,\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \quad \|\,|\psi_j^{'\mathsf{bad},4}\rangle\,\| \leq \|\,|\psi_j^{'\mathsf{bad}}\rangle\,\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right).$$

Here, $x_{1L} = D_1(x_L) \oplus x_R$ and $x_{1R} = x_L$ for each summand of $|\psi_j^{\mathsf{good},4}\rangle$ and $|\psi_j^{'\mathsf{good},4}\rangle$.

Proof. The first property follows from the first property of Proposition 3 and the first property in the claim on the actions of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$. In addition, the second property follows from the second property in the claim on the actions of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$. Below, we show the third property.

Let $\Pi_{D_3:\not\perp}$ and $\Pi_{D_3:\perp}$ be the projections onto the spaces spanned by the vectors $|x, y, z\rangle \otimes |D_1, D_2, D_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |x_{2L}, x_{2R}\rangle$ such that $D_3(x_{2L}) \neq \perp$ and $D_3(x_{2L}) = \perp$, respectively.

Remark 14. *Before going into details, here we provide an intuition behind the following analysis. Roughly speaking, we will bound the norm of the vectors that are good before the application of the second $O_{\mathrm{UP}.2}$ but become bad after that, depending on $D_3(x_{2L}) \neq \perp$ and $D_3(x_{2L}) = \perp$. Intuitively, $D_3(x_{2L}) \neq \perp$ and $D_3(x_{2L}) = \perp$ imply that the value x_{2L} is entangled with the database for f_3 or is not, respectively. Therefore we need different analysis depending on $D_3(x_{2L}) \neq \perp$ and $D_3(x_{2L}) = \perp$. In addition, we can focus on the vectors that are bad* and *preregular after the application of $O_{\mathrm{UP}.2}$ because, when we measure the entire state after the second application of $O_{\mathrm{UP}.2}$, we always obtain a preregular state. In summary, our first goal is to bound the norms of $\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_3:\not\perp}|\psi_j^{\mathsf{good},3}\rangle$ and $\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_3:\perp}|\psi_j^{\mathsf{good},3}\rangle$.*

We have

$$
\begin{aligned}
&\Pi_{D_3:\not\perp}|\psi_j^{\mathsf{good},3}\rangle \\
&= \sum_{\substack{x,y,z,D_1,D_2,D_F \\ (D_1,D_2,D_F):\text{good} \\ D_1(x_L)\neq\perp, D_2(x_{1L})\neq\perp \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\otimes|D_1,D_2,[D_F]_3\rangle\otimes|x_{1L},x_{1R}\rangle\otimes|x_{2L},x_{2R}\rangle \\
&= \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{good} \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle\otimes|D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle\otimes|x_{1L},x_{1R}\rangle\otimes|x_{2L},x_{2R}\rangle,
\end{aligned}
$$

where $x_{1L} := D_1(x_L) \oplus x_R$, $x_{1R} := x_L$, $x_{2L} := \alpha \oplus x_{1R}$, and $x_{2R} := x_{1L}$ for each summand in the right hand side. Now we have that

$$
\begin{aligned}
&\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_3:\not\perp}|\psi_j^{\mathsf{good},3}\rangle \\
&= \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{good} \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle\otimes|D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle \\
&\qquad\qquad\otimes|x_{1L},x_{1R}\rangle\otimes|x_{2L},x_{2R}\rangle \\
&= \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}\sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{good} \\ [D_F]_3(x_{2L})\neq\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle\otimes|D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle \\
&\qquad\qquad\otimes|x_{1L},x_{1R}\rangle\otimes|0^{n/2},0^{n/2}\rangle \qquad (4.24) \\
&\quad+\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}\sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{\sqrt{2^{n/2}}}a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle \qquad (4.25) \\
&\qquad\qquad\otimes|D_1\rangle\left(|D_2\rangle-\sum_{\gamma}\frac{1}{\sqrt{2^{n/2}}}|D_2\cup(x_{1L},\gamma)\rangle\right)|[D_F]_3\rangle \\
&\qquad\qquad\otimes|x_{1L},x_{1R}\rangle\otimes|0^{n/2},0^{n/2}\rangle \\
&\quad-\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}\sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{n/2}}a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle \qquad (4.26) \\
&\qquad\qquad\otimes|D_1\rangle\left(|D_2\cup(x_{1L},\gamma)\rangle-|D^{\mathsf{invalid}}_{\gamma}\rangle\right)|[D_F]_3\rangle \\
&\qquad\qquad\otimes|x_{1L},x_{1R}\rangle\otimes|\alpha\oplus\gamma,0^{n/2}\rangle \\
&\quad+\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}\sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F):\text{good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{n/2}}a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle \qquad (4.27) \\
&\qquad\qquad\otimes|D_1\rangle\left(2\sum_{\delta}\frac{1}{\sqrt{2^{n/2}}}|D_2\cup(x_{1L},\delta)\rangle-|D_2\rangle\right)|[D_F]_3\rangle \\
&\qquad\qquad\otimes|x_{1L},x_{1R}\rangle\otimes|\widehat{0^{n/2}},0^{n/2}\rangle
\end{aligned}
$$

holds, where the second equation follows from the first property of Proposition 3 to f_2 (the term (4.24) corresponds to the term "$|x\rangle\,|y \oplus \alpha\rangle \otimes |D \cup (x, \alpha)\rangle$" in the proposition, and the terms (4.25), (4.26), (4.27) correspond to the three terms (3.13)-(3.15)).

On the term (4.24), we have

$$(4.24) = 0 \tag{4.28}$$

since all databases are good.

On the term (4.25), we have

$$\begin{aligned}(4.25) = \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1, D_2\cup(x_{1L},\alpha), D_F)\,:\,\text{good} \\ [D_F]_3(x_{2L})\neq\perp}} & \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x, y, z\rangle \\ & \otimes |D_1\rangle \left(|D_2\rangle - \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |D_2 \cup (x_{1L}, \gamma)\rangle \right) |[D_F]_3\rangle \\ & \otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle \end{aligned}$$

$$= \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1, D_2\cup(x_{1L},\alpha), D_F)\,:\,\text{good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x, y, z\rangle \otimes |D_1, D_2, [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle \tag{4.29}$$

$$- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1, D_2\cup(x_{1L},\alpha), D_F)\,:\,\text{good} \\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x, y, z\rangle \otimes |D_1, D_2 \cup (x_{1L}, \gamma), [D_F]_3\rangle \otimes |x_{1L}, x_{1R}\rangle \otimes |0^{n/2}, 0^{n/2}\rangle\,. \tag{4.30}$$

First, we upper bound the norm of the term (4.29). For each (x, y, z, D_1, D_2, D_F) such that $D_1(x_L) \neq \perp$ and $D_2(x_{1L}) = \perp$ (recall that $x_{1L} := x_R \oplus D_1(x_L)$), the number of α such that $[D_F]_3(x_{2L}) \neq \perp$ (recall that $x_{2L} := x_L \oplus \alpha$) and $(D_1, D_2 \cup (x_{1L}, \alpha), D_F)$ becomes good is at most $|D_F| \leq j$. Hence, by applying Lemma 3 we have

$$\|(4.29)\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right). \tag{4.31}$$

Second, we upper bound the norm of the term (4.30). If a tuple $(x, (D_1, D_2 \cup (x_L, \gamma), D_F))$ satisfies the conditions

1. $D_1(x_L) \neq \perp$,
2. $(D_1, D_2 \cup (x_{1L}, \gamma), D_F)$ is bad,

then the number of α such that

1. $(D_1, D_2 \cup (x_{1L}, \alpha), D_F)$ becomes good,
2. $D_2(x_{1L}) = \perp$ (here, $x_{1L} := D_1(x_L) \oplus x_R$), and
3. $[D_F]_3(x_{2L}) \neq \perp$ (here, $x_{2L} := \alpha \oplus x_L$),

is at most $|D_F| \leq j$. Hence, by applying Lemma 5, we have

$$\|(4.30)\| \leq O\left(\frac{j}{2^{n/2}}\right). \tag{4.32}$$

From (4.29)–(4.32),

$$\|(4.25)\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{4.33}$$

follows.

On the term (4.26), we have

$$\begin{aligned}(4.26) &= -\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F\\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle \\ &\qquad\qquad \otimes |D_1\rangle\left(|D_2\cup(x_{1L},\gamma)\rangle - |D_\gamma^{\mathsf{invalid}}\rangle\right)|[D_F]_3\rangle \\ &\qquad\qquad \otimes |x_{1L},x_{1R}\rangle\otimes|\alpha\oplus\gamma,0^{n/2}\rangle \\ &= -\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{3n/2}} a^{(j),3}_{x,y,z,D_1,D_2,D_F}\,|x,y,z\rangle\otimes|D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle \\ &\qquad\qquad \otimes|x_{1L},x_{1R}\rangle\otimes|0^{n/2},0^{n/2}\rangle \\ &= 0, \end{aligned} \tag{4.34}$$

where the second equality holds since Π_{prereg} cancels the terms with invalid databases and those with $\alpha\oplus\gamma\neq 0^{n/2}$, and the last equality holds since Π_{bad} cancels good databases.

On the term (4.27), first we have

$$\begin{aligned}(4.27) &= \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle \\ &\qquad\qquad \otimes|D_1\rangle\left(2\sum_\delta\frac{1}{\sqrt{2^{n/2}}}|D_2\cup(x_{1L},\delta)\rangle - |D_2\rangle\right)|[D_F]_3\rangle \\ &\qquad\qquad \otimes|x_{1L},x_{1R}\rangle\otimes|\widehat{0^{n/2}},0^{n/2}\rangle \\ &= \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,\delta,D_1,D_2,D_F\\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})\neq\perp}} \frac{2}{2^n} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle\otimes|D_1,D_2\cup(x_{1L},\delta),[D_F]_3\rangle \\ &\qquad\qquad \otimes|x_{1L},x_{1R}\rangle\otimes|0^{n/2},0^{n/2}\rangle, \end{aligned} \tag{4.35}$$

$$\begin{aligned} &- \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})\neq\perp}} \frac{1}{\sqrt{2^{3n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle\otimes|D_1,D_2,[D_F]_3\rangle \\ &\qquad\qquad \otimes|x_{1L},x_{1R}\rangle\otimes|0^{n/2},0^{n/2}\rangle \end{aligned} \tag{4.36}$$

$$= -\frac{2}{2^{n/2}}\cdot(4.30) - \frac{1}{\sqrt{2^{n/2}}}\cdot(4.29). \tag{4.37}$$

Hence

$$\|(4.27)\| \le O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{4.38}$$

follows from (4.31) and (4.32).

From (4.24)–(4.28), (4.33) (4.34), and (4.38),

$$\left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_F:\not\perp}\,|\psi_j^{\mathsf{good},3}\rangle\right\| \le O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{4.39}$$

follows.

In the same way as we obtained (4.24)–(4.27), by applying the first property of Proposition 3 to f_2 we have

$$\begin{aligned}&\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_3:\perp}\,|\psi_j^{\mathsf{good},3}\rangle \\ &= \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})=\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle\otimes|D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle \\ &\qquad\qquad \otimes|x_{1L},x_{1R}\rangle\otimes|x_{2L},x_{2R}\rangle \\ &= \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F\\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp\\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\text{good}\\ [D_F]_3(x_{2L})=\perp}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F}\,|x,y,z\rangle\otimes|D_1,D_2\cup(x_{1L},\alpha),[D_F]_3\rangle \\ &\qquad\qquad \otimes|x_{1L},x_{1R}\rangle\otimes|0^{n/2},0^{n/2}\rangle \end{aligned} \tag{4.40}$$

$$+\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \otimes |D_1\rangle \left(|D_2\rangle - \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |D_2 \cup (x_{1L},\gamma)\rangle \right) |[D_F]_3\rangle \otimes |x_{1L},x_{1R}\rangle \otimes |0^{n/2},0^{n/2}\rangle \tag{4.41}$$

$$-\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \otimes |D_1\rangle \left(|D_2 \cup (x_{1L},\gamma)\rangle - |D^{\mathsf{invalid}}_{\gamma}\rangle \right) |[D_F]_3\rangle \otimes |x_{1L},x_{1R}\rangle \otimes |\alpha\oplus\gamma,0^{n/2}\rangle \tag{4.42}$$

$$+\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \otimes |D_1\rangle \left(2\sum_{\delta} \tfrac{1}{\sqrt{2^{n/2}}} |D_2 \cup (x_{1L},\delta)\rangle - |D_2\rangle \right) |[D_F]_3\rangle \otimes |x_{1L},x_{1R}\rangle \otimes |\widehat{0^{n/2}},0^{n/2}\rangle\,. \tag{4.43}$$

On the term (4.40), we have

$$(4.40) = 0 \tag{4.44}$$

since all databases are good.

On the term (4.41), we have

$$(4.41) = \Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \otimes |D_1\rangle \left(|D_2\rangle - \sum_{\gamma} \frac{1}{\sqrt{2^{n/2}}} |D_2 \cup (x_{1L},\gamma)\rangle \right) |[D_F]_3\rangle \otimes |x_{1L},x_{1R}\rangle \otimes |0^{n/2},0^{n/2}\rangle$$

$$= \Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{\sqrt{2^{n/2}}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \otimes |D_1,D_2,[D_F]_3\rangle \otimes |x_{1L},x_{1R}\rangle \otimes |0^{n/2},0^{n/2}\rangle \tag{4.45}$$

$$-\Pi_{\mathsf{bad}} \sum_{\substack{x,y,z,\alpha,\gamma,D_1,D_2,D_F \\ D_1(x_L)\neq\perp, D_2(x_{1L})=\perp \\ (D_1,D_2\cup(x_{1L},\alpha),D_F)\,:\,\mathrm{good} \\ [D_F]_3(x_{2L})=\perp}} \frac{1}{2^{n/2}} a^{(j),3}_{x,y,z,D_1,D_2\cup(x_{1L},\alpha),D_F} |x,y,z\rangle \otimes |D_1,D_2\cup(x_{1L},\gamma),[D_F]_3\rangle \otimes |x_{1L},x_{1R}\rangle \otimes |0^{n/2},0^{n/2}\rangle\,. \tag{4.46}$$

The term (4.45) is zero since all databases are good. Below, we give an upper bound of the norm of the term (4.46). Note that, for each tuple $(x,\alpha,(D_1,D_2,D_F))$ that satisfies

1. $D_1(x_L)\neq\perp$,
2. $(D_1,D_2\cup(x_{1L},\alpha),D_F)$ is good, and
3. $[D_F]_3(x_{2L})=\perp$ (here, $x_{1L}:=D_1(x_L)\oplus x_R$ and $x_{2L}:=\alpha\oplus x_L$),

the number of γ such that $(D_1\cup(x_L,\gamma),D_2,D_F)$ becomes bad is at most $|D_F|\leq j$. Hence, by applying Lemma 4, we have

$$\|(4.46)\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right). \tag{4.47}$$

From (4.45)–(4.47),

$$\|(4.41)\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{4.48}$$

follows.

On the term (4.42), we can show

$$(4.42) = 0 \tag{4.49}$$

in the same way as we showed (4.34).

On the term (4.43), we have

$$(4.43) = -\frac{2}{2^{n/2}} \cdot (4.46) - \frac{1}{\sqrt{2^{n/2}}} \cdot (4.45).$$

Hence

$$\|(4.43)\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{4.50}$$

holds.

From (4.40)–(4.44) and (4.48)–(4.50),

$$\left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_F:\perp}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \tag{4.51}$$

follows.

Therefore,

$$\begin{aligned}
&\left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&\leq \left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_F:\not\perp}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| + \left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\Pi_{D_F:\perp}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&\leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right)
\end{aligned} \tag{4.52}$$

follows from (4.39) and (4.51).

Since $O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\left|\psi_j\right\rangle = \Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\left|\psi_j\right\rangle$,

$$\begin{aligned}
&\left\|\left|\psi_j^{\mathsf{bad},4}\right\rangle\right\| \\
&= \left\|O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\left|\psi_j\right\rangle - \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&= \left\|\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}O_{\mathrm{UP}.3}O_{\mathrm{UP}.2}O_{\mathrm{UP}.1}\left|\psi_j\right\rangle - \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&= \left\|\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left(\left|\psi_j^{\mathsf{good},3}\right\rangle + \left|\psi_j^{\mathsf{bad},3}\right\rangle\right) - \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| \\
&\leq \left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{good},3}\right\rangle\right\| + \left\|\Pi_{\mathsf{prereg}}O_{\mathrm{UP}.2}\left|\psi_j^{\mathsf{bad},3}\right\rangle\right\| \\
&\leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) + \left\|\left|\psi_j^{\mathsf{bad},3}\right\rangle\right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) + \left\|\left|\psi_j^{\mathsf{bad}}\right\rangle\right\|
\end{aligned}$$

follows from the claim on the action of $O_{\mathrm{UP}.3}$ and $O'_{\mathrm{UP}.3}$. We can show

$$\left\|\left|\psi_j^{'\mathsf{bad},4}\right\rangle\right\| \leq O\left(\sqrt{\frac{j}{2^{n/2}}}\right) + \left\|\left|\psi_j^{'\mathsf{bad}}\right\rangle\right\| \tag{4.53}$$

in the same way, and the third property of the claim also holds. □

Action of the second $O_{\mathrm{UP}.1}$ (and U_j).

Recall that U_j denotes the unitary operator that corresponds to $\mathcal{A}$'s offline computation after the j-th query. Let $\left|\psi_{j+1}^{\mathsf{good}}\right\rangle := U_j\Pi_{\mathsf{good}}\Pi_{\mathsf{reg}}O_{\mathrm{UP}.1}\left|\psi_j^{\mathsf{good},4}\right\rangle$, $\left|\psi_{j+1}^{\mathsf{bad}}\right\rangle := \left|\psi_{j+1}\right\rangle - \left|\psi_{j+1}^{\mathsf{good}}\right\rangle$, $\left|\psi_{j+1}^{'\mathsf{good}}\right\rangle := U_j\Pi_{\mathsf{good}}\Pi_{\mathsf{reg}}O_{\mathrm{UP}.1}\left|\psi_j^{'\mathsf{good},4}\right\rangle$, and $\left|\psi_{j+1}^{'\mathsf{bad}}\right\rangle := \left|\psi'_{j+1}\right\rangle - \left|\psi_{j+1}^{'\mathsf{good}}\right\rangle$. Then we can show these $\left|\psi_{j+1}^{\mathsf{good}}\right\rangle$, $\left|\psi_{j+1}^{\mathsf{bad}}\right\rangle$, $\left|\psi_{j+1}^{'\mathsf{good}}\right\rangle$, and $\left|\psi_{j+1}^{'\mathsf{bad}}\right\rangle$ satisfy the desired properties in Proposition 6, in the same way as we showed the claim on the action of the second $O_{\mathrm{UP}.2}$. □

4.2.1.9 Finishing the Proof of Proposition 5

Proof of Proposition 5. Let $|\psi_j^{\mathsf{good}}\rangle$, $|\psi_j^{\mathsf{bad}}\rangle$, $|\psi_j^{'\mathsf{good}}\rangle$, and $|\psi_j^{'\mathsf{bad}}\rangle$ be the vectors as in Proposition 6. Then

$$\left\||\psi_{q+1}^{\mathsf{bad}}\rangle\right\| \leq \sum_{1\leq j\leq q} O\left(\sqrt{\frac{j}{2^{n/2}}}\right) \leq O\left(\sqrt{\frac{j^3}{2^{n/2}}}\right) \tag{4.54}$$

follows. Similarly,

$$\left\||\psi_{q+1}^{'\mathsf{bad}}\rangle\right\| \leq O\left(\sqrt{\frac{j^3}{2^{n/2}}}\right) \tag{4.55}$$

holds.

Recall that $\mathsf{tr}_{\mathcal{D}_{123}}$ and $\mathsf{tr}_{\mathcal{D}_{12F}}$ denote the partial trace operations over the databases for LR_3 and LR_3', respectively. Then

$$\mathsf{td}\left(\mathsf{tr}_{\mathcal{D}_{123}}\left(|\psi_{q+1}^{\mathsf{good}}\rangle\langle\psi_{q+1}^{\mathsf{good}}|\right), \mathsf{tr}_{\mathcal{D}_{12F}}\left(|\psi_{q+1}^{'\mathsf{good}}\rangle\langle\psi_{q+1}^{'\mathsf{good}}|\right)\right) = 0 \tag{4.56}$$

follows from (4.10) and (4.11).

Therefore

$$\begin{aligned}
\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_3,\mathsf{LR}_3'}(\mathcal{A}) &\leq \mathsf{td}\left(\mathsf{tr}_{\mathcal{D}_{123}}\left(|\psi_{q+1}\rangle\langle\psi_{q+1}|\right), \mathsf{tr}_{\mathcal{D}_{12F}}\left(|\psi'_{q+1}\rangle\langle\psi'_{q+1}|\right)\right) \\
&\leq \mathsf{td}\left(\mathsf{tr}_{\mathcal{D}_{123}}\left(|\psi_{q+1}^{\mathsf{good}}\rangle\langle\psi_{q+1}^{\mathsf{good}}|\right), \mathsf{tr}_{\mathcal{D}_{12F}}\left(|\psi_{q+1}^{'\mathsf{good}}\rangle\langle\psi_{q+1}^{'\mathsf{good}}|\right)\right) + 2\left\||\psi_{q+1}^{\mathsf{bad}}\rangle\right\| + 2\left\||\psi_{q+1}^{'\mathsf{bad}}\rangle\right\| \\
&\leq O\left(\sqrt{\frac{j^3}{2^{n/2}}}\right)
\end{aligned} \tag{4.57}$$

holds, which completes the proof. □

4.2.2 Hardness of Distinguishing LR_2'' from RF

The goal of this subsection is to show the following proposition.

Proposition 7. $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_2'',\mathsf{RF}}(q)$ *is in* $O\left(\sqrt{q^3/2^{n/2}}\right)$.

Let $F_1 : \{0,1\}^{n/2}\times\{0,1\}^{n/2} \to \{0,1\}^{n/2}$ and $F_2' : \{0,1\}^{n/2}\times\{0,1\}^{n/2}\times\{0,1\}^{n/2} \to \{0,1\}^{n/2}$ be independent random functions. Let $\mathsf{RF}' : \{0,1\}^{n/2}\times\{0,1\}^{n/2} \to \{0,1\}^{n/2}\times\{0,1\}^{n/2}$ be the function defined by

$$\mathsf{RF}'(x_L, x_R) := (F_2'(x_{1L}, x_{1R}, x_R), x_{1L}),$$

where $(x_{1L}, x_{1R}) := (F_1(x_L, x_R), x_L)$ (see Fig. 4.7). Note that RF' is in fact a random function since F_1 and F_2' are

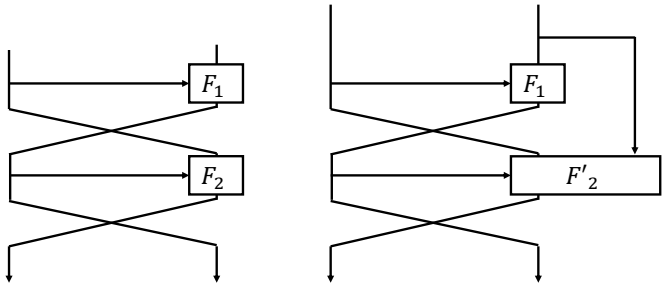


Figure 4.7: LR_2'' and RF'.

random functions. In what follows, we show

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}''_2,\mathsf{RF}'}(q) \le O\left(\sqrt{q^3/2^{n/2}}\right)$$

instead of showing $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}''_2,\mathsf{RF}}(q) \le O\left(\sqrt{q^3/2^{n/2}}\right)$.

We use the same proof strategy as in Section 4.2.1. That is, we define good and bad databases for LR''_2 and RF' in such a way that

1. There exists a one-to-one correspondence between good databases for LR''_2 and those for RF'.
2. The behavior of the oracle LR''_2 on a good database is almost the same as that of the oracle RF' on the corresponding good database.
3. "Good" states change to "bad" states with a small probability.

Intuitively, we define "bad" databases as those with collisions on the leftmost $(n/2)$ bits of the input to F_2 or F'_2, and "good" databases as those without such collisions.

4.2.2.1 Quantum Oracle of LR''_2

Let us define the unitary operator $O_{\mathrm{UP}.i}$ that computes the state update of the first round by

$$O_{\mathrm{UP}.i} : |x_{(i-1)L}, x_{(i-1)R}\rangle\,|y_L, y_R\rangle \mapsto |x_{(i-1)L}, x_{(i-1)R}\rangle\,|(y_L, y_R) \oplus (F_i(x_{(i-1)L}, x_{(i-1)R}), x_{(i-1)L})\rangle\,.$$

$O_{\mathrm{UP}.i}$ can be implemented by making one query to F_i. Then $O_{\mathsf{LR}''_2}$ can be implemented as follows by using $O_{\mathrm{UP}.1}$ and $O_{\mathrm{UP}.2}$:

1. Take $|x\rangle\,|y\rangle = |x_{0L}, x_{0R}\rangle\,|y_L, y_R\rangle$ as an input.
2. Compute the state (x_{1L}, x_{1R}) by querying $|x_{0L}, x_{0R}\rangle\,|0^n\rangle$ to $O_{\mathrm{Up}.1}$, and obtain
$$|x_{0L}, x_{0R}\rangle\,|y_L, y_R\rangle \otimes |x_{1L}, x_{1R}\rangle\,.$$
3. Query $|x_{1L}, x_{1R}\rangle\,|y_L, y_R\rangle$ to $O_{\mathrm{UP}.2}$, and obtain
$$|x\rangle\,|y \oplus \mathsf{LR}''_2(x)\rangle \otimes |x_{1L}, x_{1R}\rangle\,.$$
4. Uncompute Step 2 to obtain
$$|x\rangle\,|y \oplus \mathsf{LR}''_2(x)\rangle\,.$$
5. Return $|x\rangle\,|y \oplus \mathsf{LR}''_2(x)\rangle$.

4.2.2.2 Quantum Oracle of RF'

The quantum oracle of RF' is implemented in the same way as LR''_2, except that the second round state update oracle $O_{\mathrm{UP}.2}$ is replaced with another oracle $O'_{\mathrm{UP}.2}$ defined as

$$O'_{\mathrm{UP}.2} : |x_{0R}, x_{1L}, x_{1R}\rangle\,|y_L, y_R\rangle \mapsto |x_{0R}, x_{1L}, x_{1R}\rangle\,|(y_L, y_R) \oplus (F'_2(x_{1L}, x_{1R}, x_{0R}), x_{1L})\rangle\,.$$

In what follows, we assume that the oracles of F_1, F_2, and F'_2 are implemented with the recording standard oracle with errors, and we use D_1, D_2, and D'_2 to denote (valid) databases for F_1, F_2, and F'_2, respectively.

4.2.2.3 Good and Bad Databases for LR''_2

Here we introduce the notion of *good* and *bad* for each tuple (D_1, D_2) of valid database for LR''_2. We say that a valid database D_2 is *without overlap* if each pair of distinct entries (x_{1L}, x_{1R}, β) and $(x'_{1L}, x'_{1R}, \beta')$ in D_2 satisfies $x_{1L} \neq x'_{1L}$. We say that (D_1, D_2) is good if D_2 is without overlap, and for each entry $(x_{1L}, x_{1R}, \beta) \in D_2$, there exists exactly one entry $(x_{0L}, x_{0R}, \alpha) \in D_1$ such that $\alpha = x_{1L}$ and $x_{1R} = x_{0L}$. We say that (D_1, D_2) is bad if it is not good.

4.2.2.4 Good and Bad Databases for RF'

Next, we introduce the notion of *good* and *bad* for each tuple (D_1, D_2') of valid database for RF'. In addition, we say that a valid database D_2' is *without overlap* if each pair of distinct entries $(x_{1L}, x_{1R}, x_{0R}, \beta)$ and $(x'_{1L}, x'_{1R}, x'_{0R}, \beta')$ in D_2' satisfies $x_{1L} \neq x'_{1L}$. We say that (D_1, D_2') is good if D_2' is without overlap, and for each entry $(x_{1L}, x_{1R}, x_{0R}, \beta) \in D_2'$, there exists exactly one entry $(x_{0L}, x_{0R}, \alpha) \in D_1$ such that $\alpha = x_{1L}$ and $x_{1R} = x_{0L}$. We say that (D_1, D_2') is bad if it is not good.

In addition, we say that a valid database D_2' for F_2' is *normal* if $D_2'(x_{1L}, x_{1R}, x_{0R}) \neq \perp$, then $D_2'(x'_{1L}, x_{1R}, x_{0R}) = \perp$ for all $x'_{1L} \neq x_{1L}$. Note that, for each good database (D_1, D_2') for RF', D_2' becomes normal by definition.

4.2.2.5 Compatibility of D_2' with D_2

For a valid and normal database D_2' for F_2' without overlap, let $[D_2']_2$ be the valid database for F_2 such that $(x_{1L}, x_{1R}, \beta) \in D_2$ if and only if there is a unique x_{0R} such that $(x_{1L}, x_{1R}, x_{0R}, \beta) \in D_2'$. Then $[D_2']_2$ is without overlap. We say that a valid database D_2 for F_2 without overlap is compatible with D_2' if $D_2 = [D_2']_2$.

Remark 15. *For each good database (D_1, D_2) for LR_2'', a unique D_2' without overlap exists such that $[D_2']_2 = D_2$ and (D_1, D_2') is a good database for RF', by the definition of good databases. Similarly, for each good database (D_1, D_2') for RF', $(D_1, [D_2']_2)$ becomes a good database for LR_2''. That is, there exists a one-to-one correspondence between good databases for LR_2'' and those for RF'.*

The following lemma shows that the behavior of $O'_{\mathrm{UP}.2}$ on a valid and normal databases D_2' for F_2' without overlap is the same as that of $O_{\mathrm{UP}.2}$ on the corresponding database $[D_2']_2$ for F_2.

Lemma 6. *It holds that*

$$\begin{aligned}&\langle \tilde{x}_{0R}, \tilde{x}_{1L}, \tilde{x}_{1R}, \tilde{y}_L, \tilde{y}_R| \otimes \langle \tilde{D}_2'| \, O'_{\mathrm{UP}.2} \, |x_{0R}, x_{1L}, x_{1R}, y_L, y_R\rangle \otimes |D_2'\rangle \\ &\quad = \langle \tilde{x}_{0R}, \tilde{x}_{1L}, \tilde{x}_{1R}, \tilde{y}_L, \tilde{y}_R| \otimes \langle [\tilde{D}_2']_2| \, O_{\mathrm{UP}.2} \, |x_{0R}, x_{1L}, x_{1R}, y_L, y_R\rangle \otimes |[D_2']_2\rangle\end{aligned}$$

for any $x_{0R}, x_{1L}, x_{1R}, y_L, y_R, \tilde{x}_{0R}, \tilde{x}_{1L}, \tilde{x}_{1R}, \tilde{y}_L, \tilde{y}_R \in \{0,1\}^{n/2}$ and any valid and normal databases D_2' and $\tilde{D}_2'$ for F_2' without overlap.

We omit to write the proof since the lemma can be shown in the same way as we showed Lemma 1.

Let $\mathcal{A}$ be an adversary that makes at most q quantum queries. Let $|\psi_j\rangle$ and $|\psi_j'\rangle$ be the joint quantum states of $\mathcal{A}$ and the oracle just before making the j-th query when $\mathcal{A}$ runs relative to LR_2'' and RF', respectively. In addition, by $|\psi_{q+1}\rangle$ and $|\psi'_{q+1}\rangle$ we similarly denote the states just before the final measurement, by abuse of notation. Then the following proposition holds.

Proposition 8. *For each $j = 1, \ldots, q+1$, there exist vectors $|\psi_j^{\mathsf{good}}\rangle$, $|\psi_j^{\mathsf{bad}}\rangle$, $|\psi_j^{'\mathsf{good}}\rangle$, $|\psi_j^{'\mathsf{bad}}\rangle$, and complex number $a^{(j)}_{x,y,z,D_1,D_2'}$ such that*

$$\begin{aligned}|\psi_j\rangle &= |\psi_j^{\mathsf{good}}\rangle + |\psi_j^{\mathsf{bad}}\rangle, \quad |\psi_j'\rangle = |\psi_j^{'\mathsf{good}}\rangle + |\psi_j^{'\mathsf{bad}}\rangle, \\ |\psi_j^{\mathsf{good}}\rangle &= \sum_{\substack{x,y,z,D_1,D_2' \\ (D_1,D_2') \,:\, good}} a^{(j)}_{x,y,z,D_1,D_2'} \, |x,y,z\rangle \otimes |D_1, [D_2']_2\rangle, \\ |\psi_j^{'\mathsf{good}}\rangle &= \sum_{\substack{x,y,z,D_1,D_2' \\ (D_1,D_2') \,:\, good}} a^{(j)}_{x,y,z,D_1,D_2'} \, |x,y,z\rangle \otimes |D_1, D_2'\rangle,\end{aligned}$$

the vector $|D_1, D_2'\rangle$ in $|\psi_j^{'\mathsf{good}}\rangle$ (resp., $|D_1, [D_2']_2\rangle$ in $|\psi_j^{\mathsf{good}}\rangle$) has non-zero quantum amplitude only if $|D_1| \leq 2(j-1)$ and $|D_2'| \leq j-1$, and

$$\| \, |\psi_j^{\mathsf{bad}}\rangle \, \| \leq \left\| |\psi_{j-1}^{\mathsf{bad}}\rangle \right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right), \quad \| \, |\psi_j^{'\mathsf{bad}}\rangle \, \| \leq \left\| |\psi_{j-1}^{'\mathsf{bad}}\rangle \right\| + O\left(\sqrt{\frac{j}{2^{n/2}}}\right)$$

hold (we set $|\psi_0^{\mathsf{bad}}\rangle = 0$ and $|\psi_0^{'\mathsf{bad}}\rangle = 0$).

The proposition can be shown in a similar way as we showed Proposition 6, and thus we omit to write the entire proof. Since here only two random functions are involved in each oracle while three random functions are involved in each oracle in Proposition 6, the proof becomes simpler: When we prove Proposition 8, we can skip showing the claims that correspond to those for the actions of $O_{\mathrm{UP}.2}$ in the proof of Proposition 6.

Now we can show that $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}''_2,\mathsf{RF}'}(\mathcal{A}) \leq O\left(\sqrt{q^3/2^{n/2}}\right)$ follows from Proposition 8 in the same way as we showed that Proposition 5 follows from Proposition 6. Therefore Proposition 7 holds.

4.2.3 Proof of Theorem 9

This subsection finishes our proof of Theorem 9, by using the results given in Sections 4.2.1 and 4.2.2.

Proof of Theorem 9. First, let us modify LR_4 in such a way that the state updates of the third and fourth rounds are replaced with $(x_{2L}, x_{2R}) \mapsto (x_{3L}, x_{3R}) := (F(x_{2L}, x_{2R}), x_{2L})$ and $(x_{3L}, x_{3R}) \mapsto (x_{4L}, x_{4R}) := (F'(x_{3L}, x_{3R}), x_{3L})$, respectively, where $F, F' : \{0,1\}^{n/2} \times \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ are random functions. Recall that the modified function is denoted by LR''_4. In addition, recall that LR'''_4 is the composition of LR_2 with a random function $\mathsf{RF} : \{0,1\}^n \to \{0,1\}^n$ (see Fig. 4.3).

Then, by applying Proposition 5 twice, we can show that

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4,\mathsf{LR}''_4}(q) \leq O\left(\sqrt{\frac{q^3}{2^{n/2}}}\right) \tag{4.58}$$

holds. In addition,

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}''_4,\mathsf{LR}'''_4}(q) \leq O\left(\sqrt{\frac{q^3}{2^{n/2}}}\right) \tag{4.59}$$

follows from Proposition 7, and

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}'''_4,\mathsf{RF}}(q) = 0 \tag{4.60}$$

holds since LR_2 is a permutation.

From Theorem 5, (4.58), (4.59), and (4.60), we have

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4,\mathsf{RP}}(q) \leq \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}_4,\mathsf{LR}''_4}(q) + \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}''_4,\mathsf{LR}'''_4}(q) + \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LR}'''_4,\mathsf{RF}}(q) + \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{RF},\mathsf{RP}}(q) \leq O\left(\sqrt{\frac{q^3}{2^{n/2}}}\right),$$

which completes the proof of the theorem. □

4.3 Matching Upper Bound

Here we show that the query lower bound derived from Theorem 9 is tight by showing the matching upper bound (i.e., we show the latter half of Theorem 7). Again, we consider the case that all round functions of LR_4 are truly random functions, and show the following theorem.

Theorem 10. *A quantum algorithm $\mathcal{A}$ exists that makes $O(2^{n/6})$ quantum queries and satisfies $\mathbf{Adv}^{\mathrm{qPRP}}_{\mathsf{LR}_4}(\mathcal{A}) = \Omega(1)$.*

Proof intuition. Intuitively, our distinguishing attack is just a quantum version of a classical collision-finding-based distinguishing attack [Pat91]. A classical attack distinguishes LR_4 from a random permutation by finding a collision of a function that takes values in $\{0,1\}^{n/2}$, which requires $O(\sqrt{2^{n/2}}) = O(2^{n/4})$ queries in the quantum setting. However, finding a collision of the function requires only $O(\sqrt[3]{2^{n/2}}) = O(2^{n/6})$ queries in the quantum setting, which enables us to build a $O(2^{n/6})$-query quantum distinguisher. (Note that we can generally find a collision of random functions from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$ with $O(\sqrt[3]{2^{n/2}}) = O(2^{n/6})$ quantum queries [Zha15].)

4.3.1 Proof of Theorem 10

First, we describe an overview of a classical attack [Pat91]. Let us denote the composition of two independent random functions from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$ by $\mathsf{RF} \circ \mathsf{RF}$.

4.3.1.1 An Overview of a Classical Attack

Suppose that we are given an oracle access to O, which is either the 4-round Luby-Rackoff construction LR_4 or a random permutation from $\{0,1\}^n$ to $\{0,1\}^n$. Let us define a function $G^O : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ that depends on O by

$$G^O(x) := \left(O(0^{n/2}, x)\right)_R \oplus x, \tag{4.61}$$

where $\left(O(0^{n/2}, x)\right)_R$ is the right half $n/2$ bits of $O(0^{n/2}, x)$. We can implement G^O by making $O(1)$ queries.

When O is the 4-round Luby-Rackoff construction LR_4, we have that $G^O(x) = f_3(f_2(x \oplus f_1(0^{n/2}))) \oplus f_1(0^{n/2})$ holds. Thus, if all round functions of LR_4 are truly random functions, the function distribution of G^O will be the same as that of the composition of two independent random functions $\mathsf{RF} \circ \mathsf{RF}$. On the other hand, when O is a random permutation from $\{0,1\}^n$ to $\{0,1\}^n$, the function distribution of G^O will be almost the same as that of the truly random function RF from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$.

Since $\mathsf{RF} \circ \mathsf{RF}$ has twice as many collisions as RF, we can distinguish LR_4 from a truly random permutation by making $O((2^{n/2})^{1/2}) = O(2^{n/4})$ queries to G^O.

4.3.1.2 Conversion of the Classical Attack to a Quantum Attack

Next, we explain how to convert the classical attack above into a quantum attack that makes $O(2^{n/6})$ quantum queries and prove Theorem 10. The following lemma is crucial. It shows that we can distinguish $\mathsf{RF} \circ \mathsf{RF}$ from RF by making $O((2^{n/2})^{1/3}) = O(2^{n/6})$ quantum queries.

Lemma 7. *Let us denote the composition of two independent random functions from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$ by $\mathsf{RF} \circ \mathsf{RF}$. Then, a quantum algorithm $\mathcal{B}$ exists that makes $O(2^{n/6})$ quantum queries and satisfies $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{B}) = \Omega(1)$. That is, an algorithm exists that distinguishes $\mathsf{RF} \circ \mathsf{RF}$ from a random function with a constant probability, by making $O(2^{n/6})$ quantum queries.*

Proof. We use the following fact that is shown by Ambainis [Amb04, Amb07].

Fact 1 ([Amb04, Amb07]). *Let X and Y be finite sets, and $F : X \to Y$ be a function. Then there is a quantum algorithm that judges if distinct elements $x_1, x_2 \in X$ exist such that $F(x_1) = F(x_2)$ with bounded error by making $O(|X|^{2/3})$ quantum queries to F.*

Let $[N] \subset \{0,1\}^{n/2}$ denote the subset $\{0, 1, \ldots, N-1\}$ for each integer $1 \le N \le 2^{n/2}$. By using the above fact, we can deduce that for $1 \le N \le 2^{n/2}$ a quantum algorithm $\mathcal{D}_N$ exists such that, given oracle access to a function $F : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$, it outputs 1 if distinct elements $x_1, x_2 \in [N]$ exist such that $F(x_1) = F(x_2)$, and it outputs 0 otherwise, with an error that is smaller than $1/30$, by making $O(|N|^{2/3})$ quantum queries. (We can make such $\mathcal{D}_N$ by iteratively running Ambainis' algorithm $O(1)$ times for $F|_{[N]} : [N] \to \{0,1\}^{n/2}$, which is the restriction of F to $[N]$.)

Here we give an analysis of the qPRF advantage of $\mathcal{D}_N$ on $\mathsf{RF}\circ\mathsf{RF}$, for each N. For a function $F : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ and a subset $Z \subseteq \{0,1\}^{n/2}$, let coll^F_Z denote the event that F has a collision in Z, i.e., there are distinct $x_1, x_2 \in Z$ such that $F(x_1) = F(x_2)$. Then, we have that

$$\Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right] = \left(1 - \frac{1}{2^{n/2}}\right) \cdot \left(1 - \frac{2}{2^{n/2}}\right) \cdots \left(1 - \frac{N-1}{2^{n/2}}\right) = \prod_{j=1}^{N-1}\left(1 - \frac{j}{2^{n/2}}\right) \tag{4.62}$$

holds, where F is chosen from $\mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$ uniformly at random. In addition, when F_1 and F_2 are chosen from $\mathsf{Func}(\{0,1\}^{n/2}, \{0,1\}^{n/2})$ uniformly at random, we have that

$$\Pr_{F_1,F_2}\left[\neg\mathsf{coll}^{F_2\circ F_1}_{[N]}\right] = \Pr_{F_2}\left[\neg\mathsf{coll}^{F_2}_{F_1([N])}\middle|\neg\mathsf{coll}^{F_1}_{[N]}\right] \cdot \Pr_{F_1}\left[\neg\mathsf{coll}^{F_1}_{[N]}\right] = \left(\Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right)^2. \tag{4.63}$$

Now we have that

$$\begin{aligned}\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{D}_N) = \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{RF},\mathsf{RF}\circ\mathsf{RF}}(\mathcal{D}_N) &= \left|\Pr_F\left[\mathcal{D}_N^F() \to 1\right] - \Pr_{F_1,F_2}\left[\mathcal{D}_N^{F_2\circ F_1}() \to 1\right]\right| \\ &\ge \left|\Pr_F\left[\mathsf{coll}^F_{[N]}\right] - \Pr_{F_1,F_2}\left[\mathsf{coll}^{F_2\circ F_1}_{[N]}\right]\right| - \frac{2}{30},\end{aligned} \tag{4.64}$$

where we used the property that the error of $\mathcal{D}_N$ is smaller than $1/30$. In addition, from (4.63), it follows that

$$\left|\Pr_F\left[\mathsf{coll}^F_{[N]}\right] - \Pr_{F_1,F_2}\left[\mathsf{coll}^{F_2\circ F_1}_{[N]}\right]\right| = \Pr_{F_1,F_2}\left[\mathsf{coll}^{F_2\circ F_1}_{[N]}\right] - \Pr_F\left[\mathsf{coll}^F_{[N]}\right] = \left(1 - \left(\Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right)^2\right) - \left(1 - \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right)$$
$$= \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\left(1 - \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right) \tag{4.65}$$

holds. Therefore, we have that

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{D}_N) \geq \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\left(1 - \Pr_F\left[\neg\mathsf{coll}^F_{[N]}\right]\right) - \frac{2}{30} \tag{4.66}$$

holds. Now we show the following claim.

Claim 5. *There exists a parameter N_0 that is in $O(2^{n/4})$, and*

$$\frac{3}{5} \geq \prod_{j=1}^{N_0-1}\left(1 - \frac{j}{2^{n/2}}\right) \geq \frac{1}{5} \tag{4.67}$$

holds for sufficiently large n.

Proof. First, let us denote $p_N := \prod_{j=1}^{N-1}\left(1 - \frac{j}{2^{n/2}}\right)$. For each $1 \leq N \leq 2^{n/2}$, we have that

$$\prod_{j=1}^{N-1}\left(1 - \frac{j}{2^{n/2}}\right) \geq \left(1 - \frac{N}{2^{n/2}}\right)^N = \left(\left(1 - \frac{N}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N}}\right)^{-\frac{N^2}{2^{n/2}}} \tag{4.68}$$

holds. In addition,

$$\prod_{j=1}^{N-1}\left(1 - \frac{j}{2^{n/2}}\right) \leq \prod_{j=1}^{N-1}\left(e^{-\frac{j}{2^{n/2}}}\right) = e^{-\frac{N(N-1)}{2\cdot 2^{n/2}}} \tag{4.69}$$

holds. Thus

$$e^{-\frac{N(N-1)}{2\cdot 2^{n/2}}} \geq p_N \geq \left(\left(1 - \frac{N}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N}}\right)^{-\frac{N^2}{2^{n/2}}} \tag{4.70}$$

holds.

Next, let $N_0 := 2^{n/4}\cdot\sqrt{2\log 2}$. Then

$$e^{-\frac{N_0(N_0-1)}{2\cdot 2^{n/2}}} = e^{-\frac{N_0\cdot N_0}{2\cdot 2^{n/2}}} + \left(e^{-\frac{N_0(N_0-1)}{2\cdot 2^{n/2}}} - e^{-\frac{N_0\cdot N_0}{2\cdot 2^{n/2}}}\right) = \frac{1}{2} + \left(\left(\frac{1}{2}\right)^{\frac{N_0-1}{N_0}} - \frac{1}{2}\right) \tag{4.71}$$

holds, and thus $e^{-\frac{N_0(N_0-1)}{2\cdot 2^{n/2}}} \leq 3/5$ holds for sufficiently large n. In addition, since the function $f(x) = (1-x)^{-1/x}$ increases as x increases for $0 < x < 1$ and $\lim_{x\to+0} f(x) = e$ holds, we have that

$$\left(1 - \frac{N_0}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N_0}} \leq e + \frac{1}{10} \tag{4.72}$$

holds for sufficiently large n. Thus

$$\left(\left(1 - \frac{N_0}{2^{n/2}}\right)^{-\frac{2^{n/2}}{N_0}}\right)^{-\frac{N_0^2}{2^{n/2}}} \geq \left(e + \frac{1}{10}\right)^{-\frac{N_0^2}{2^{n/2}}} = \left(e + \frac{1}{10}\right)^{-2\log 2} \geq \frac{1}{5} \tag{4.73}$$

holds for sufficiently large n.

Therefore, for $N_0 := 2^{n/4}\cdot\sqrt{2\log 2}$,

$$\frac{3}{5} \geq p_{N_0} \geq \frac{1}{5} \tag{4.74}$$

holds for sufficiently large n. Hence the claim follows. □

From the above claim and (4.62), a parameter N_0 exists that is in $O(2^{n/4})$, and

$$\frac{3}{5} \geq \Pr_F\left[\neg\mathsf{coll}^F_{[N_0]}\right] \geq \frac{1}{5} \tag{4.75}$$

holds for sufficiently large n. Hence, from (4.64) we have that

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{D}_{N_0}) \geq \frac{1}{5}\left(1-\frac{3}{5}\right) - \frac{2}{30} = \frac{1}{75} \geq \Omega(1). \tag{4.76}$$

Therefore, if we let $\mathcal{B} := \mathcal{D}_{N_0}$, this $\mathcal{B}$ satisfies the claim of the lemma, since (4.76) holds and $\mathcal{D}_{N_0}$ makes at most $O((N_0)^{2/3}) = O((2^{n/4})^{2/3}) = O(2^{n/6})$ quantum queries. □

Next we show the following proposition.

Proposition 9. *A quantum algorithm $\mathcal{A}$ exists that makes $O(2^{n/6})$ quantum queries and satisfies $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{LR}_4}(\mathcal{A}) = \Omega(1)$.*

Proof. Suppose that we are given an oracle access to O, which is either the 4-round Luby-Rackoff construction LR_4 or a random function from $\{0,1\}^n$ to $\{0,1\}^n$. Recall that the function $G^O : \{0,1\}^{n/2} \to \{0,1\}^{n/2}$ is defined by

$$G^O(x) := \left(O(0^{n/2}, x)\right)_R \oplus x, \tag{4.77}$$

where $\left(O(0^{n/2}, x)\right)_R$ is the right half $n/2$ bits of $O(0^{n/2}, x)$. We can implement a quantum circuit that computes G^O by making $O(1)$ queries.[4]

Now we define a quantum algorithm $\mathcal{A}$ as the following three-step procedure.

1. Let $\mathcal{B}$ be the same algorithm as in Lemma 7.
2. Run $\mathcal{B}$ relative to G^O.
3. If $\mathcal{B}$ returns 1, output 1. If $\mathcal{B}$ returns 0, output 0.

Here we analyze $\mathcal{A}$. When O is the 4-round Luby-Rackoff construction LR_4, we have that $G^O(x) = f_3(f_2(x \oplus f_1(0^{n/2}))) \oplus f_1(0^{n/2})$ holds. Since we are considering the case that all round functions of LR_4 are truly random functions, the function distribution of G^O will be the same as that of $\mathsf{RF}\circ\mathsf{RF}$. On the other hand, when O is a random function from $\{0,1\}^n$ to $\{0,1\}^n$, the function distribution of G^O will be the same as that of the truly random function from $\{0,1\}^{n/2}$ to $\{0,1\}^{n/2}$. Thus, from Lemma 7 we have that

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{LR}_4}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RF}\circ\mathsf{RF}}(\mathcal{B}) = \Omega(1) \tag{4.78}$$

holds. In addition, since $\mathcal{B}$ makes at most $O(2^{n/6})$ quantum queries and G makes only $O(1)$ queries to O, $\mathcal{A}$ makes at most $O(2^{n/6})$ quantum queries. Therefore the claim of the proposition holds. □

Finally we prove Theorem 10.

Proof of Theorem 10. Let $\mathcal{A}$ be the same algorithm as in Proposition 9. Then, from Proposition 9 it follows that

$$\mathbf{Adv}^{\mathrm{qPRP}}_{\mathsf{LR}_4}(\mathcal{A}) \geq \mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{LR}_4}(\mathcal{A}) - \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{RP},\mathsf{RF}}(\mathcal{A}) \geq \Omega(1) - O(1/2^{n/2}) = \Omega(1), \tag{4.79}$$

where we used the fact that, for any quantum adversary $\mathcal{A}'$ that makes at most q queries, the distinguishing advantage $\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{RP},\mathsf{RF}}(\mathcal{A}')$ is upper bounded by $O(q^3/2^n)$ for a random function and a random permutation from $\{0,1\}^n$ to $\{0,1\}^n$ (see Theorem 5). Thus the claim of the theorem holds. □

[4]Here we have to truncate O's outputs by using a technique observed in [HS18].

Chapter 5

Provably Quantum-Secure TBC

This chapter shows a new construction LRWQ that converts quantum-secure block ciphers into quantum-secure tweakable block ciphers. The result of this chapter is significant to understand (post-)quantum security of symmetric-key cryptography mainly from the theoretical perspective. Since Kaplan et al. showed the efficient quantum attack on the LRW construction [KLLN16a], the problem of whether it is possible to make a quantum-secure TBC based on a qPRP has been unresolved. This problem is of theoretical interest because TBCs play important roles to build efficient symmetric-key schemes such as MACs and authenticated encryption schemes in the classical setting. This chapter solves the problem by showing the new construction LRWQ is secure. Together with the results of Chapter 4, we can deduce that a quantum-secure TBC exists if a qPRF exists. See also Section 1.3 for an overview of the result, and Section 1.7 for the relationship of the results in this chapter with those in other chapters.

Section 5.1 reviews previous constructions and describes the new construction. Section 5.2 provides security proof of the construction.

5.1 A Quantum-Secure TBC

Since our construction is a variant of the LRW constructions [LRW02], we first review them before introducing ours.

5.1.1 The LRW Constructions

Liskov, Rivest, and Wagner introduced constructions that convert (classically) secure block ciphers into (classically) secure tweakable block ciphers, which are called the LRW constructions [LRW02].

Let $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be a block cipher and h be an almost 2-xor-universal hash function. Then the first construction, which we denote by LRW1, is defined as

$$\mathsf{LRW1}[E]^T_K(M) = E_K(E_K(M) \oplus T).$$

The second construction, which we denote by LRW2, is defined as

$$\mathsf{LRW2}[E]^T_{(K,h)}(M) = E_K(M \oplus h(T)) \oplus h(T),$$

where h is a part of the key. See Fig. 5.1[1].

Roughly speaking, both LRW1 and LRW2 are shown to be secure up to about $2^{n/2}$ queries (if h is a $1/2^n$-almost 2-xor-universal hash function) in the classical setting. LRW2 is also proven to be secure even if the decryption oracle is available to adversaries (That is, LRW2 is a tweakable strong pseudorandom permutation. LRW1 is not a tweakable strong pseudorandom permutation since it is broken if the decryption oracle is available).

In the quantum setting, however, Kaplan et al. showed that LRW2 can be distinguished from a tweakable random permutation in polynomial time (in n) if quantum queries to keyed oracles are allowed [KLLN16a].

An overview of their attack is as follows: Choose two tweaks $T \neq T'$ and define a function F^O by $F^O(M) := O(T, M) \oplus O(T', M)$, where O is a quantum oracle such that $O = \widetilde{\mathsf{RP}}$ or $O = \mathsf{LRW2}$. Then, we can show that $F^O(M \oplus s) = F^O(M)$ holds for $s := h(T) \oplus h(T')$ and all M if $O = \mathsf{LRW2}$, which implies that F^O is a periodic function, but F^O is far from periodic when $O = \widetilde{\mathsf{RP}}$. Therefore, we can distinguish LRW2 from $\widetilde{\mathsf{RP}}$ in polynomial time by using Simon's period finding quantum algorithm [Sim94, Sim97].

[1] We use the terms LRW1 and LRW2 following previous works [LST12, LS13].

Figure 5.1: The LRW constructions. LRW1 is depicted on the left, and LRW2 is depicted on the right.

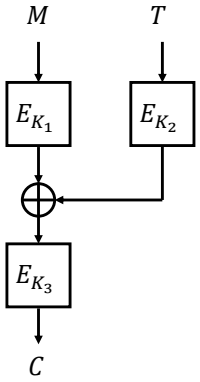


Figure 5.2: Specification of LRWQ$[E]$.

Similarly, we can distinguish LRW1 from a tweakable random permutation in polynomial time with Simon's algorithm: For LRW1, we choose two messages $M \neq M'$, define a function G^O by $G^O(T) = O(T, M) \oplus O(T, M')$, and apply Simon's quantum algorithm on G^O instead of F^O. When $O = \mathsf{LRW1}$, the function G^O has the period $E_K(M) \oplus E_K(M')$. We see that the attack on LRW1 works with the same reasoning as Kaplan et al.'s attack on LRW2 works.

Note that the attack on LRW1 implies that we can efficiently find a collision for the function $\mathsf{LRW1}[E]_K^{(\cdot)}(\cdot) : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ in the quantum setting. If we can efficiently recover the value $E_K(M) \oplus E_K(M')$ and set $T' := T \oplus E_K(M) \oplus E_K(M')$, then $\mathsf{LRW1}[E]_K^T(M) = \mathsf{LRW1}[E]_K^{T'}(M')$ holds. Finding such a collision by polynomial-time CPAs is hard in the classical setting.

5.1.2 LRWQ: A Quantum-Secure Construction

We next present our construction, LRWQ, which is a three-key block-cipher based tweakable block cipher. If the block length of the underlying block cipher is n, both the block and tweak lengths of LRWQ become n.

Let E be an n-bit block cipher with k-bit keys. Then the tweakable block cipher $\mathsf{LRWQ}[E] : \{0,1\}^{3k} \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ is defined as

$$\mathsf{LRWQ}[E]^T_{(K_1,K_2,K_3)}(M) = E_{K_3}(E_{K_1}(M) \oplus E_{K_2}(T)).$$

See Fig. 5.2. LRWQ is constructed based on LRW1. To prevent the quantum polynomial time attack in Section 5.1.1, tweak is encrypted before added to $E_{K_1}(M)$. This works since intuitively, it is hard even for quantum adversaries to find (M, T) and (M', T') such that the corresponding outputs collide, i.e., $\mathsf{LRWQ}[E]^T_{(K_1,K_2,K_3)}(M) = \mathsf{LRWQ}[E]^{T'}_{(K_1,K_2,K_3)}(M')$ holds.

Unlike the classical constructions LRW1 and LRW2, as we will show in Section 5.2, LRWQ is secure against quantum attacks when it is instantiated with n-bit block ciphers that are secure against quantum attacks. LRWQ is the *first* mode of block ciphers to build a tweakable block cipher that is provably secure against quantum attacks.

5.1.2.1 Classical Security Analysis

Before going into the analysis in the quantum setting, we show that LRWQ is a secure tweakable block cipher in the classical setting against chosen plaintext attacks up to $O(2^{n/2})$ queries, and the security bound is tight. In addition, we show that LRWQ is broken in time $O(1)$ only with $O(1)$ queries if the decryption oracle is available (i.e., LRWQ is not a tweakable strong pseudorandom permutation), even in the classical setting. Define the distinguishing advantage $\mathbf{Adv}^{\mathrm{dist}}$, the pseudorandom permutation advantage $\mathbf{Adv}^{\mathrm{PRP}}$, and the tweakable pseudorandom permutation advantage $\mathbf{Adv}^{\widetilde{\mathrm{PRP}}}$ for classical adversaries in the same way as we did for quantum adversaries. Then the following proposition holds.

Proposition 10. *Let $\mathcal{A}$ be a classical adversary that makes at most q queries and runs in time τ. Then, there exist three classical adversaries $\mathcal{B}_1$, $\mathcal{B}_2$, and $\mathcal{B}_3$ that make at most q queries and run in time $\tilde{O}(\tau + q)$ such that*

$$\mathbf{Adv}^{\widetilde{\mathrm{PRP}}}_{\mathsf{LRWQ}[E]}(\mathcal{A}) \leq \sum_{i=1,2,3} \mathbf{Adv}^{\mathrm{PRP}}_{E}(\mathcal{B}_i) + O\left(\frac{q^2}{2^n}\right) \tag{5.1}$$

holds. In addition, there exists a classical algorithm C that makes $O(2^{n/2})$ queries and runs in time $\tilde{O}(2^{n/2})$ such that $\mathbf{Adv}^{\widetilde{\mathrm{PRP}}}_{\mathsf{LRWQ}[E]}(C) = \Theta(1)$. If the decryption oracle is also available to adversaries, there exists an algorithm C' that distinguishes $\mathsf{LRWQ}[E]$ from $\widetilde{\mathsf{RP}}$ in time $\tilde{O}(1)$ by making only $O(1)$ queries with a constant probability.

This proposition can be shown in a straightforward manner, but we give a proof intuition below.

First, we give a proof intuition for (5.1). When E is an ideally random block cipher, $\mathbf{Adv}^{\widetilde{\mathrm{PRP}}}_{\mathsf{LRW1}[E]}(\mathcal{A})$ is upper bounded by $O(q^2/2^n)$, as shown by Liskov, Rivest, and Wagner (See Theorem 1 of [LRW02]). Let $\mathsf{LRW1}'[E]$ be the tweakable block cipher defined as $\mathsf{LRW1}'[E]((K_1, K_3), T, M) := E_{K_3}(E_{K_1}(M) \oplus T)$ (i.e., $\mathsf{LRW1}'$ is a two-key version of LRW1). Then, intuitively, $\mathsf{LRW1}'[E]$ is harder to distinguish from $\widetilde{\mathsf{RP}}$ (a tweakable random permutation) than to distinguish $\mathsf{LRW1}[E]$ from $\widetilde{\mathsf{RP}}$, but easier to distinguish than $\mathsf{LRWQ}[E]$. Thus, roughly speaking, $\mathbf{Adv}^{\widetilde{\mathrm{PRP}}}_{\mathsf{LRWQ}[E]}(\mathcal{A}) \leq \mathbf{Adv}^{\widetilde{\mathrm{PRP}}}_{\mathsf{LRW1}'[E]}(\mathcal{A}) \leq \mathbf{Adv}^{\widetilde{\mathrm{PRP}}}_{\mathsf{LRW1}[E]}(\mathcal{A}) \leq O(q^2/2^n)$ holds, which proves (5.1) when E is an ideally random block cipher. It follows from standard hybrid arguments that (5.1) also holds for the case that E is not necessarily an ideally random block cipher. (See also the proof of Proposition 13. In the classical setting, a random permutation can efficiently be simulated by lazy sampling.)

Second, we show the existence of an algorithm C in Proposition 10. Let $\mathcal{O}$ be the encryption oracle, which is either $\mathsf{LRWQ}[E]$ or a tweakable random permutation $\widetilde{\mathsf{RP}}$. Let C be a classical algorithm that runs the following procedure: First, find a pair (M, T) and (M', T') such that $M \neq M' \wedge T \neq T'$ and $\mathcal{O}(T, M) = \mathcal{O}(T', M')$ by querying random elements to $\mathcal{O}$, and store the answers in a list. If such a pair is not found after making about $2^{n/2}$ queries, stop and output 0. Second, check whether $\mathcal{O}(T', M) = \mathcal{O}(T, M')$ holds (which can be done in time $\tilde{O}(1)$ by making $O(1)$ queries). Finally, output 1 if $\mathcal{O}(T', M) = \mathcal{O}(T, M')$, and output 0 if $\mathcal{O}(T', M) \neq \mathcal{O}(T, M')$. Then this algorithm C runs in time $\tilde{O}(2^{n/2})$ and makes at most $O(2^{n/2})$ queries. It is easy to see that C outputs 1 with an overwhelming probability when $\mathcal{O} = \mathsf{LRWQ}[E]$ and outputs 0 with an overwhelming probability when $\mathcal{O} = \widetilde{\mathsf{RP}}$.

Third, we show that there exists an efficient classical chosen ciphertext attack on LRWQ. The algorithm C in the previous paragraph finds a pair $((M, T), (M', T'))$ such that $M \neq M' \wedge T \neq T'$ and $\mathcal{O}(T, M) = \mathcal{O}(T', M')$ by just querying random elements to the encryption oracle, which costs $O(2^{n/2})$ queries. However, if the decryption oracle is available, we can modify C so that it can find such a pair with only $O(1)$ queries as follows: First, query (T, M) to the encryption oracle for some tweak T and plaintext M to get the answer C, and then query (T', C) to the decryption oracle for another tweak T' to obtain the answer M'. Then the pair $((M, T), (M', T'))$ satisfies $M \neq M' \wedge T \neq T'$ with an overwhelming probability, and $\mathcal{O}(T, M) = \mathcal{O}(T', M') = C$ holds. Let C' be the algorithm that is defined in the same way as C except that it finds such a pair $((M, T), (M', T'))$ by only making $O(1)$ queries as above. This modified algorithm C' runs in time $\tilde{O}(1)$ and distinguishes LRWQ from $\widetilde{\mathsf{RP}}$ by making only $O(1)$ queries with an overwhelming probability. Therefore, our construction LRWQ is broken (distinguished from a tweakable random permutation) in time $\tilde{O}(1)$ with only $O(1)$ queries, if the decryption oracle is available.

5.2 q$\widetilde{\mathsf{PRP}}$ Security Proof for LRWQ

Below, we give q$\widetilde{\mathsf{PRP}}$ security proof for LRWQ. The goal is to show the following theorem.

Theorem 11. *Let $\mathcal{A}$ be a quantum algorithm that runs in time τ, makes at most q quantum queries, and uses Q qubits. Then there exist quantum algorithms $\mathcal{B}_1$, $\mathcal{B}_2$, and $\mathcal{B}_3$ that make at most $O(q)$ quantum queries and run in time τ_1, τ_2,*

and τ_3, respectively, such that

$$\mathbf{Adv}^{\widetilde{\mathsf{qPRP}}}_{\mathsf{LRWQ}[E]}(\mathcal{A}) \leq \sum_{1\leq i\leq 3} \mathbf{Adv}^{\mathrm{qPRP}}_{E}(\mathcal{B}_i) + O\left(\sqrt{\frac{q^6}{2^n}}\right)$$

holds, where τ_1 and τ_2 are in $\tilde{O}(\tau + q^2)$, τ_3 is in $\tilde{O}(\tau + q)$, and $\tilde{O}$ suppresses factors of polynomials in n. $\mathcal{B}_1$ and $\mathcal{B}_2$ use $\tilde{O}(Q + q)$ qubits, and $\mathcal{B}_3$ uses $\tilde{O}(Q)$ qubits.

5.2.1 Indistinguishability of Tweakable Random Permutation and Random Function

Before proving Theorem 11, we show the indistinguishability of a tweakable random permutation and a random function. Let $\widetilde{\mathsf{RP}} : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a tweakable random permutation, i.e., $\widetilde{\mathsf{RP}}(t,\cdot) : \{0,1\}^n \to \{0,1\}^n$ is a random permutation for each $t \in \{0,1\}^n$. In addition, let $\mathsf{RF} : \{0,1\}^n \times \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$ be a random function. The goal of this subsection is to show the following proposition.

Proposition 11. *Let $\mathcal{A}$ be a quantum algorithm that makes at most q quantum queries. Then,*

$$\mathbf{Adv}^{\mathrm{dist}}_{\widetilde{\mathsf{RP}},\mathsf{RF}}(\mathcal{A}) \leq O\left(\sqrt{\frac{q^6}{2^n}}\right) \tag{5.2}$$

holds.

Let O_1 and O_2 be oracles of functions $f_1, f_2 : X \to Y$ that are chosen in accordance with distributions D_1 and D_2 on $\mathsf{Func}(X,Y)$, respectively. In addition, let D_1^Z be the distribution on $\mathsf{Func}(Z \times X, Y)$ such that, if we sample a function F in accordance with D_1^Z, $F(z,\cdot) \in \mathsf{Func}(X,Y)$ is sampled in accordance with D_1 independently for each $z \in Z$. Let D_2^Z be the distribution which is defined from D_2 in the same way. Define O_1^Z and O_2^Z to be the oracles of functions $F_1, F_2 : Z \times X \to Y$ that are chosen in accordance with distributions D_1^Z and D_2^Z, respectively. Then the following proposition, which was first essentially shown by Zhandry [Zha12a] and later generalized by Song and Yun [SY17], holds. Note that, in the following proposition, we consider (quantum) information theoretic adversaries and do not care whether they are efficient quantum algorithms.

Proposition 12 (Theorem 1.1 in [Zha12a], Theorem 3.3 in [SY17])**.** *For any quantum query adversary $\mathcal{A}$ that makes at most q quantum queries, there exists an adversary $\mathcal{B}$ that makes $2q$ quantum queries and satisfies*

$$\mathbf{Adv}^{\mathrm{dist}}_{O_1^Z,O_2^Z}(\mathcal{A}) \leq 12\sqrt{q^3 \cdot \mathbf{Adv}^{\mathrm{dist}}_{O_1,O_2}(\mathcal{B})}. \tag{5.3}$$

Combining Proposition 12 and Theorem 5, we can prove Proposition 11 as follows.

Proof of Proposition 11. Let X, Y, and Z be $\{0,1\}^n$. In addition, let O_1, O_2 denote the oracle of a random function and a random permutation (from $\{0,1\}^n$ to $\{0,1\}^n$), respectively. Then O_1^Z and O_2^Z become the oracles of $\widetilde{\mathsf{RP}}$ and RF, respectively. Then, from Proposition 12 and Theorem 5, it follows that a quantum adversary $\mathcal{B}$ exists that makes at most $2q$ quantum queries and satisfies

$$\mathbf{Adv}^{\mathrm{dist}}_{O_1^Z,O_2^Z}(\mathcal{A}) \leq 12\sqrt{q^3 \cdot \mathbf{Adv}^{\mathrm{dist}}_{O_1,O_2}(\mathcal{B})} = 12\sqrt{q^3 \cdot \mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{RP}}(\mathcal{B})} \leq O\left(\sqrt{q^6/2^n}\right), \tag{5.4}$$

which completes the proof. □

Remark 16. *The upper bound given in Proposition 11 is much larger than that in Theorem 5. We expect that the bound in* (5.2) *is not tight, while a better provable security bound is not known.*

5.2.2 Notations, Definitions, and Some Basic Properties

Here we introduce notations, definitions, and basic properties that are used to prove Theorem 11. Let $f_0, f_1 : \{0,1\}^n \to \{0,1\}^n$ denote random functions. Let $f_{\mathsf{small}} : \{0,1\}^n \to \{0,1\}^n$ and $f_{\mathsf{big}} : \{0,1\}^{3n} \to \{0,1\}^n$ also be random functions. Let us define three functions $\mathsf{FSum}, \mathsf{FSF}_{\mathrm{small}}, \mathsf{FSF}_{\mathrm{big}} : \{0,1\}^{2n} \to \{0,1\}^n$ by

$$\begin{aligned}
\mathsf{FSum}(M,T) &:= f_0(M) \oplus f_1(T),\\
\mathsf{FSF}_{\mathrm{small}}(M,T) &:= f_{\mathsf{small}}\left(\mathsf{FSum}(M,T)\right),\\
\mathsf{FSF}_{\mathrm{big}}(M,T) &:= f_{\mathsf{big}}\left(M,T,\mathsf{FSum}(M,T)\right).
\end{aligned}$$

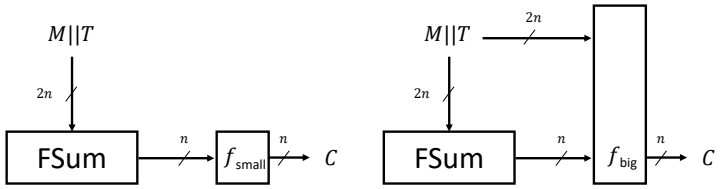


Figure 5.3: Comparison of $\mathsf{FSF}_{\text{small}}(M,T)$ and $\mathsf{FSF}_{\text{big}}(M,T)$.

See Fig. 5.3 for figures of FSum, $\mathsf{FSF}_{\text{small}}$, and $\mathsf{FSF}_{\text{big}}$. Note that $\mathsf{FSF}_{\text{small}}$ is defined in the same way as $\mathsf{LRWQ}[E]$ except that it uses random functions instead of block ciphers. $\mathsf{FSF}_{\text{big}}$ is completely indistinguishable from a random function since f_{big} is a random function.

Reduction to qPRF *Security of* $\mathsf{FSF}_{\text{small}}$. The following proposition shows that the problem of proving $\widetilde{\text{qPRP}}$ security of $\mathsf{LRWQ}[E]$ can be reduced to the problem of proving qPRF security of $\mathsf{FSF}_{\text{small}}$ when the underlying block cipher is a secure qPRP.

Proposition 13. *Let $\mathcal{A}$ be a quantum algorithm that runs in time τ, makes at most q quantum queries, and uses Q qubits. Then there exist quantum algorithms $\mathcal{B}_1$, $\mathcal{B}_2$, and $\mathcal{B}_3$ that make at most $O(q)$ quantum queries and run in time τ_1, τ_2, and τ_3, respectively, such that*

$$\mathbf{Adv}^{\widetilde{\text{qPRP}}}_{\mathsf{LRWQ}[E]}(\mathcal{A}) \le \sum_{1\le i\le 3} \mathbf{Adv}^{\text{qPRP}}_{E}(\mathcal{B}_i) + \mathbf{Adv}^{\text{qPRF}}_{\mathsf{FSF}_{\text{small}}}(\mathcal{A}) + O\left(\sqrt{\frac{q^6}{2^n}}\right)$$

holds, where τ_1 and τ_2 are in $\tilde{O}(\tau + q^2)$, τ_3 is in $\tilde{O}(\tau + q)$, and $\tilde{O}$ suppresses factors of polynomials in n. $\mathcal{B}_1$ and $\mathcal{B}_2$ use $\tilde{O}(Q + q)$ qubits, and $\mathcal{B}_3$ uses $\tilde{O}(Q)$ qubits.

Proof. Let $h_i : \{0,1\}^n \to \{0,1\}^n$ be E_{K_i} or RF_i, where RF_i is a random function, for $1 \le i \le 3$. Let $\mathsf{LRWQ}'[h_1,h_2,h_3]$ be the function that is the same as $\mathsf{LRWQ}[E]$ except that E_{K_i} is replaced with h_i for each i (if $h_i = E_{K_i}$ for all i, $\mathsf{LRWQ}'[h_1,h_2,h_3]$ is completely the same as $\mathsf{LRWQ}[E]$). Without loss of generality we assume that choosing a random key for E and encryption with E can be done in time $\tilde{O}(1)$ by using $\tilde{O}(1)$ qubits.

Suppose that we are given access to a quantum oracle O_3, which is either E_{K_3} (the key K_3 is chosen randomly) or a random function $\mathsf{RF}_3 : \{0,1\}^n \to \{0,1\}^n$. Then, we construct an algorithm $\mathcal{B}_3$ to distinguish E_{K_3} from RF_3 as follows: First, $\mathcal{B}_3$ chooses keys K_1 and K_2 for E uniformly at random. Then $\mathcal{B}_3$ runs $\mathcal{A}$, simulating the oracle of $\mathsf{LRWQ}'[E_{K_1},E_{K_2},E_{K_3}] = \mathsf{LRWQ}[E]$ or $\mathsf{LRWQ}'[E_{K_1},E_{K_2},\mathsf{RF}_3]$ by computing E_{K_1} and E_{K_2} by itself, and computing E_{K_3} or RF_3 by making queries to O_3. (If O_3 is E_{K_3}, then $\mathcal{B}_3$ perfectly simulates $\mathsf{LRWQ}[E]$. Otherwise $\mathcal{B}_3$ perfectly simulates $\mathsf{LRWQ}'[E_{K_1},E_{K_2},\mathsf{RF}_3]$.) Finally, $\mathcal{B}_3$ outputs what $\mathcal{A}$ outputs. Then $\mathcal{B}_3$ runs in time $\tilde{O}(\tau + q)$, makes at most $O(q)$ quantum queries to O_3, uses $\tilde{O}(Q)$ qubits, and

$$\mathbf{Adv}^{\text{dist}}_{\mathsf{LRWQ}[E],\mathsf{LRWQ}'[E_{K_1},E_{K_2},\mathsf{RF}_3]}(\mathcal{A}) = \mathbf{Adv}^{\text{qPRF}}_{E}(\mathcal{B}_3) \le \mathbf{Adv}^{\text{qPRP}}_{E}(\mathcal{B}_3) + O\left(\frac{q^3}{2^n}\right) \tag{5.5}$$

holds, where we used Theorem 5 for the last inequality.

Next, suppose that we are given access to a quantum oracle O_1, which is either E_{K_1} (the key K_1 is chosen randomly) or a random function $\mathsf{RF}_1 : \{0,1\}^n \to \{0,1\}^n$. Then, we construct an algorithm $\mathcal{B}_1$ to distinguish E_{K_1} from RF_1 as follows: $\mathcal{B}_1$ runs $\mathcal{A}$, simulating the oracle of $\mathsf{LRWQ}'[E_{K_1},E_{K_2},\mathsf{RF}_3]$ or $\mathsf{LRWQ}'[\mathsf{RF}_1,E_{K_2},\mathsf{RF}_3]$ by simulating RF_3 as in Corollary 1, choosing K_2 and computing E_{K_2} by itself, and computing E_{K_1} or RF_1 by making queries to O_1. (If O_1 is E_{K_1}, then $\mathcal{B}_1$ perfectly simulates $\mathsf{LRWQ}'[E_{K_1},E_{K_2},\mathsf{RF}_3]$. Otherwise $\mathcal{B}_1$ perfectly simulates $\mathsf{LRWQ}'[\mathsf{RF}_1,E_{K_2},\mathsf{RF}_3]$.) Finally, $\mathcal{B}_1$ outputs what $\mathcal{A}$ outputs. Since Corollary 1 holds, it follows that $\mathcal{B}_1$ runs in time $\tilde{O}(\tau + q^2)$, makes at most

$O(q)$ quantum queries to O_1, uses $\tilde{O}(Q+q)$ qubits, and

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LRWQ}'[E_{K_1},E_{K_2},\mathsf{RF}_3],\mathsf{LRWQ}'[\mathsf{RF}_1,E_{K_2},\mathsf{RF}_3]}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{qPRF}}_{E}(\mathcal{B}_1) \le \mathbf{Adv}^{\mathrm{qPRP}}_{E}(\mathcal{B}_1) + O\left(\frac{q^3}{2^n}\right) \tag{5.6}$$

holds. Similarly, we can show that there exists a quantum algorithm $\mathcal{B}_2$ that runs in time $\tilde{O}(\tau+q^2)$, makes at most $O(q)$ quantum queries, uses $\tilde{O}(Q+q)$ qubits, and

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{LRWQ}'[\mathsf{RF}_1,E_{K_2},\mathsf{RF}_3],\mathsf{LRWQ}'[\mathsf{RF}_1,\mathsf{RF}_2,\mathsf{RF}_3]}(\mathcal{A}) \le \mathbf{Adv}^{\mathrm{qPRP}}_{E}(\mathcal{B}_2) + O\left(\frac{q^3}{2^n}\right) \tag{5.7}$$

holds.

Since the distribution of the function $\mathsf{LRWQ}'[\mathsf{RF}_1,\mathsf{RF}_2,\mathsf{RF}_3]$ is the same as that of $\mathsf{FSF}_{\mathrm{small}}$,

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{LRWQ}'[\mathsf{RF}_1,\mathsf{RF}_2,\mathsf{RF}_3]}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{FSF}_{\mathrm{small}}}(\mathcal{A}) \tag{5.8}$$

follows. In addition,

$$\mathbf{Adv}^{\mathrm{dist}}_{\widetilde{\mathsf{RP}},\mathsf{RF}}(\mathcal{A}) \le O\left(\sqrt{\frac{q^6}{2^n}}\right) \tag{5.9}$$

follows from Proposition 11.

Therefore, the claim of the proposition follows from (5.5), (5.6), (5.7), (5.8), and (5.9). □

The most difficult part in the security proof for LRWQ is to show qPRF security of $\mathsf{FSF}_{\mathrm{small}}$, which is equivalent to showing indistinguishability of $\mathsf{FSF}_{\mathrm{small}}$ and $\mathsf{FSF}_{\mathrm{big}}$ since $\mathsf{FSF}_{\mathrm{big}}$ is completely indistinguishable from a random function, i.e., to show the following proposition.

Proposition 14. *For a quantum algorithm $\mathcal{A}$ that makes at most q quantum queries,*

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{FSF}_{\mathrm{small}}}(\mathcal{A}) \left(= \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{FSF}_{\mathrm{small}},\mathsf{FSF}_{\mathrm{big}}}\right) \le O\left(\sqrt{\frac{q^4}{2^n}}\right) \tag{5.10}$$

holds.

5.2.3 Review of How to Show Quantum Oracle Indistinguishability with RstOE

Proposition 14 is somewhat similar to Proposition 5 in that both of them claim a single oracle O_1 is indistinguishable from another oracle O_2, where O_1 and O_2 are the quantum oracles of functions that are made of random functions. Thus, to prove Proposition 14, we use the same proof strategy as that for Proposition 5. In what follows we review the proof strategy for Proposition 5. Note that this section focuses on quantum information-theoretic adversaries, and we model quantum algorithms as in Section 2.4.1. We first describe the proof strategy formally, and then explain some informal intuition behind it.

Goal. Suppose that there are functions $F^{f_1,\dots,f_r}, G^{g_1,\dots,g_s} : \mathcal{X} \to \mathcal{Y}$ that have access to functions $f_1,\dots,f_r$ and $g_1,\dots,g_s$ in a black-box manner, respectively. Our goal is to give an upper bound on the distinguishing advantage of an adversary $\mathcal{A}$ between $F^{f_1,\dots,f_r}$ and $G^{g_1,\dots,g_s}$ when each f_i and g_j are random functions.

Oracle implementations using RstOE. Below, we assume that elements in $\mathcal{X}$ and $\mathcal{Y}$ are encoded into m-bit strings and n-bit strings for some positive integers m and n, respectively.

When each f_i is a fixed function (but not a random function), let $O_F^{f_1,\dots,f_r}$ denote the quantum oracle of $F^{f_1,\dots,f_r}$. We assume that the unitary operator $O_F^{f_1,\dots,f_r}$ of the oracle $O_F^{f_1,\dots,f_r}$ is realized as a quantum circuit with oracle gates (that make queries to $f_1,\dots,f_r$) and suppose that ℓ ancilla qubits are used to compute F. The ancilla qubits are supposed to be $|0^\ell\rangle$ before and after each evaluation of F when $f_1,\dots,f_r$ are some fixed functions. That is, we assume that $O_F^{f_1,\dots,f_r}$ is a unitary operator such that $O_F^{f_1,\dots,f_r} : |x\rangle|y\rangle \otimes |0^\ell\rangle \mapsto |x\rangle|y \oplus F^{f_1,\dots,f_r}(x)\rangle \otimes |0^\ell\rangle$ holds, when each f_i is fixed.

When $f_1,\dots,f_r$ are random functions $\mathsf{RF}_1,\dots,\mathsf{RF}_r$, we assume that they are implemented by using the recording oracle with errors RstOE. We regard $O_F^{\mathsf{RF}_1,\dots,\mathsf{RF}_r}$ as the quantum oracle of which quantum states are combinations of (superposed) valid databases for $\mathsf{RF}_1,\dots,\mathsf{RF}_r$ and the ℓ ancilla qubits. Then, the joint quantum state of $\mathcal{A}$ and $O_F^{\mathsf{RF}_1,\dots,\mathsf{RF}_r}$ is described as

$$\sum_{u,\mathcal{DB}_F,\xi_\ell} a_{u,\mathcal{DB}_F,\xi_\ell} |u\rangle \otimes |\mathcal{DB}_F\rangle |\xi_\ell\rangle,$$

where u corresponds to $\mathcal{A}$'s state, each $\mathcal{DB}_F = (D_1, \ldots, D_r)$ denotes a (combined) database for $\mathsf{RF}_1, \ldots, \mathsf{RF}_r$, each ξ_ℓ is a classical ℓ-bit string, and $a_{u,\mathcal{DB}_F,\xi_\ell}$ satisfies $\sum_{u,\mathcal{DB}_F,\xi_\ell} |a_{u,\mathcal{DB}_F,\xi_\ell}|^2 = 1$. Below, we just write O_F instead of $O_F^{\mathsf{RF}_1,\ldots,\mathsf{RF}_r}$ for simplicity.

Similarly, when $g_1, \ldots, g_s$ are random functions $\mathsf{RF}'_1, \ldots, \mathsf{RF}'_s$, we assume that the quantum oracle O_G of $G^{\mathsf{RF}'_1,\ldots,\mathsf{RF}'_s}$ are implemented by using RstOE. We assume that O_G uses ℓ' ancilla qubits to compute G. We denote a (combined) database for $\mathsf{RF}'_1, \ldots, \mathsf{RF}'_s$ by $\mathcal{DB}_G := (D'_1, \ldots, D'_s)$, where D'_i is a valid database for each RF'_i.

Good and bad databases. Next, we classify valid databases for O_F and O_G into *good* and *bad* databases, which correspond to good and bad transcripts in classical security proofs. The important point is that the classification is done in such a way that there is a one-to-one correspondence between good databases for O_F and those for O_G. For each good database $\mathcal{DB}_F$ for O_F, we denote the corresponding good database for O_G by $[\mathcal{DB}_F]_G$. Similarly, for each good database $\mathcal{DB}_G$ for O_G, we denote the corresponding database for O_F by $[\mathcal{DB}_G]_F$.

An upper bound of the oracle distinguishing advantage. Let $\mathcal{A}$ be an oracle-aided quantum algorithm that makes at most q quantum queries. Let $|\psi_i\rangle$ (resp., $|\psi'_i\rangle$) be the entire quantum state just before the i-th query when $\mathcal{A}$ runs relative to O_F (resp., O_G). By abuse of notation, let $|\psi_{q+1}\rangle$ (resp., $|\psi'_{q+1}\rangle$) be the entire quantum state just before the final measurement.

The technically hardest part to give an upper bound of $\mathbf{Adv}^{\mathrm{dist}}_{O_F,O_G}(\mathcal{A})$ is to show that, for $i = 1, \ldots, q+1$, there exist vectors $|\psi_i^{'\mathsf{good}}\rangle$, $|\psi_i^{'\mathsf{bad}}\rangle$, $|\psi_i^{\mathsf{good}}\rangle$, and $|\psi_i^{\mathsf{bad}}\rangle$ that satisfy the following properties.

1. $|\psi'_i\rangle = |\psi_i^{'\mathsf{good}}\rangle + |\psi_i^{'\mathsf{bad}}\rangle$ and $|\psi_i\rangle = |\psi_i^{\mathsf{good}}\rangle + |\psi_i^{\mathsf{bad}}\rangle$.
2. There exists complex number $a^{(i)}_{xyz\mathcal{DB}_G}$ such that

$$|\psi_i^{'\mathsf{good}}\rangle = \sum_{\substack{x,y,z \\ \mathcal{DB}_G:\text{good database for } O_G}} a^{(i)}_{xyz\mathcal{DB}_G} |x,y,z\rangle \otimes |\mathcal{DB}_G\rangle, \text{ and} \tag{5.11}$$

$$|\psi_i^{\mathsf{good}}\rangle = \sum_{\substack{x,y,z \\ \mathcal{DB}_G:\text{good database for } O_G}} a^{(i)}_{xyz\mathcal{DB}_G} |x,y,z\rangle \otimes |[\mathcal{DB}_G]_F\rangle \tag{5.12}$$

   hold, where x, y, and z correspond to $\mathcal{A}$'s register to send queries to oracles, register to receive answers from oracles, and register for offline computation, respectively.
3. It holds that

$$\left\||\psi_i^{'\mathsf{bad}}\rangle\right\| \leq \left\||\psi_{i-1}^{'\mathsf{bad}}\rangle\right\| + \epsilon_{\mathsf{bad}}^{'(i-1)} \text{ and } \left\||\psi_i^{\mathsf{bad}}\rangle\right\| \leq \left\||\psi_{i-1}^{\mathsf{bad}}\rangle\right\| + \epsilon_{\mathsf{bad}}^{(i-1)} \tag{5.13}$$

   for some positive values $\epsilon_{\mathsf{bad}}^{'(i-1)}$ and $\epsilon_{\mathsf{bad}}^{(i-1)}$ (we set $|\psi_0^{'\mathsf{bad}}\rangle = |\psi_0^{\mathsf{bad}}\rangle = 0$, $|\psi_1^{'\mathsf{bad}}\rangle = |\psi_1^{\mathsf{bad}}\rangle = 0$, and $\epsilon_{\mathsf{bad}}^{(0)} = \epsilon_{\mathsf{bad}}^{'(0)} = 0$).

The following proposition ensures that we will obtain an upper bound of the distinguishing advantage of $\mathcal{A}$ when we prove the existence of such vectors $|\psi_i^{'\mathsf{good}}\rangle$, $|\psi_i^{'\mathsf{bad}}\rangle$, $|\psi_i^{\mathsf{good}}\rangle$, and $|\psi_i^{\mathsf{bad}}\rangle$.

Proposition 15. *Suppose that there exist vectors $|\psi_i^{'\mathsf{good}}\rangle$, $|\psi_i^{'\mathsf{bad}}\rangle$, $|\psi_i^{\mathsf{good}}\rangle$, and $|\psi_i^{\mathsf{bad}}\rangle$ that satisfy the above three properties. Then, $\mathbf{Adv}^{\mathrm{dist}}_{O_F,O_G}(\mathcal{A}) \leq \sum_{1\leq i\leq q} \epsilon_{\mathsf{bad}}^{'(i)} + \sum_{1\leq i\leq q} \epsilon_{\mathsf{bad}}^{(i)}$ holds.*

Though this proposition is essentially proved in Chapter 4, here we give a proof for completeness.

Proof. From (5.13), it follows that $\left\||\psi_{q+1}^{'\mathsf{bad}}\rangle\right\| \leq \sum_{1\leq i\leq q} \epsilon_{\mathsf{bad}}^{'(i)}$ and $\left\||\psi_{q+1}^{\mathsf{bad}}\rangle\right\| \leq \sum_{1\leq i\leq q} \epsilon_{\mathsf{bad}}^{(i)}$. In addition,

$$\mathsf{td}\left(\mathrm{Tr}_{O_F}\left(|\psi_{q+1}^{\mathsf{good}}\rangle\langle\psi_{q+1}^{\mathsf{good}}|\right), \mathrm{Tr}_{O_G}\left(|\psi_{q+1}^{'\mathsf{good}}\rangle\langle\psi_{q+1}^{'\mathsf{good}}|\right)\right) = 0$$

follows from (5.11) and (5.12), where Tr_{O_F} and Tr_{O_G} denote the partial trace over the quantum systems of the oracle's states. Thus we have

$$\begin{aligned}\mathbf{Adv}^{\mathrm{dist}}_{O_F,O_G}(\mathcal{A}) &\leq \mathsf{td}\left(\mathrm{Tr}_{O_F}\left(|\psi_{q+1}\rangle\langle\psi_{q+1}|\right), \mathrm{Tr}_{O_G}\left(|\psi'_{q+1}\rangle\langle\psi'_{q+1}|\right)\right) \leq \left\||\psi_{q+1}^{\mathsf{bad}}\rangle\right\| + \left\||\psi_{q+1}^{'\mathsf{bad}}\rangle\right\| \\ &\leq \sum_{1\leq i\leq q} \epsilon_{\mathsf{bad}}^{'(i)} + \sum_{1\leq i\leq q} \epsilon_{\mathsf{bad}}^{(i)},\end{aligned} \tag{5.14}$$

which completes the proof. □

Intuitions. Here we explain some intuitions behind the above proof strategy. First, when we define good and bad databases, we choose good databases so that the following conditions will hold (in addition that there exists a one-to-one correspondence between good databases for O_F and those for O_G).

1. The behavior of O_F on a good database $\mathcal{DB}_F$ is the same as that of O_G on the corresponding database $[\mathcal{DB}_F]_G$.
2. The "probability" (in a quantum sense) that a good database $\mathcal{DB}_F$ (resp., $\mathcal{DB}_G$) changes to a bad database at each query to O_F (resp., O_G) is small.

The first condition ensures that the adversary cannot distinguish O_F and O_G as long as databases are good, which leads to the existence of vectors $|\psi_i^{\mathsf{good}}\rangle$ and $|\psi_i^{'\mathsf{good}}\rangle$ that satisfies (5.11) and (5.12) for each i. (Recall that, in the proof of Proposition 15, (5.11) and (5.12) for $i = q+1$ lead to the property that the adversary's distinguishing advantage is bounded by $\| |\psi_{q+1}^{\mathsf{bad}}\rangle \| + |\psi_{q+1}^{'\mathsf{bad}}\rangle \|$.) The "probability" in the second condition corresponds to the terms $\left(\epsilon_{\mathsf{bad}}^{(i)}\right)^2$ and $\left(\epsilon_{\mathsf{bad}}^{'(i)}\right)^2$. If we can show that $\left(\epsilon_{\mathsf{bad}}^{(i)}\right)^2$ and $\left(\epsilon_{\mathsf{bad}}^{'(i)}\right)^2$ are very small, we can show the indistinguishability of O_F and O_G through Proposition 15. In a later section, to show that the "probability" is really small, we decompose O_F (resp., O_G) into a sequence of $\mathsf{RstOE}_{f_1}, \ldots, \mathsf{RstOE}_{f_r}$ (resp., $\mathsf{RstOE}_{g_1}, \ldots, \mathsf{RstOE}_{g_s}$), and prove that the "probability" that a good database changes to a bad database is small at each query to RstOE_{f_j} (resp., RstOE_{g_j}) for each j.

5.2.4 Quantum Oracles and Databases for $\mathsf{FSF}_{\mathsf{small}}$ and $\mathsf{FSF}_{\mathsf{big}}$

To use the proof strategy in the previous subsection, we describe how the quantum oracles of $\mathsf{FSF}_{\mathsf{small}}$ and $\mathsf{FSF}_{\mathsf{big}}$ are implemented with f_0, f_1, and f_{small} or f_{big}, and define good and bad databases in such a way that there exists a one-to-one correspondence between good databases for $\mathsf{FSF}_{\mathsf{small}}$ and those for $\mathsf{FSF}_{\mathsf{big}}$.

Implementations of the Quantum Oracles of $\mathsf{FSF}_{\mathsf{small}}$ *and* $\mathsf{FSF}_{\mathsf{big}}$. We assume that the quantum oracle of $\mathsf{FSF}_{\mathsf{small}}$ is implemented as follows when f_0, f_1, and f_{small} are given as quantum oracles. Suppose that $|M,T\rangle|Y\rangle$ is queried to the oracle of $\mathsf{FSF}_{\mathsf{small}}$. Here, $|Y\rangle$ is the register to which the answer from the oracle will be added.

1. Query M to the oracle f_0 to obtain the state
$$|M,T\rangle|Y\rangle \otimes |f_0(M)\rangle\,. \tag{5.15}$$
2. Query T to the oracle f_1 to obtain the state
$$|M,T\rangle|Y\rangle \otimes |f_0(M)\rangle|f_1(T)\rangle\,. \tag{5.16}$$
3. Add $f_0(M)$ and $f_1(T)$ to obtain the state
$$|M,T\rangle|Y\rangle \otimes |f_0(M)\rangle|f_1(T)\rangle \otimes |\mathsf{FSum}(M,T)\rangle\,. \tag{5.17}$$
4. Query $\mathsf{FSum}(M,T)$ to the oracle of f_{small} and add the answer to $|Y\rangle$ to obtain
$$|M,T\rangle|Y \oplus \mathsf{FSF}_{\mathsf{small}}(M,T)\rangle \otimes |f_0(M)\rangle|f_1(T)\rangle \otimes |\mathsf{FSum}(M,T)\rangle\,. \tag{5.18}$$
5. Uncompute Steps 1–3 to obtain $|M,T\rangle|Y \oplus \mathsf{FSF}_{\mathsf{small}}(M,T)\rangle$.

We assume that the quantum oracle of $\mathsf{FSF}_{\mathsf{big}}$ is implemented in the same way, except that the query in the fourth step is $(M,T,\mathsf{FSum}(M,T))$ to f_{big} instead of $\mathsf{FSum}(M,T)$ to f_{small}. See also Fig. 5.4.

In what follows, as explained in Section 5.2.3, we assume that the quantum oracles of the random functions f_0, f_1, f_{small}, and f_{big} are implemented by using the recording standard oracle with errors, and thus the oracles $\mathsf{FSF}_{\mathsf{small}}$ and $\mathsf{FSF}_{\mathsf{big}}$ keep the databases (and the ancillary qubits that are temporarily used in (5.15)–(5.18)) as their states. Let $O_{\mathsf{FSF}_{\mathsf{small}}}$ and $O_{\mathsf{FSF}_{\mathsf{big}}}$ denote the unitary operators of the oracles $\mathsf{FSF}_{\mathsf{small}}$ and $\mathsf{FSF}_{\mathsf{big}}$ to respond to queries as above.

Good and bad databases. Here we define *good* and *bad* databases for $\mathsf{FSF}_{\mathsf{small}}$ and $\mathsf{FSF}_{\mathsf{big}}$ in such a way that there exists a one-to-one correspondence between good databases for $\mathsf{FSF}_{\mathsf{small}}$ and those for $\mathsf{FSF}_{\mathsf{big}}$.

Let D_0, D_1, D_{small}, and D_{big} denote (valid) databases for f_0, f_1, f_{small}, and f_{big}, respectively. The oracles $\mathsf{FSF}_{\mathsf{small}}$ and $\mathsf{FSF}_{\mathsf{big}}$ keep (quantum superpositions of) tuples of databases $(D_0, D_1, D_{\mathsf{small}})$ and $(D_0, D_1, D_{\mathsf{big}})$, respectively.

We say that a tuple of bit strings $\mathcal{E} = (W_0, W_1, Z_0, Z_1, V, C)$, where $W_i, Z_i, V, C \in \{0,1\}^n$, is an *expansion* if $V = Z_0 \oplus Z_1$. We say that a (combined) database $\mathcal{DB}_{\mathsf{small}} = (D_0, D_1, D_{\mathsf{small}})$ for $\mathsf{FSF}_{\mathsf{small}}$ (resp., $\mathcal{DB}_{\mathsf{big}} = (D_0, D_1, D_{\mathsf{big}})$ for $\mathsf{FSF}_{\mathsf{big}}$) is *good* if and only if it satisfies the following condition.

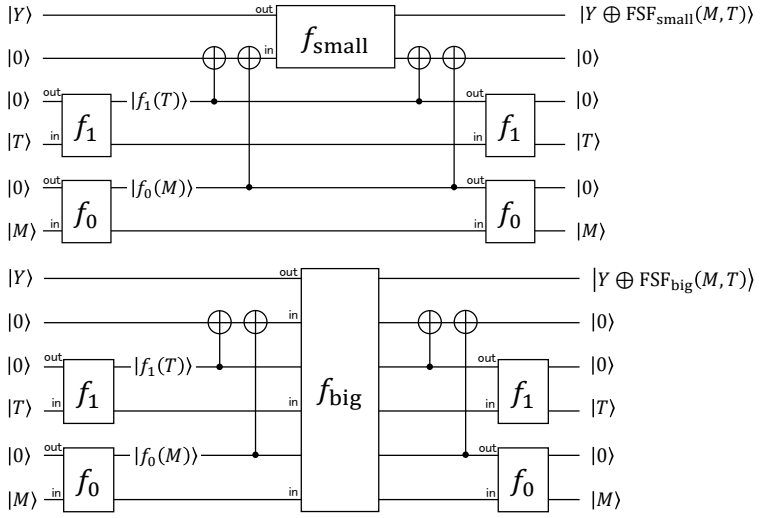


Figure 5.4: Implementation of $\mathsf{FSF}_{\text{small}}$ and $\mathsf{FSF}_{\text{big}}$. "in" and "out" denote the registers to send queries and receive answers, respectively. The functions f_0, f_1, f_{small}, and f_{big} will be implemented with the recording standard oracle with errors in security proofs.

> For each entry $(V, C) \in D_{\mathsf{small}}$ (resp., $(W_0||W_1||V, C) \in D_{\mathsf{big}}$), there exists a unique expansion $\mathcal{E} = (W_0, W_1, Z_0, Z_1, V, C)$ such that $(W_0, Z_0) \in D_0$ and $(W_1, Z_1) \in D_1$.

We call the unique expansion $\mathcal{E}$ the *expansion of* (V, C) *in* $\mathcal{DB}_{\mathsf{small}}$ (resp., the *expansion of* $(W_0||W_1||V, C)$ *in* $\mathcal{DB}_{\mathsf{big}}$). We say that a (valid) database is *bad* if it is not good.

Intuition behind good and bad databases. Intuitively, a valid database $\mathcal{DB}_{\mathsf{small}} = (D_0, D_1, D_{\mathsf{small}})$ for $\mathsf{FSF}_{\text{small}}$ (resp., $\mathcal{DB}_{\mathsf{big}} = (D_0, D_1, D_{\mathsf{big}})$ for $\mathsf{FSF}_{\text{big}}$) is bad if and only if, there exist an element (V, C) in the database D_{small} (which records transcripts for f_{small}) and two or more pairs $((W_0, Z_0), (W_1, Z_1)) \in D_0 \times D_1$ (D_0 and D_1 records transcripts for f_0 and f_1, respectively) such that $Z_0 \oplus Z_1 = V$ (i.e., $f_0(W_0) \oplus f_1(W_1) = V$). Otherwise the database is good. Note that the database is defined to be bad when such a pair exists even if W_0 and W_1 are not queried to f_0 and f_1 at the same time: A natural definition of bad transcripts in the classical setting is that, a transcript is defined to be bad if and only if, there exist a record $(V, C = f_{\mathsf{small}}(V))$ and two or more pairs of records $((W_0, Z_0 = f_0(W_0)), (W_1, Z_1 = f_1(W_1)))$ such that $Z_0 \oplus Z_1 = V$, and W_0 *and* W_1 *are queried at the same time*. However, in the quantum setting, the compressed oracle technique (and the recording oracle with errors) cannot record the information about whether certain pair of inputs are queried at the same time.[2] Thus we defined good and bad databases as above.

A one-to-one correspondence between good databases. By the above definition, we can define a one-to-one correspondence between the set of good databases for $\mathsf{FSF}_{\text{small}}$ and that for $\mathsf{FSF}_{\text{big}}$. We say that a valid database D_{big} for f_{big} is *consistent* if there does not exist distinct element $(W_0||W_1||V, C)$ and $(W_0'||W_1'||V', C')$ in D_{big} that satisfy (i) $W_0 = W_0' \wedge W_1 = W_1'$ but $V \neq V'$, or (ii) $V = V'$ but $C \neq C'$.[3] Note that, if there exist valid databases D_0 and D_1 such that $\mathcal{DB}_{\mathsf{big}} := (D_0, D_1, D_{\mathsf{big}})$ becomes a (combined) good database for $\mathsf{FSF}_{\text{big}}$, D_{big} is consistent. For a consistent database D_{big} for f_{big}, let $[D_{\mathsf{big}}]_{\mathsf{small}}$ be the database for f_{small} such that $(V, C) \in [D_{\mathsf{big}}]_{\mathsf{small}}$ if and only if $(W_0||W_1||V, C) \in D_{\mathsf{big}}$ for some $W_0, W_1 \in \{0,1\}^n$. In addition, for a (combined) good database $\mathcal{DB}_{\mathsf{big}} = (D_0, D_1, D_{\mathsf{big}})$ for $\mathsf{FSF}_{\text{small}}$, let $[\mathcal{DB}_{\mathsf{big}}]_{\mathsf{small}} := (D_0, D_1, [D_{\mathsf{big}}]_{\mathsf{small}})$. Then, the mapping $\mathcal{DB}_{\mathsf{big}} \mapsto [\mathcal{DB}_{\mathsf{big}}]_{\mathsf{small}}$ gives a one-to-one correspondence between good databases for $\mathsf{FSF}_{\text{big}}$ and those for $\mathsf{FSF}_{\text{small}}$: For a (combined) good database $\mathcal{DB}_{\mathsf{small}} = (D_0, D_1, D_{\mathsf{small}})$ for $\mathsf{FSF}_{\text{small}}$, let $[D_{\mathsf{small}}]_{\mathsf{big}}$ be the database for f_{big} such that $(W_0||W_1||V, C) \in [D_{\mathsf{small}}]_{\mathsf{big}}$ if and only if $(V, C) \in D_{\mathsf{small}}$ and the expansion of (V, C) in D_{small} is $(W_0, W_1, Z_0, Z_1, V, C)$ for some $Z_0, Z_1 \in \{0,1\}^n$. Then the (combined) database $[\mathcal{DB}_{\mathsf{small}}]_{\mathsf{big}} := (D_0, D_1, [D_{\mathsf{small}}]_{\mathsf{big}})$ is a good database for $\mathsf{FSF}_{\text{big}}$. It is easy to confirm that the mapping $\mathcal{DB}_{\mathsf{small}} \mapsto [\mathcal{DB}_{\mathsf{small}}]_{\mathsf{big}}$ is the inverse of the mapping $\mathcal{DB}_{\mathsf{big}} \mapsto [\mathcal{DB}_{\mathsf{big}}]_{\mathsf{small}}$, and vice versa.

[2] It may be realized by replacing the "undefined" indicator qubit in each entry of the f table in the state of stO by q zero qubits and toggle the i-th of these qubits when the given input was submitted in i-th query. However, currently we do not have any idea on how to formalize it, while appropriately removing some records from database.

[3] In fact the first condition (i) may not happen but such a database can theoretically exist. Here we exclude the condition (i) just for theoretical completeness.

Regular and irregular states of oracles. We say that a state vector of the oracle $\mathsf{FSF}_{\mathsf{small}}$ is *irregular* if one of the databases is invalid, or ancillary qubits used in (5.15)–(5.18) are not the all-zero state $|00\cdots0\rangle$. We say that a state vector is *regular* if it is not irregular. In addition, we say that a state vector of the oracle $\mathsf{FSF}_{\mathsf{small}}$ is *pre-irregular* if one of the databases is invalid, or the least significant $2n$ qubits (the registers that correspond to $f_1(T)$ and $\mathsf{FSum}(M,T)$ in (5.16)–(5.18)) are not $|0^n\rangle|0^n\rangle$. We say that a state vector is *preregular* if it is not pre-irregular. Similarly, we define (pre-)irregular and (pre)regular states for $\mathsf{FSF}_{\mathsf{big}}$.

The following lemma shows that the behavior of $\mathsf{RstOE}_{f_{\mathsf{big}}}$ on a consistent database D_{big} is the same as that of $\mathsf{RstOE}_{f_{\mathsf{small}}}$ on the corresponding database $[D_{\mathsf{big}}]_{\mathsf{small}}$.

Lemma 8. *Let D_{big} and D'_{big} be consistent databases for $\mathsf{FSF}_{\mathsf{big}}$. Then, for arbitrary $\tilde{M},\tilde{T},\tilde{M}',\tilde{T}' \in \{0,1\}^n$ and $\tilde{V},\tilde{V}',\tilde{Y},\tilde{Y}' \in \{0,1\}^n$,*

$$\begin{aligned}&\langle D'_{\mathsf{big}}|\langle\tilde{M}'||\tilde{T}'||\tilde{V}',\tilde{Y}'|\,\mathsf{RstOE}_{f_{\mathsf{big}}}\,|\tilde{M}||\tilde{T}||\tilde{V},\tilde{Y}\rangle\,|D_{\mathsf{big}}\rangle\\ &\quad=\langle[D'_{\mathsf{big}}]_{\mathsf{small}}|\langle\tilde{M}'||\tilde{T}'||\tilde{V}',\tilde{Y}'|\,I_{2n}\otimes\mathsf{RstOE}_{f_{\mathsf{small}}}\,|\tilde{M}||\tilde{T}||\tilde{V},\tilde{Y}\rangle\,|[D_{\mathsf{big}}]_{\mathsf{small}}\rangle\end{aligned}\tag{5.19}$$

holds.

Proof. It suffices to show the claim in the case that $\tilde{M}=\tilde{M}'$, $\tilde{T}=\tilde{T}'$, and $\tilde{V}=\tilde{V}'$ hold, since oracles do not affect input registers. Moreover, when $\mathsf{RstOE}_{f_{\mathsf{big}}}$ acts on $|\tilde{M}||\tilde{T}||\tilde{V},\tilde{Y}\rangle\,|D_{\mathsf{big}}\rangle$, $O_{f_{\mathsf{big}}}$ affects only the register that contains information about the element of $\tilde{M}||\tilde{T}||\tilde{V}$ in D_{big}, in addition to the $\tilde{Y}$ register. Hence it suffices to show the claim in the cases that (i) D_{big} is empty, or (ii) it has only a single entry $(\tilde{M}||\tilde{T}||\tilde{V},C)$ for some C. In the case (i), $[D_{\mathsf{big}}]_{\mathsf{small}}$ is also empty, and the equation follows from (3.16) and (3.17) in Proposition 3. In the case (ii), $[D_{\mathsf{big}}]_{\mathsf{small}}$ has only a single entry $(\tilde{V},C)$, and the equation follows from (3.12)–(3.15) in Proposition 3. □

5.2.5 Proof of Proposition 14

Let $\mathcal{A}$ be a quantum algorithm that makes at most q quantum queries. Let $|\psi_i\rangle$ and $|\psi'_i\rangle$ denote the whole quantum states of $\mathcal{A}$ and the oracle just before the i-th query when $\mathcal{A}$ runs relative to $\mathsf{FSF}_{\mathsf{small}}$ and $\mathsf{FSF}_{\mathsf{big}}$, respectively. (By $|\psi_{q+1}\rangle$ and $|\psi'_{q+1}\rangle$ we denote the whole quantum states just before the final measurement when $\mathcal{A}$ runs relative to $\mathsf{FSF}_{\mathsf{small}}$ and $\mathsf{FSF}_{\mathsf{big}}$, respectively, by abuse of notation.)

The technically hardest part of proving Proposition 14 is to show the following proposition. In what follows, for each summation symbol, we separate variables over which the summation is taken and the conditions imposed on the variables by ";", to simplify notations. For example, by $\sum_{\alpha,\beta;\alpha\in A,\alpha+\beta\in B}$ we indicate that the summation is taken over all possible α and β such that $\alpha\in A$ and $\alpha+\beta\in B$.

Proposition 16. *For each $1\le i\le q+1$, there exist vectors $|\psi_i^{'\mathsf{good}}\rangle$, $|\psi_i^{'\mathsf{bad}}\rangle$, $|\psi_i^{\mathsf{good}}\rangle$, and $|\psi_i^{\mathsf{bad}}\rangle$ that satisfy the following properties.*

1. *$|\psi'_i\rangle=|\psi_i^{'\mathsf{good}}\rangle+|\psi_i^{'\mathsf{bad}}\rangle$ and $|\psi_i\rangle=|\psi_i^{\mathsf{good}}\rangle+|\psi_i^{\mathsf{bad}}\rangle$.*
2. *There exists complex number $a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}}$ such that*

$$|\psi_i^{'\mathsf{good}}\rangle=\sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}})\text{:valid and good}}}a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}}\,|M,T\rangle\,|Y\rangle\,|Z\rangle\otimes|D_0,D_1,D_{\mathsf{big}}\rangle,\tag{5.20}$$

and

$$|\psi_i^{\mathsf{good}}\rangle=\sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}})\text{:valid and good}}}a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}}\,|M,T\rangle\,|Y\rangle\,|Z\rangle\otimes|[D_0,D_1,D_{\mathsf{big}}]_{\mathsf{small}}\rangle\tag{5.21}$$

hold, where (M,T), Y, and Z correspond to $\mathcal{A}$'s register to send queries to oracles, register to receive answers from oracles, and register for offline computation, respectively.

3. *For each database $(D_0,D_1,D_{\mathsf{big}})$ in $|\psi_i^{'\mathsf{good}}\rangle$ (resp., $(D_0,D_1,D_{\mathsf{small}})$ in $|\psi_i^{\mathsf{good}}\rangle$) with non-zero quantum amplitude, $|D_0|\le 2(i-1)$, $|D_1|\le 2(i-1)$, and $|D_{\mathsf{big}}|\le i-1$ (resp., $|D_{\mathsf{small}}|\le i-1$).*
4. *$\left\||\psi_i^{'\mathsf{bad}}\rangle\right\|\le\left\||\psi_{i-1}^{'\mathsf{bad}}\rangle\right\|+O\left(\sqrt{\frac{i^2}{2^n}}\right)$ and $\left\||\psi_i^{\mathsf{bad}}\rangle\right\|\le\left\||\psi_{i-1}^{\mathsf{bad}}\rangle\right\|+O\left(\sqrt{\frac{i^2}{2^n}}\right)$ hold.*

Let RstOE_{f_0}, RstOE_{f_1}, $\mathsf{RstOE}_{f_{\mathsf{small}}}$, and $\mathsf{RstOE}_{f_{\mathsf{big}}}$ be the recording standard oracle with errors for f_0, f_1, f_{small}, and f_{big}, respectively. Then, the unitary operators $O_{\mathsf{FSF}_{\mathrm{small}}}$ and $O_{\mathsf{FSF}_{\mathrm{big}}}$ are decomposed into 7 unitary operators as

$$O_{\mathsf{FSF}_{\mathrm{small}}} = \mathsf{RstOE}^*_{f_0} \cdot \mathsf{RstOE}^*_{f_1} \cdot \mathsf{XOR}^* \cdot \mathsf{RstOE}_{f_{\mathsf{small}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0}$$

and

$$O_{\mathsf{FSF}_{\mathrm{big}}} = \mathsf{RstOE}^*_{f_0} \cdot \mathsf{RstOE}^*_{f_1} \cdot \mathsf{XOR}^* \cdot \mathsf{RstOE}_{f_{\mathsf{big}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0},$$

respectively, where XOR denotes the unitary operation to add the values $f_0(M)$ and $f_1(T)$ in Step 3 (state (5.17)) of the implementation of the oracles, which is defined by $\mathsf{XOR}\,|a\rangle\,|b\rangle\,|c\rangle = |a\rangle\,|b\rangle\,|c \oplus a \oplus b\rangle$.

To show the proposition, we study how the states $|\psi'_i\rangle$ and $|\psi_i\rangle$ change when the 7 unitary operators act, in a sequential order. First, we show the following lemma.

Lemma 9 (Action of RstOE_{f_0})**.** *Suppose that there exist i and vectors $|\psi_j^{'\mathsf{good}}\rangle$, $|\psi_j^{'\mathsf{bad}}\rangle$, $|\psi_j^{\mathsf{good}}\rangle$, and $|\psi_j^{\mathsf{bad}}\rangle$ that satisfy the four properties in Proposition 16 for $j = 1, \ldots, i$. Then, there exist vectors $|\psi_i^{'\mathsf{good},1}\rangle$, $|\psi_i^{'\mathsf{bad},1}\rangle$, $|\psi_i^{\mathsf{good},1}\rangle$, and $|\psi_i^{\mathsf{bad},1}\rangle$ that satisfy the following properties.*

1. $\mathsf{RstOE}_{f_0}\,|\psi'_i\rangle = |\psi_i^{'\mathsf{good},1}\rangle + |\psi_i^{'\mathsf{bad},1}\rangle$ *and* $\mathsf{RstOE}_{f_0}\,|\psi_i\rangle = |\psi_i^{\mathsf{good},1}\rangle + |\psi_i^{\mathsf{bad},1}\rangle$.
2. *There exists complex number $a^{(i),1}_{MTYZD_0D_1D_{\mathsf{big}}}$ such that*

$$|\psi_i^{'\mathsf{good},1}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\perp}} a^{(i),1}_{MTYZD_0D_1D_{\mathsf{big}}}\,|M,T\rangle\,|Y\rangle\,|Z\rangle \otimes |D_0, D_1, D_{\mathsf{big}}\rangle \otimes |D_0(M)\rangle, \tag{5.22}$$

   and

$$|\psi_i^{\mathsf{good},1}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\perp}} a^{(i),1}_{MTYZD_0D_1D_{\mathsf{big}}}\,|M,T\rangle\,|Y\rangle\,|Z\rangle \otimes |[D_0, D_1, D_{\mathsf{big}}]_{\mathsf{small}}\rangle \otimes |D_0(M)\rangle \tag{5.23}$$

   hold, where (M,T), Y, and Z correspond to $\mathcal{A}$'s register to send queries to oracles, register to receive answers from oracles, and register for offline computation, respectively.
3. *For each database $(D_0, D_1, D_{\mathsf{big}})$ in $|\psi_i^{'\mathsf{good},1}\rangle$ (resp., $(D_0, D_1, D_{\mathsf{small}})$ in $|\psi_i^{\mathsf{good},1}\rangle$) with non-zero quantum amplitude, $|D_0| \le 2(i-1)+1$, $|D_1| \le 2(i-1)$, and $|D_{\mathsf{big}}| \le i-1$ (resp., $|D_{\mathsf{small}}| \le i-1$).*
4. $\left\||\psi_i^{'\mathsf{bad},1}\rangle\right\| \le \left\||\psi_i^{'\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i^2}{2^n}}\right)$ *and* $\left\||\psi_i^{\mathsf{bad},1}\rangle\right\| \le \left\||\psi_i^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i^2}{2^n}}\right)$ *hold.*

Proof. Let Π_{valid} denote the projection onto the space spanned by the vectors that correspond to valid databases. Then, by applying Proposition 3 to RstOE_{f_0}, we have that

$$\begin{aligned}
&\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}\,|\psi_i^{'\mathsf{good}}\rangle\\
&\quad= \Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0} \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid and good}}} a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}}\,|M,T\rangle\,|Y\rangle\,|Z\rangle \otimes |D_0, D_1, D_{\mathsf{big}}\rangle\\
&\quad= \Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0} \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}\,|M,T\rangle\,|Y\rangle\,|Z\rangle \otimes |D_0\cup(M,\alpha), D_1, D_{\mathsf{big}}\rangle\\
&\qquad+ \Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0} \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid}\\D_0(M)=\perp\\(D_0,D_1,D_{\mathsf{big}}):\text{good}}} a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}}\,|M,T\rangle\,|Y\rangle\,|Z\rangle \otimes |D_0, D_1, D_{\mathsf{big}}\rangle\\
&\quad= \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}\,|M,T\rangle\,|Y\rangle\,|Z\rangle \otimes |D_0\cup(M,\alpha), D_1, D_{\mathsf{big}}\rangle \otimes |\alpha\rangle
\end{aligned} \tag{5.24}$$

$$- \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} \frac{1}{2^n} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes |D_0\cup(M,\gamma), D_1, D_{\mathsf{big}}\rangle \otimes |\gamma\rangle \tag{5.25}$$

$$+ \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\perp\\ (D_0,D_1,D_{\mathsf{big}}):\text{good}}} \frac{1}{\sqrt{2^n}} a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes |D_0\cup(M,\alpha), D_1, D_{\mathsf{big}}\rangle \otimes |\alpha\rangle \tag{5.26}$$

$$+ |\epsilon'\rangle$$

holds, where

$$|\epsilon'\rangle = \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} \frac{1}{\sqrt{2^n}} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes \left(|D_0\rangle - \sum_\gamma \frac{1}{\sqrt{2^n}} |D_0\cup(M,\gamma)\rangle\right) |D_1, D_{\mathsf{big}}\rangle \otimes |\alpha\rangle \tag{5.27}$$

$$+ \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} \frac{1}{2^n} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes \left(2\sum_\gamma \frac{1}{\sqrt{2^n}} |D_0\cup(M,\gamma)\rangle - |D_0\rangle\right) |D_1, D_{\mathsf{big}}\rangle \otimes |\widehat{0^n}\rangle \tag{5.28}$$

$$+ \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\perp\\ (D_0,D_1,D_{\mathsf{big}}):\text{good}}} \frac{1}{\sqrt{2^n}} a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes \left(|D_0\rangle - \sum_\gamma \frac{1}{\sqrt{2^n}} |D_0\cup(M,\gamma)\rangle\right) |D_1, D_{\mathsf{big}}\rangle \otimes |\widehat{0^n}\rangle\,. \tag{5.29}$$

The terms (5.24), (5.25), and (5.26) correspond to (the valid component of) the terms (3.12), (3.14), and (3.16), respectively. In addition, the terms (5.27), (5.28), and (5.29) correspond to (the valid component of) the terms (3.13), (3.15), and (3.17), respectively. Let us denote the terms (5.27), (5.28), and (5.29) by $|(5.27)\rangle$, $|(5.28)\rangle$, and $|(5.29)\rangle$, respectively. Then

$$\begin{aligned}\||(5.27)\rangle\|^2 &= \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} \frac{1}{2^n} \left|a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}\right|^2 + \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} \frac{1}{2^{2n}} \left|a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}\right|^2\\ &\le O\left(\frac{1}{2^n}\right)\end{aligned}$$

holds. Similarly we have $\||(5.29)\rangle\|^2 \le O\left(\frac{1}{2^n}\right)$. In addition,

$$\begin{aligned}\||(5.28)\rangle\|^2 &\le 5 \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\perp}} \left| \sum_{\substack{\alpha;\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} \frac{a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}}{2^n} \right|^2\\ &\le 5 \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\perp\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} \frac{\left|a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}\right|^2}{2^n}\\ &\le O\left(\frac{1}{2^n}\right),\end{aligned}$$

where we used the convexity of the function $X \mapsto X^2$. Hence

$$\| |\epsilon'\rangle \| \leq O\left(\sqrt{\frac{1}{2^n}}\right) \tag{5.30}$$

holds.

In the same way, we can show

$$\begin{aligned}
\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}|\psi_i^{\mathsf{good}}\rangle = & \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\mathrm{valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\mathrm{good}}} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \\
& \qquad \otimes |D_0\cup(M,\alpha),D_1,[D_{\mathsf{big}}]_{\mathsf{small}}\rangle\otimes|\alpha\rangle \\
& - \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\mathrm{valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\mathrm{good}}} \frac{1}{2^n} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \\
& \qquad \otimes |D_0\cup(M,\gamma),D_1,[D_{\mathsf{big}}]_{\mathsf{small}}\rangle\otimes|\gamma\rangle \\
& + \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\mathrm{valid}\\D_0(M)=\perp\\(D_0,D_1,D_{\mathsf{big}}):\mathrm{good}}} \frac{1}{\sqrt{2^n}} a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \\
& \qquad \otimes |D_0\cup(M,\alpha),D_1,[D_{\mathsf{big}}]_{\mathsf{small}}\rangle\otimes|\alpha\rangle \\
& + |\epsilon\rangle,
\end{aligned} \tag{5.31}$$

where $|\epsilon\rangle$ is a vector such that $\||\epsilon\rangle\| \leq O\left(\sqrt{\frac{1}{2^n}}\right)$.

Now, set

$$|\psi_i^{\mathsf{good},1}\rangle := \Pi_{\mathsf{good}}\left(\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}|\psi_i^{\mathsf{good}}\rangle - |\epsilon\rangle\right), \quad |\psi_i^{\mathsf{bad},1}\rangle := \mathsf{RstOE}_{f_0}|\psi_i\rangle - |\psi_i^{\mathsf{good},1}\rangle, \tag{5.32}$$

and

$$|\psi_i'^{\mathsf{good},1}\rangle := \Pi_{\mathsf{good}}\left(\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}|\psi_i'^{\mathsf{good}}\rangle - |\epsilon'\rangle\right), \quad |\psi_i'^{\mathsf{bad},1}\rangle := \mathsf{RstOE}_{f_0}|\psi_i'\rangle - |\psi_i'^{\mathsf{good},1}\rangle, \tag{5.33}$$

where Π_{good} denotes the projection onto the space spanned by the vectors that correspond to good databases. Then the first, second, and third properties of Lemma 9 immediately follow from the corresponding properties in Proposition 16 and the definitions of $|\psi_i^{\mathsf{good},1}\rangle$ and $|\psi_i'^{\mathsf{good},1}\rangle$.

Below, we show the fourth property. Let us denote the terms (5.24), (5.25), and (5.26) by $|(5.24)\rangle$, $|(5.25)\rangle$, and $|(5.26)\rangle$, respectively. In addition, let Π_{bad} denote the projection onto the space spanned by the vectors that correspond to bad databases. Then,

$$\Pi_{\mathsf{bad}}|(5.24)\rangle = 0 \tag{5.34}$$

holds since all the databases in $|(5.24)\rangle$ are good.

On the term (5.25), we have that

$$\begin{aligned}
\Pi_{\mathsf{bad}}|(5.25)\rangle = & - \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\mathrm{valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\mathrm{good}\\(D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}):\mathrm{bad}}} \frac{1}{2^n} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \\
& \qquad \otimes |D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}\rangle\otimes|\gamma\rangle \\
= & - \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\mathrm{valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\mathrm{good}\\\exists T'\mathrm{s.t.}D_1(T')\neq\perp\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\perp\\(D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}):\mathrm{bad}}} \frac{1}{2^n} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \\
& \qquad \otimes |D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}\rangle\otimes|\gamma\rangle \qquad (5.35) \\
& - \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\mathrm{valid}\\D_0(M)=\perp\\(D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\mathrm{good}\\\nexists T'\mathrm{s.t.}D_1(T')\neq\perp\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\perp\\(D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}):\mathrm{bad}}} \frac{1}{2^n} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \\
& \qquad \otimes |D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}\rangle\otimes|\gamma\rangle \qquad (5.36)
\end{aligned}$$

holds.

Here we give an upper bound of the norm of the term (5.35). If a tuple $(M, (D_0 \cup (M,\gamma), D_1, D_{\mathsf{big}}))$ satisfies

1. $D_0(M) = \bot$, and
2. $(D_0 \cup (M,\gamma), D_1, D_{\mathsf{big}})$ is bad,

then the number of α that satisfies

1. $(D_0 \cup (M,\alpha), D_1, D_{\mathsf{big}})$ becomes good, and
2. there exists T' such that $D_1(T') \neq \bot$ and $[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T') \oplus \alpha) \neq \bot$

is at most $|D_1| \cdot |D_{\mathsf{big}}| \leq 2(i-1)^2$. Hence

$$
\begin{aligned}
&\left\| \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\bot\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}\\ \exists T'\text{s.t.}D_1(T')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\bot\\ (D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}):\text{bad}}} \frac{1}{2^n} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}} |M,T\rangle|Y\rangle|Z\rangle \otimes |D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}\rangle \otimes |\gamma\rangle \right\|^2 \\
&= \sum_{\substack{M,T,Y,Z,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\bot\\ (D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}):\text{bad}}} \frac{1}{2^{2n}} \left| \sum_{\substack{\alpha;(D_0\cup(M,\alpha),D_1,D_{\mathsf{big}})\text{is good, and}\\ \exists T'\text{s.t.}D_1(T')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\bot}} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}} \right|^2 \\
&\leq \sum_{\substack{M,T,Y,Z,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\bot\\ (D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}):\text{bad}}} \frac{2(i-1)^2}{2^{2n}} \sum_{\substack{\alpha;(D_0\cup(M,\alpha),D_1,D_{\mathsf{big}})\text{is good, and}\\ \exists T'\text{s.t.}D_1(T')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\bot}} \left| a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}} \right|^2 \\
&= \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\bot\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}\\ \exists T'\text{s.t.}D_1(T')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\bot}} \left| a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}} \right|^2 \cdot \sum_{\substack{\gamma;\\ (D_0\cup(M,\gamma),D_1,D_{\mathsf{big}})\text{is bad}}} \frac{2(i-1)^2}{2^{2n}} \\
&\leq \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\bot\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}\\ \exists T'\text{s.t.}D_1(T')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\bot}} \left| a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}} \right|^2 \cdot \frac{2(i-1)^2}{2^n} \\
&\leq O\left(\frac{i^2}{2^n}\right) \qquad (5.37)
\end{aligned}
$$

holds, where we used the convexity of the function $X \mapsto X^2$ for the first inequality.

Next, we give an upper bound of the norm of the term (5.36). If a tuple $(M, (D_0 \cup (M,\alpha), D_1, D_{\mathsf{big}}))$ satisfies

1. $D_0(M) = \bot$,
2. $(D_0 \cup (M,\alpha), D_1, D_{\mathsf{big}})$ is good, and
3. there does not exist T' such that $D_1(T') \neq \bot$ and $[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T') \oplus \alpha) \neq \bot$,

then the number of γ such that $(D_0 \cup (M,\gamma), D_1, D_{\mathsf{big}})$ becomes bad is at most $|D_1| \cdot |D_{\mathsf{big}}| \le 2(i-1)^2$. Hence

$$\begin{aligned}
&\left\| \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\bot\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}\\ \nexists T'\text{s.t.}D_1(T')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\bot\\ (D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}):\text{bad}}} \frac{1}{2^n} a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}} |M,T\rangle|Y\rangle|Z\rangle \right.\\
&\qquad\qquad \left. \otimes |D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}\rangle \otimes |\gamma\rangle \right\|^2\\
&= \sum_{\substack{M,T,Y,Z,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\bot\\ \nexists T'\text{s.t.}D_1(T')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\bot\\ (D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}):\text{bad}}} \left| \sum_{\substack{\alpha;\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} \frac{a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}}{2^n} \right|^2\\
&\le \sum_{\substack{M,T,Y,Z,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\bot\\ \nexists T'\text{s.t.}D_1(T')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\bot\\ (D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}):\text{bad}}} \sum_{\substack{\alpha;\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}}} \frac{\left|a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}\right|^2}{2^n}\\
&= \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid}\\ D_0(M)=\bot\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{good}\\ \nexists T'\text{s.t.}D_1(T')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_1(T')\oplus\alpha)\neq\bot}} \left|a^{(i)}_{MTYZD_0\cup(M,\alpha)D_1D_{\mathsf{big}}}\right|^2 \cdot \frac{\left|\{\gamma \middle| (D_0\cup(M,\gamma),D_1,D_{\mathsf{big}}) : \text{bad}\}\right|}{2^n}\\
&\le O\left(\frac{i^2}{2^n}\right) \qquad (5.38)
\end{aligned}$$

holds, where we used the convexity of the function $X \mapsto X^2$ for the first inequality.

From (5.35)–(5.38),

$$\|\Pi_{\mathsf{bad}} |(5.25)\rangle\| \le O\left(\sqrt{\frac{i^2}{2^n}}\right) \qquad (5.39)$$

follows.

Moreover,

$$\begin{aligned}
\|\Pi_{\mathsf{bad}} |(5.26)\rangle\|^2 &= \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)=\bot\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{bad}}} \frac{\left|a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}}\right|^2}{2^n}\\
&= \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)=\bot\\ (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}):\text{bad}}} \left|a^{(i)}_{MTYZD_0D_1D_{\mathsf{big}}}\right|^2 \cdot \frac{\left|\left\{\alpha \middle| (D_0\cup(M,\alpha),D_1,D_{\mathsf{big}}) \text{ is bad}\right\}\right|}{2^n}\\
&\le O\left(\sqrt{\frac{i^2}{2^n}}\right) \qquad (5.40)
\end{aligned}$$

can be shown in a similar way as we showed (5.38).

From (5.34), (5.39), and (5.40),

$$\left\|\Pi_{\mathsf{bad}}\left(\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}\left|\psi_i^{'\mathsf{good}}\right\rangle-\left|\epsilon'\right\rangle\right)\right\|\leq O\left(\sqrt{\frac{i^2}{2^n}}\right) \tag{5.41}$$

follows. Since this inequality and (5.30) hold,

$$\begin{aligned}
\left\|\left|\psi_i^{'\mathsf{bad},1}\right\rangle\right\| &= \left\|\mathsf{RstOE}_{f_0}\left|\psi_i'\right\rangle-\left|\psi_i^{'\mathsf{good},1}\right\rangle\right\| \\
&= \left\|\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}\left|\psi_i'\right\rangle-\Pi_{\mathsf{good}}\left(\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}\left|\psi_i^{\mathsf{good}}\right\rangle-\left|\epsilon'\right\rangle\right)\right\| \\
&= \left\|\Pi_{\mathsf{bad}}\left(\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}\left|\psi_i^{'\mathsf{good}}\right\rangle-\left|\epsilon'\right\rangle\right)+\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}\left|\psi_i^{'\mathsf{bad}}\right\rangle+\left|\epsilon'\right\rangle\right\| \\
&\leq \left\|\Pi_{\mathsf{bad}}\left(\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}\left|\psi_i^{'\mathsf{good}}\right\rangle-\left|\epsilon'\right\rangle\right)\right\|+\left\|\left|\psi_i^{'\mathsf{bad}}\right\rangle\right\|+\left\|\left|\epsilon'\right\rangle\right\| \\
&\leq \left\|\left|\psi_i^{'\mathsf{bad}}\right\rangle\right\|+O\left(\sqrt{\frac{i^2}{2^n}}\right)
\end{aligned} \tag{5.42}$$

holds, which implies that the fourth property holds for $\left|\psi_i^{'\mathsf{bad},1}\right\rangle$[4]. We can prove the fourth property for $\left|\psi_i^{\mathsf{bad},1}\right\rangle$ in the same way. □

The following lemma shows how the states $\mathsf{RstOE}_{f_0}\left|\psi_i'\right\rangle$ and $\mathsf{RstOE}_{f_0}\left|\psi_i\right\rangle$ change when $\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}$ act on them.

Lemma 10 (Action of $\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}$)**.** *Suppose that there exist i and vectors $\left|\psi_j^{'\mathsf{good}}\right\rangle$, $\left|\psi_j^{'\mathsf{bad}}\right\rangle$, $\left|\psi_j^{\mathsf{good}}\right\rangle$, and $\left|\psi_j^{\mathsf{bad}}\right\rangle$ that satisfy the four properties in Proposition 16 for $j=1,\ldots,i$. Then, there exist vectors $\left|\psi_i^{'\mathsf{good},2}\right\rangle$, $\left|\psi_i^{'\mathsf{bad},2}\right\rangle$, $\left|\psi_i^{\mathsf{good},2}\right\rangle$, and $\left|\psi_i^{\mathsf{bad},2}\right\rangle$ that satisfy the following properties.*

1. $\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}\cdot\mathsf{RstOE}_{f_0}\left|\psi_i'\right\rangle=\left|\psi_i^{'\mathsf{good},2}\right\rangle+\left|\psi_i^{'\mathsf{bad},2}\right\rangle$ *and* $\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}\cdot\mathsf{RstOE}_{f_0}\left|\psi\right\rangle=\left|\psi_i^{\mathsf{good},2}\right\rangle+\left|\psi_i^{\mathsf{bad},2}\right\rangle$.
2. *There exists complex number $a^{(i),2}_{MTYZD_0D_1D_{\mathsf{big}}}$ such that*

$$\left|\psi_i^{'\mathsf{good},2}\right\rangle=\sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\perp\wedge D_1(T)\neq\perp}} a^{(i),2}_{MTYZD_0D_1D_{\mathsf{big}}}\left|M,T\right\rangle\left|Y\right\rangle\left|Z\right\rangle\otimes\left|D_0,D_1,D_{\mathsf{big}}\right\rangle \\ \otimes\left|D_0(M)\right\rangle\left|D_1(T)\right\rangle\left|D_0(M)\oplus D_1(T)\right\rangle,$$

   and

$$\left|\psi_i^{\mathsf{good},2}\right\rangle=\sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\perp\wedge D_1(T)\neq\perp}} a^{(i),2}_{MTYZD_0D_1D_{\mathsf{big}}}\left|M,T\right\rangle\left|Y\right\rangle\left|Z\right\rangle\otimes\left|[D_0,D_1,D_{\mathsf{big}}]_{\mathsf{small}}\right\rangle \\ \otimes\left|D_0(M)\right\rangle\left|D_1(T)\right\rangle\left|D_0(M)\oplus D_1(T)\right\rangle$$

   hold, where (M,T), Y, and Z correspond to $\mathcal{A}$'s register to send queries to oracles, register to receive answers from oracles, and register for offline computation, respectively.
3. *For each database $(D_0,D_1,D_{\mathsf{big}})$ in $\left|\psi_i^{'\mathsf{good},2}\right\rangle$ (resp., $(D_0,D_1,D_{\mathsf{small}})$ in $\left|\psi_i^{\mathsf{good},2}\right\rangle$) with non-zero quantum amplitude, $|D_0|\leq 2(i-1)+1$, $|D_1|\leq 2(i-1)+1$, and $|D_{\mathsf{big}}|\leq i-1$ (resp., $|D_{\mathsf{small}}|\leq i-1$).*
4. $\left\|\left|\psi_i^{'\mathsf{bad},2}\right\rangle\right\|\leq\left\|\left|\psi_i^{'\mathsf{bad}}\right\rangle\right\|+O\left(\sqrt{\frac{i^2}{2^n}}\right)$ *and* $\left\|\left|\psi_i^{\mathsf{bad},2}\right\rangle\right\|\leq\left\|\left|\psi_i^{\mathsf{bad}}\right\rangle\right\|+O\left(\sqrt{\frac{i^2}{2^n}}\right)$ *hold.*

This lemma can be shown in the same way as we showed Lemma 9. Thus we omit to write the proof.

The next lemma shows how the state changes when $\mathsf{RstOE}_{f_{\mathsf{big}}}$ and $\mathsf{RstOE}_{f_{\mathsf{small}}}$ act on the states $\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}\cdot\mathsf{RstOE}_{f_0}\left|\psi_i'\right\rangle$ and $\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}\cdot\mathsf{RstOE}_{f_0}\left|\psi_i\right\rangle$, respectively.

Lemma 11 (Action of $\mathsf{RstOE}_{f_{\mathsf{small}}}$ and $\mathsf{RstOE}_{f_{\mathsf{big}}}$)**.** *Suppose that there exist i and vectors $\left|\psi_j^{'\mathsf{good}}\right\rangle$, $\left|\psi_j^{'\mathsf{bad}}\right\rangle$, $\left|\psi_j^{\mathsf{good}}\right\rangle$, and $\left|\psi_j^{\mathsf{bad}}\right\rangle$ that satisfy the four properties in Proposition 16 for $j=1,\ldots,i$. Then, there exist vectors $\left|\psi_i^{'\mathsf{good},3}\right\rangle$, $\left|\psi_i^{'\mathsf{bad},3}\right\rangle$, $\left|\psi_i^{\mathsf{good},3}\right\rangle$, and $\left|\psi_i^{\mathsf{bad},3}\right\rangle$ that satisfy the following properties.*

[4]Note that all the databases of $\mathsf{RstOE}_{f_0}\left|\psi_i^{'\mathsf{good}}\right\rangle$ are valid, and thus $\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_0}\left|\psi_i^{'\mathsf{good}}\right\rangle=\mathsf{RstOE}_{f_0}\left|\psi_i^{'\mathsf{good}}\right\rangle$ holds.

1. $\mathsf{RstOE}_{f_{\mathsf{big}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0} |\psi_i'\rangle = |\psi_i^{'\mathsf{good},3}\rangle + |\psi_i^{'\mathsf{bad},3}\rangle$ *and* $\mathsf{RstOE}_{f_{\mathsf{small}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0} |\psi_i\rangle = |\psi_i^{\mathsf{good},3}\rangle + |\psi_i^{\mathsf{bad},3}\rangle$.

2. *There exists complex number* $a^{(i),3}_{MTYZD_0D_1D_{\mathsf{big}}}$ *such that*

$$|\psi_i^{'\mathsf{good},3}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\perp\wedge D_1(T)\neq\perp}} a^{(i),3}_{MTYZD_0D_1D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes |D_0,D_1,D_{\mathsf{big}}\rangle \otimes |D_0(M)\rangle |D_1(T)\rangle |D_0(M)\oplus D_1(T)\rangle,$$

and

$$|\psi_i^{\mathsf{good},3}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\perp\wedge D_1(T)\neq\perp}} a^{(i),3}_{MTYZD_0D_1D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes |[D_0,D_1,D_{\mathsf{big}}]_{\mathsf{small}}\rangle \otimes |D_0(M)\rangle |D_1(T)\rangle |D_0(M)\oplus D_1(T)\rangle$$

hold, where (M,T)*,* Y*, and* Z *correspond to* $\mathcal{A}$*'s register to send queries to oracles, register to receive answers from oracles, and register for offline computation, respectively.*

3. *For each database* $(D_0,D_1,D_{\mathsf{big}})$ *in* $|\psi_i^{'\mathsf{good},3}\rangle$ *(resp.,* $(D_0,D_1,D_{\mathsf{small}})$ *in* $|\psi_i^{\mathsf{good},3}\rangle$*) with non-zero quantum amplitude,* $|D_0|\le 2(i-1)+1$*,* $|D_1|\le 2(i-1)+1$*, and* $|D_{\mathsf{big}}|\le i$ *(resp.,* $|D_{\mathsf{small}}|\le i$*).*

4. $\left\||\psi_i^{'\mathsf{bad},3}\rangle\right\| \le \left\||\psi_i^{'\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i^2}{2^n}}\right)$ *and* $\left\||\psi_i^{\mathsf{bad},3}\rangle\right\| \le \left\||\psi_i^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i^2}{2^n}}\right)$ *hold.*

Proof. From Lemma 10, it follows that there exist vectors $|\psi_i^{'\mathsf{good},2}\rangle$, $|\psi_i^{'\mathsf{bad},2}\rangle$, $|\psi_i^{\mathsf{good},2}\rangle$, and $|\psi_i^{\mathsf{bad},2}\rangle$ that satisfy the four properties in Lemma 10.

Define $|\psi_i^{'\mathsf{good},3}\rangle := \Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_{\mathsf{big}}} |\psi_i^{'\mathsf{good},2}\rangle$, $|\psi_i^{'\mathsf{bad},3}\rangle := \mathsf{RstOE}_{f_{\mathsf{big}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0} |\psi_i'\rangle - |\psi_i^{'\mathsf{good},3}\rangle$, $|\psi_i^{\mathsf{good},3}\rangle := \Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_{\mathsf{small}}} |\psi_i^{\mathsf{good},2}\rangle$, and $|\psi_i^{\mathsf{bad},3}\rangle := \mathsf{RstOE}_{f_{\mathsf{small}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0} |\psi_i\rangle - |\psi_i^{\mathsf{good},3}\rangle$. Then the first property obviously holds. The second property immediately follows from Lemma 8 and the second property in Lemma 10[5]. The third property follows from the third property in Lemma 10. On the fourth property, we have

$$\begin{aligned}\left\||\psi_i^{\mathsf{bad},3}\rangle\right\| &= \left\|\mathsf{RstOE}_{f_{\mathsf{small}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0} |\psi_i\rangle - \Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_{\mathsf{small}}} |\psi_i^{\mathsf{good},2}\rangle\right\| \\ &= \left\|\Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_{\mathsf{small}}} \left(|\psi_i^{\mathsf{good},2}\rangle + |\psi_i^{\mathsf{bad},2}\rangle\right) - \Pi_{\mathsf{valid}}\mathsf{RstOE}_{f_{\mathsf{small}}} |\psi_i^{\mathsf{good},2}\rangle\right\| \\ &\le \left\||\psi_i^{\mathsf{bad},2}\rangle\right\| \le \left\||\psi_i^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i^2}{2^n}}\right).\end{aligned}$$

Thus the fourth property holds for $|\psi_i^{\mathsf{bad},3}\rangle$. The fourth property for $|\psi_i^{'\mathsf{bad},3}\rangle$ can be shown in the same way. □

The next lemma shows how the states $\mathsf{RstOE}_{f_{\mathsf{big}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0} |\psi_i'\rangle$ and $\mathsf{RstOE}_{f_{\mathsf{small}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0} |\psi_i\rangle$ change when $\mathsf{RstOE}^*_{f_1} \cdot \mathsf{XOR}^*$ acts on them.

Lemma 12 (Action of $\mathsf{RstOE}^*_{f_1} \cdot \mathsf{XOR}^*$)**.** *Suppose that there exist* i *and vectors* $|\psi_j^{'\mathsf{good}}\rangle$*,* $|\psi_j^{'\mathsf{bad}}\rangle$*,* $|\psi_j^{\mathsf{good}}\rangle$*, and* $|\psi_j^{\mathsf{bad}}\rangle$ *that satisfy the four properties in Proposition 16 for* $j = 1,\dots,i$*. Then, there exist vectors* $|\psi_i^{'\mathsf{good},4}\rangle$*,* $|\psi_i^{'\mathsf{bad},4}\rangle$*,* $|\psi_i^{\mathsf{good},4}\rangle$*, and* $|\psi_i^{\mathsf{bad},4}\rangle$ *that satisfy the following properties.*

1. $\mathsf{RstOE}^*_{f_1} \cdot \mathsf{XOR}^* \cdot \mathsf{RstOE}_{f_{\mathsf{big}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0} |\psi_i'\rangle = |\psi_i^{'\mathsf{good},4}\rangle + |\psi_i^{'\mathsf{bad},4}\rangle$ *and* $\mathsf{RstOE}^*_{f_1} \cdot \mathsf{XOR}^* \cdot \mathsf{RstOE}_{f_{\mathsf{small}}} \cdot \mathsf{XOR} \cdot \mathsf{RstOE}_{f_1} \cdot \mathsf{RstOE}_{f_0} |\psi_i\rangle = |\psi_i^{\mathsf{good},4}\rangle + |\psi_i^{\mathsf{bad},4}\rangle$.

2. *There exists complex number* $a^{(i),4}_{MTYZD_0D_1D_{\mathsf{big}}}$ *such that*

$$|\psi_i^{'\mathsf{good},4}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\perp}} a^{(i),4}_{MTYZD_0D_1D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes |D_0,D_1,D_{\mathsf{big}}\rangle \otimes |D_0(M)\rangle,$$

[5]Note that all the databases in $|\psi_i^{'\mathsf{good},3}\rangle$ and $|\psi_i^{\mathsf{good},3}\rangle$ with non-zero quantum amplitude are good, by definition of good database and the first property of Proposition 3 (the equations (3.12)–(3.15))

and

$$|\psi_i^{\mathsf{good},4}\rangle = \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)\neq\bot}} a^{(i),4}_{MTYZD_0D_1D_{\mathsf{big}}} |M,T\rangle|Y\rangle|Z\rangle \otimes |[D_0,D_1,D_{\mathsf{big}}]_{\mathsf{small}}\rangle \otimes |D_0(M)\rangle$$

hold, where (M,T), Y, and Z correspond to $\mathcal{A}$'s register to send queries to oracles, register to receive answers from oracles, and register for offline computation, respectively.

3. *For each database $(D_0,D_1,D_{\mathsf{big}})$ in $|\psi_i^{'\mathsf{good},4}\rangle$ (resp., $(D_0,D_1,D_{\mathsf{small}})$ in $|\psi_i^{\mathsf{good},4}\rangle$) with non-zero quantum amplitude, $|D_0|\le 2(i-1)+1$, $|D_1|\le 2i$, and $|D_{\mathsf{big}}|\le i$ (resp., $|D_{\mathsf{small}}|\le i$).*

4. $\left\||\psi_i^{'\mathsf{bad},4}\rangle\right\| \le \left\||\psi_i^{'\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i^2}{2^n}}\right)$ *and* $\left\||\psi_i^{\mathsf{bad},4}\rangle\right\| \le \left\||\psi_i^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i^2}{2^n}}\right)$ *hold.*

Proof. From Lemma 11, it follows that there exist vectors $|\psi_i^{'\mathsf{good},3}\rangle$, $|\psi_i^{'\mathsf{bad},3}\rangle$, $|\psi_i^{\mathsf{good},3}\rangle$, and $|\psi_i^{\mathsf{bad},3}\rangle$ that satisfy the four properties in Lemma 11.

Let Π_{prereg} denote the projection onto the space that is spanned by the vectors corresponding to preregular states. Note that, when we measure the states $\mathsf{RstOE}^*_{f_1}\cdot\mathsf{XOR}^*\cdot\mathsf{RstOE}_{f_{\mathsf{big}}}\cdot\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}\cdot\mathsf{RstOE}_{f_0}|\psi_i'\rangle$ and $\mathsf{RstOE}^*_{f_1}\cdot\mathsf{XOR}^*\cdot\mathsf{RstOE}_{f_{\mathsf{small}}}\cdot\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}\cdot\mathsf{RstOE}_{f_0}|\psi_i\rangle$, we always obtain preregular states (see (5.15)–(5.18)).

Define $|\psi_i^{'\mathsf{good},4}\rangle := \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}\mathsf{RstOE}^*_{f_1}\cdot\mathsf{XOR}^*|\psi_i^{'\mathsf{good},3}\rangle$, $|\psi_i^{'\mathsf{bad},4}\rangle := \mathsf{RstOE}^*_{f_1}\cdot\mathsf{XOR}^*\cdot\mathsf{RstOE}_{f_{\mathsf{big}}}\cdot\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}\cdot\mathsf{RstOE}_{f_0}|\psi_i'\rangle - |\psi_i^{'\mathsf{good},4}\rangle$, $|\psi_i^{\mathsf{good},4}\rangle := \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}\mathsf{RstOE}^*_{f_1}\cdot\mathsf{XOR}^*|\psi_i^{\mathsf{good},3}\rangle$, and $|\psi_i^{\mathsf{bad},4}\rangle := \mathsf{RstOE}^*_{f_1}\cdot\mathsf{XOR}^*\cdot\mathsf{RstOE}_{f_{\mathsf{small}}}\cdot\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}\cdot\mathsf{RstOE}_{f_0}|\psi_i\rangle - |\psi_i^{\mathsf{good},4}\rangle$. Then the first property obviously holds.

Since $\mathsf{XOR}^*=\mathsf{XOR}$, by applying the first property of Proposition 3 ((3.12)–(3.15)), we have

$$\begin{aligned}
\Pi_{\mathsf{prereg}}\mathsf{RstOE}^*_{f_1}\mathsf{XOR}^*|\psi_i^{'\mathsf{good},3}\rangle &= \Pi_{\mathsf{prereg}}\mathsf{RstOE}^*_{f_1}\sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)\neq\bot\wedge D_1(T)\neq\bot}} a^{(i),3}_{MTYZD_0D_1D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \otimes |D_0,D_1,D_{\mathsf{big}}\rangle\otimes|D_0(M)\rangle|D_1(T)\rangle\\
&= \Pi_{\mathsf{prereg}}\mathsf{RstOE}^*_{f_1}\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \otimes |D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}\rangle\otimes|D_0(M)\rangle|\alpha\rangle\\
&= \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \otimes |D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}\rangle\otimes|D_0(M)\rangle\\
&\quad+\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{1}{\sqrt{2^n}}a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \otimes|D_0\rangle\left(|D_1\rangle-\sum_{\gamma}\frac{1}{\sqrt{2^n}}|D_1\cup(T,\gamma)\rangle\right)|D_{\mathsf{big}}\rangle\otimes|D_0(M)\rangle\\
&\quad-\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{1}{2^n}a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \otimes|D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}\rangle\otimes|D_0(M)\rangle\\
&\quad+\frac{1}{2^{3n/2}}\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}|M,T\rangle|Y\rangle|Z\rangle \otimes|D_0\rangle\left(2\sum_{\delta}\frac{1}{\sqrt{2^n}}|D_1\cup(T,\delta)\rangle-|D_1\rangle\right)|D_{\mathsf{big}}\rangle\otimes|D_0(M)\rangle.
\end{aligned} \tag{5.43}$$

Similarly,

$$\Pi_{\mathsf{prereg}}\mathsf{RstOE}^{*}_{f_1}\mathsf{XOR}^{*}\left|\psi_i^{\mathsf{good},3}\right\rangle = \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\bot\wedge D_1(T)=\bot}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}\left|M,T\right\rangle\left|Y\right\rangle\left|Z\right\rangle \otimes\left|D_0,D_1\cup(T,\alpha),[D_{\mathsf{big}}]_{\mathsf{small}}\right\rangle\otimes\left|D_0(M)\right\rangle \tag{5.44}$$

$$+\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{1}{\sqrt{2^n}}a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}\left|M,T\right\rangle\left|Y\right\rangle\left|Z\right\rangle \otimes\left|D_0\right\rangle\left(\left|D_1\right\rangle-\sum_{\gamma}\frac{1}{\sqrt{2^n}}\left|D_1\cup(T,\gamma)\right\rangle\right)\left|[D_{\mathsf{big}}]_{\mathsf{small}}\right\rangle \otimes\left|D_0(M)\right\rangle \tag{5.45}$$

$$-\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{1}{2^n}a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}\left|M,T\right\rangle\left|Y\right\rangle\left|Z\right\rangle \otimes\left|D_0,D_1\cup(T,\alpha),[D_{\mathsf{big}}]_{\mathsf{small}}\right\rangle\otimes\left|D_0(M)\right\rangle \tag{5.46}$$

$$+\frac{1}{2^{3n/2}}\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\bot\wedge D_1(T)=\bot}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}\left|M,T\right\rangle\left|Y\right\rangle\left|Z\right\rangle \otimes\left|D_0\right\rangle\left(2\sum_{\delta}\frac{1}{\sqrt{2^n}}\left|D_1\cup(T,\delta)\right\rangle-\left|D_1\right\rangle\right)\left|[D_{\mathsf{big}}]_{\mathsf{small}}\right\rangle \otimes\left|D_0(M)\right\rangle \tag{5.47}$$

holds. Now, the second and third properties follows from the second and third properties of Lemma 11 and the equations (5.43)–(5.47).

Let $|(5.44)\rangle, \ldots, |(5.47)\rangle$ denote the terms (5.44)–(5.47), respectively. Then

$$\Pi_{\mathsf{bad}}\left|(5.44)\right\rangle = \Pi_{\mathsf{bad}}\left|(5.46)\right\rangle = 0 \tag{5.48}$$

since all the databases in (5.44) and (5.46) are good.

If a tuple $(T,(D_0,D_1,D_{\mathsf{big}}))$ satisfies that $D_1(T)=\bot$ and $(D_0,D_1,D_{\mathsf{big}})$ is bad, then the number of α such that

1. $(D_0,D_1\cup(T,\alpha),D_{\mathsf{big}})$ is good, and
2. there exists M' such that $D_0(M')\neq\bot$ and $[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot$

is at most $|D_0|\cdot|D_{\mathsf{big}}|\leq 2i^2$. In addition, if a tuple $(T,(D_0,D_1,D_{\mathsf{big}}))$ satisfies that $D_1(T)=\bot$ and $(D_0,D_1,D_{\mathsf{big}})$ is bad, then there does not exist α such that

1. $(D_0,D_1\cup(T,\alpha),D_{\mathsf{big}})$ is good, and
2. there does not exist M' such that $D_0(M')\neq\bot$ and $[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot$.

Therefore,

$$\left\|\Pi_{\mathsf{bad}}\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{1}{\sqrt{2^n}}a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}\left|M,T\right\rangle\left|Y\right\rangle\left|Z\right\rangle \otimes\left|D_0,D_1,[D_{\mathsf{big}}]_{\mathsf{small}}\right\rangle\otimes\left|D_0(M)\right\rangle\right\|^2$$

$$=\left\|\sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\(D_0,D_1,D_{\mathsf{big}}):\text{ bad}\\(D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\D_0(M)\neq\bot\wedge D_1(T)=\bot\\\exists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \frac{1}{\sqrt{2^n}}a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}\left|M,T\right\rangle\left|Y\right\rangle\left|Z\right\rangle \otimes\left|D_0,D_1,[D_{\mathsf{big}}]_{\mathsf{small}}\right\rangle\otimes\left|D_0(M)\right\rangle\right\|^2$$

$$
\begin{aligned}
&= \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}})\text{: bad}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{1}{2^n} \left| \sum_{\substack{\alpha;\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}})\text{:good}\\ \exists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} \right|^2 \\
&\leq \sum_{\substack{M,T,Y,Z,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1,D_{\mathsf{big}})\text{: bad}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{2i^2}{2^n} \sum_{\substack{\alpha;\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}})\text{:good}\\ \exists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \left| a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} \right|^2 \\
&\leq O\left(\frac{i^2}{2^n}\right)
\end{aligned} \tag{5.49}
$$

holds.

In addition, if a tuple $(T, (D_0, D_1, D_{\mathsf{big}}))$ satisfies that $D_1(T) = \bot$ and $(D_0, D_1 \cup (T, \gamma), D_{\mathsf{big}})$ is bad, then the number of α such that

1. $(D_0, D_1 \cup (T, \alpha), D_{\mathsf{big}})$ is good, and
2. there exists M' such that $D_0(M') \neq \bot$ and $[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M') \oplus \alpha) \neq \bot$

is at most $|D_0| \cdot |D_{\mathsf{big}}| \leq 2i^2$. Therefore,

$$
\begin{aligned}
&\left\| \Pi_{\mathsf{bad}} \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}})\text{:valid and good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot\\ \exists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \frac{1}{\sqrt{2^n}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} |M,T\rangle|Y\rangle|Z\rangle \right. \\
&\qquad \left. \otimes |D_0\rangle \left(\sum_{\gamma} \frac{1}{\sqrt{2^n}} |D_1 \cup (T,\gamma)\rangle \right) |[D_{\mathsf{big}}]_{\mathsf{small}}\rangle \otimes |D_0(M)\rangle \right\|^2 \\
&= \left\| \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}})\text{:good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot\\ (D_0,D_1\cup(T,\gamma),D_{\mathsf{big}})\text{: bad}\\ \exists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \frac{1}{2^n} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} |M,T\rangle|Y\rangle|Z\rangle \right. \\
&\qquad \left. \otimes |D_0, D_1 \cup (T,\gamma), [D_{\mathsf{big}}]_{\mathsf{small}}\rangle \otimes |D_0(M)\rangle \right\|^2 \\
&= \sum_{\substack{M,T,Y,Z,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\gamma),D_{\mathsf{big}})\text{: bad}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{1}{2^{2n}} \left| \sum_{\substack{\alpha;\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}})\text{:good}\\ \exists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} \right|^2 \\
&\leq \sum_{\substack{M,T,Y,Z,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\gamma),D_{\mathsf{big}})\text{: bad}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{2i^2}{2^{2n}} \sum_{\substack{\alpha;\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}})\text{:good}\\ \exists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \left| a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} \right|^2 \\
&\leq \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}})\text{:good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot\\ \exists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \frac{2i^2}{2^n} \left| a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} \right|^2 \\
&\leq O\left(\frac{i^2}{2^n}\right)
\end{aligned} \tag{5.50}
$$

holds. Moreover, if a tuple $(T, (D_0, D_1 \cup (T,\alpha), D_{\mathsf{big}}))$ satisfies

1. $D_1(T) = \bot$ and $(D_0, D_1 \cup (T,\alpha), D_{\mathsf{big}})$ is good, and
2. there does not exist M' such that $D_0(M') \neq \bot$ and $[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M') \oplus \alpha) \neq \bot$,

then the number of γ such that $(D_0, D_1 \cup (T,\gamma), D_{\mathsf{big}})$ becomes bad is at most $|D_0| \cdot |D_{\mathsf{big}}| \leq 2i^2$. Therefore,

$$\left\| \Pi_{\mathsf{bad}} \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot\\ \nexists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \frac{1}{\sqrt{2^n}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes |D_0\rangle \left(\sum_\gamma \frac{1}{\sqrt{2^n}} |D_1 \cup (T,\gamma)\rangle \right) |[D_{\mathsf{big}}]_{\mathsf{small}}\rangle \otimes |D_0(M)\rangle \right\|^2$$

$$= \left\| \sum_{\substack{M,T,Y,Z,\alpha,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot\\ (D_0,D_1\cup(T,\gamma),D_{\mathsf{big}}):\text{ bad}\\ \nexists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \frac{1}{2^n} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes |D_0, D_1 \cup (T,\gamma), [D_{\mathsf{big}}]_{\mathsf{small}}\rangle \otimes |D_0(M)\rangle \right\|^2$$

$$= \sum_{\substack{M,T,Y,Z,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\gamma),D_{\mathsf{big}}):\text{ bad}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} \left| \sum_{\substack{\alpha;\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{good}\\ \nexists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \frac{a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}}}{2^n} \right|^2$$

$$\leq \sum_{\substack{M,T,Y,Z,\gamma,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\gamma),D_{\mathsf{big}}):\text{ bad}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} \sum_{\substack{\alpha;\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{good}\\ \nexists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \frac{\left| a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} \right|^2}{2^n}$$

$$= \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot\\ \nexists M'\text{s.t.}D_0(M')\neq\bot\wedge[D_{\mathsf{big}}]_{\mathsf{small}}(D_0(M')\oplus\alpha)\neq\bot}} \left| a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} \right|^2 \cdot \frac{\left| \left\{ \gamma \middle| (D_0, D_1 \cup (T,\gamma), D_{\mathsf{big}}) \text{ is bad} \right\} \right|}{2^n}$$

$$\leq O\left(\frac{i^2}{2^n}\right) \tag{5.51}$$

holds. From (5.50) and (5.51),

$$\left\| \Pi_{\mathsf{bad}} \sum_{\substack{M,T,Y,Z,\alpha,(D_0,D_1,D_{\mathsf{big}});\\ (D_0,D_1\cup(T,\alpha),D_{\mathsf{big}}):\text{valid and good}\\ D_0(M)\neq\bot\wedge D_1(T)=\bot}} \frac{1}{\sqrt{2^n}} a^{(i),3}_{MTYZD_0D_1\cup(T,\alpha)D_{\mathsf{big}}} |M,T\rangle |Y\rangle |Z\rangle \otimes |D_0\rangle \left(\sum_\gamma \frac{1}{\sqrt{2^n}} |D_1 \cup (T,\gamma)\rangle \right) |[D_{\mathsf{big}}]_{\mathsf{small}}\rangle \otimes |D_0(M)\rangle \right\|^2$$

$$\leq O\left(\frac{i^2}{2^n}\right) \tag{5.52}$$

follows.

Since (5.49) and (5.52) hold, we have

$$\|\Pi_{\mathsf{bad}}\,|(5.45)\rangle\| \le O\left(\sqrt{\frac{i^2}{2^n}}\right), \|\Pi_{\mathsf{bad}}\,|(5.47)\rangle\| \le O\left(\sqrt{\frac{i^2}{2^n}}\right). \tag{5.53}$$

Therefore,

$$\left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}\mathsf{RstOE}^*_{f_1}\mathsf{XOR}^*\,|\psi_i^{\mathsf{good},3}\rangle\right\| \le O\left(\sqrt{\frac{i^2}{2^n}}\right)$$

follows from (5.44)–(5.47), and (5.48) and (5.53). Thus we have

$$\begin{aligned}
\left\||\psi_i^{\mathsf{bad},4}\rangle\right\| &= \left\|\mathsf{RstOE}^*_{f_1}\cdot\mathsf{XOR}^*\cdot\mathsf{RstOE}_{f_{\mathsf{big}}}\cdot\mathsf{XOR}\cdot\mathsf{RstOE}_{f_1}\cdot\mathsf{RstOE}_{f_0}\,|\psi_i\rangle - |\psi_i^{\mathsf{good},4}\rangle\right\| \\
&= \left\|\Pi_{\mathsf{prereg}}\mathsf{RstOE}^*_{f_1}\cdot\mathsf{XOR}^*\left(|\psi_i^{\mathsf{good},3}\rangle + |\psi_i^{\mathsf{bad},3}\rangle\right) - \Pi_{\mathsf{good}}\Pi_{\mathsf{prereg}}\mathsf{RstOE}^*_{f_1}\mathsf{XOR}^*\,|\psi_i^{\mathsf{good},3}\rangle\right\| \\
&\le \left\|\Pi_{\mathsf{bad}}\Pi_{\mathsf{prereg}}\mathsf{RstOE}^*_{f_1}\cdot\mathsf{XOR}^*\,|\psi_i^{\mathsf{good},3}\rangle\right\| + \left\||\psi_i^{\mathsf{bad},3}\rangle\right\| \\
&\le \left\||\psi_i^{\mathsf{bad},3}\rangle\right\| + O\left(\sqrt{\frac{i^2}{2^n}}\right) \le \left\||\psi_i^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i^2}{2^n}}\right)
\end{aligned}$$

which implies that the fourth property for $|\psi_i^{\mathsf{bad},4}\rangle$ holds. The fourth property for $|\psi_i^{'\mathsf{bad},4}\rangle$ can be shown in the same way. □

Proof of Proposition 16. We prove the proposition by induction on i. The claim obviously holds when $i = 1$ by setting $|\psi_1^{'\mathsf{bad}}\rangle = 0$ and $|\psi_1^{\mathsf{bad}}\rangle = 0$.

Suppose that the claim holds for $i = 1, \ldots, k$ for some k. Then, by Lemma 9, Lemma 10, Lemma 11, and Lemma 12, there exist vectors $|\psi_k^{'\mathsf{good},4}\rangle$, $|\psi_k^{'\mathsf{bad},4}\rangle$, $|\psi_k^{\mathsf{good},4}\rangle$, and $|\psi_k^{\mathsf{bad},4}\rangle$ that satisfy the first, second, and third properties in Lemma 12, and

$$\left\||\psi_k^{'\mathsf{bad},4}\rangle\right\| \le \left\||\psi_k^{'\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{k^2}{2^n}}\right), \quad \left\||\psi_k^{\mathsf{bad},4}\rangle\right\| \le \left\||\psi_k^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{k^2}{2^n}}\right) \tag{5.54}$$

hold. Moreover, in the same way as we showed Lemma 12, we can show that there exist vectors $|\psi_{k+1}^{'\mathsf{good}}\rangle$, $|\psi_{k+1}^{'\mathsf{bad}}\rangle$, $|\psi_{k+1}^{\mathsf{good}}\rangle$, and $|\psi_{k+1}^{\mathsf{bad}}\rangle$ that satisfy the first, second, and third properties in Proposition 16, and

$$\left\||\psi_{k+1}^{'\mathsf{bad}}\rangle\right\| \le \left\||\psi_k^{'\mathsf{bad},4}\rangle\right\| + O\left(\sqrt{\frac{k^2}{2^n}}\right), \quad \left\||\psi_{k+1}^{\mathsf{bad}}\rangle\right\| \le \left\||\psi_k^{\mathsf{bad},4}\rangle\right\| + O\left(\sqrt{\frac{k^2}{2^n}}\right) \tag{5.55}$$

hold[6]. From (5.54) and (5.55), it follows that $|\psi_{k+1}^{'\mathsf{good}}\rangle$, $|\psi_{k+1}^{'\mathsf{bad}}\rangle$, $|\psi_{k+1}^{\mathsf{good}}\rangle$, and $|\psi_{k+1}^{\mathsf{bad}}\rangle$ also satisfy the fourth property of Proposition 16. Therefore the claim of Proposition 16 also holds for $i = k + 1$, which completes the proof. □

Now we can show Proposition 14.

Proof of Proposition 14. Since $\mathsf{FSF}_{\mathsf{big}}$ is completely indistinguishable from a random function, we have that

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{FSF}_{\mathsf{small}}}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{dist}}_{\mathsf{FSF}_{\mathsf{small}},\mathsf{FSF}_{\mathsf{big}}}(\mathcal{A})$$

holds. In addition, since Proposition 16 holds, by applying Proposition 15, we obtain

$$\mathbf{Adv}^{\mathrm{dist}}_{\mathsf{FSF}_{\mathsf{small}},\mathsf{FSF}_{\mathsf{big}}}(\mathcal{A}) \le \sum_{1\le i\le q} O\left(\sqrt{\frac{i^2}{2^n}}\right) + \sum_{1\le i\le q} O\left(\sqrt{\frac{i^2}{2^n}}\right) \le O\left(\sqrt{\frac{q^4}{2^n}}\right), \tag{5.56}$$

which completes the proof. □

5.2.6 Finishing the Proof of Theorem 11

Theorem 11 immediately follows from Proposition 13 and Proposition 14.

[6] $\mathsf{RstOE}^*_{f_1}\mathsf{XOR}^*$ in the proof of Lemma 12 corresponds to $U_k\mathsf{RstOE}^*_{f_0}$ in this proof. U_k is the unitary operator that corresponds to $\mathcal{A}$'s offline computation after the k-th query.

Chapter 6

Tight Quantum Security Bound of HMAC and NMAC in the QROM

This chapter contributes to understanding (post-)quantum security of symmetric-key cryptography mainly from the practical perspective. HMAC and NMAC are the most basic and important construction to convert Merkle-Damgård hash functions into PRFs. There already exists a previous work on quantum security of HMAC and NMAC [SY17] in the standard model, but it guarantees the security only up to $O(2^{n/5})$ or $O(2^{n/8})$ quantum queries in the QROM. This chapter proves that $O(2^{n/3})$ is the tight quantum security bound of HMAC and NMAC in the QROM (for short messages). The gap between $O(2^{n/3})$ and $O(2^{n/5})$ (or $O(2^{n/8})$) is significant in practical use cases. The result of this chapter shows that we can achieve a highly quantum-secure PRF and MAC from a hash function (or, a compression function of fixed input-output length) by using HMAC and NMAC. See also Section 1.4 for a more detailed overview, and Section 1.7 for the relationship of the results in this chapter with those in other chapters.

The organization of the chapter is as follows. Section 6.1 discusses about the security bound given in the previous work [SY17]. Section 6.2 provides a technical overview of our security proofs. Section 6.3 introduces a few technical lemmas that are used in later sections. Section 6.4 proves a proposition that is the technically hardest part in our proofs. Section 6.5 provides the security proofs of HMAC and NMAC by using the result of Section 6.4. Note that this chapter focuses on information-theoretic adversaries.

6.1 On the Security Bound Given in [SY17]

This section explains why the result in [SY17] guarantees security of NMAC up to $O(2^{n/8})$ or $O(2^{n/5})$ quantum queries when the compression function is ideally random. (Almost the same arguments apply to HMAC.)

We can reasonably deduce that the security is guaranteed up to $O(2^{n/8})$ quantum queries, and have the bound $O(2^{n/5})$ instead of $O(2^{n/8})$ if we assume a conjecture.

First, we describe the original result on NMAC in the standard model (under the assumption that the compression function is a qPRF), and then translate it into the corresponding claim in the quantum random oracle model where the compression function is a random oracle.

6.1.0.1 The Original Result on NMAC

Let $f : \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ be a function, and for each $K \in \{0,1\}^n$ let f_K denote the function $f_K(x) = f(x||K)$. For an adversary $\mathcal{A}$ and the keyed function f_K, define the *qPRF advantage under random leakage* by

$$\mathbf{Adv}^{\text{qPRF-rl}}_{f_K}(\mathcal{A}) := \left|\Pr\left[1 \leftarrow \mathcal{A}^{f_K,H}(H(K))\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\rho,H}(w)\right]\right|, \tag{6.1}$$

where $\rho : \{0,1\}^m \to \{0,1\}^n$ and $H : \{0,1\}^n \to \{0,1\}^n$ are random functions, and $w \xleftarrow{\$} \{0,1\}^n$.

In the previous work, Song and Yun showed the following proposition.

Proposition 17 (Theorem 5.2 in [SY17])**.** *For any adversary $\mathcal{A}$ that makes at most Q quantum queries to NMAC or a random function, where the length of each message is upper bounded by $m \cdot \ell$, we can construct adversaries $\mathcal{A}_d$ and $\mathcal{A}_{rl}$ such that*

$$\mathbf{Adv}^{\text{qPRF}}_{\text{NMAC}^f_{K_1,K_2}}(\mathcal{A}) \le \mathbf{Adv}^{\text{qPRF}}_{f_K}(\mathcal{A}_d) + 34(\ell+1)\sqrt{Q^3 \cdot \mathbf{Adv}^{\text{qPRF-rl}}_{f_K}(\mathcal{A}_{rl})}, \tag{6.2}$$

where $\mathcal{A}_d$ makes at most Q quantum queries to f_K or a random function, and $\mathcal{A}_{rl}$ makes at most $4Q$ queries to f_K or a random function and at most $6Q$ queries to H.

6.1.0.2 Translation of Proposition 17 into the QROM

Now, suppose that f is a random oracle. Then, similarly to (6.1), we can define the qPRF advantage under random leakage by

$$\mathbf{Adv}^{\text{qPRF-rl}}_{f_K}(\mathcal{A}) := \left|\Pr\left[1 \leftarrow \mathcal{A}^{f_K,f,H}(H(K))\right] - \Pr\left[1 \leftarrow \mathcal{A}^{\rho,f,H}(w)\right]\right|, \tag{6.3}$$

where $\rho : \{0,1\}^m \to \{0,1\}^n$ and $H : \{0,1\}^n \to \{0,1\}^n$ are random functions that are independent of f.

In what follows, let us assume $m = n$ for simplicity. Then, the proposition in the QROM (where the compression function f is a quantum random oracle) that correspond to Proposition 17 would be like the following proposition, though we do not provide a formal proof.

Proposition 18. *For any adversary $\mathcal{A}$ that makes at most Q quantum queries to NMAC or a random function and the quantum random oracle f, where the length of each message is upper bounded by $m \cdot \ell$, we can construct adversaries $\mathcal{A}_d$ and $\mathcal{A}_{rl}$ such that*

$$\mathbf{Adv}^{\text{qPRF}}_{\mathsf{NMAC}^f_{K_1,K_2}}(\mathcal{A}) \le \mathbf{Adv}^{\text{qPRF}}_{f_K}(\mathcal{A}_d) + O\left(\sqrt{\ell^2 Q^3 \cdot \mathbf{Adv}^{\text{qPRF-rl}}_{f_K}(\mathcal{A}_{rl})}\right), \tag{6.4}$$

where $\mathcal{A}_d$ makes at most $O(Q)$ quantum queries to f_K or a random function and at most $O(Q)$ quantum queries to the random oracle f, and $\mathcal{A}_{rl}$ makes at most $O(Q)$ quantum queries to f_K or a random function and at most $O(Q)$ quantum queries to the random oracles f and H.

Let $\mathbf{Adv}^{\text{qPRF}}_{f_K}(Q) := \max_{\mathcal{A}} \mathbf{Adv}^{\text{qPRF}}_{f_K}(\mathcal{A})$ and $\mathbf{Adv}^{\text{qPRF-rl}}_{f_K}(Q) := \max_{\mathcal{A}} \mathbf{Adv}^{\text{qPRF-rl}}_{f_K}(\mathcal{A})$, where the maximum is taken over all adversaries that make at most Q queries to each oracle. Then,

$$\mathbf{Adv}^{\text{qPRF}}_{f_K}(Q) \le \mathbf{Adv}^{\text{qPRF-rl}}_{f_K}(Q) \tag{6.5}$$

apparently holds since some information on K is leaked via H (when $\mathcal{A}$ runs relative to f_K).

Now, let us assume

$$\mathbf{Adv}^{\text{qPRF-rl}}_{f_K}(Q) = \mathbf{Adv}^{\text{qPRF}}_{f_K}(Q),$$

which may overestimate (but never underestimate) the security claim shown in Proposition 18. Then

$$\mathbf{Adv}^{\text{qPRF-rl}}_{f_K}(Q) = \mathbf{Adv}^{\text{qPRF}}_{f_K}(Q) \le O\left(\sqrt{\frac{Q^2}{2^n}}\right) \tag{6.6}$$

holds by Lemma 13. Therefore,

$$\mathbf{Adv}^{\text{qPRF}}_{\mathsf{NMAC}^f_{K_1,K_2}}(\mathcal{A}) \le O\left(\sqrt[4]{\frac{\ell^4 \cdot Q^8}{2^n}}\right). \tag{6.7}$$

follows from (6.4). When $\ell = O(1)$, the inequality (6.7) guarantees the security of NMAC only up to $O(2^{n/8})$ queries.

6.1.0.3 The Bound $O(2^{n/5})$ Based on a Conjecture

The final bound (6.7) is based on Lemma 13, which provides the current best qPRF security bound of f_K in the QROM as far as we know. However, we are not sure if the bound is tight because we do not know any distinguishing attack that matches the bound of Lemma 13.

If we assume the following conjecture instead of (6.6), we obtain the bound $O(2^{n/5})$ instead of $O(2^{n/8})$.

Conjecture 1. *It holds that* $\mathbf{Adv}^{\text{qPRF-}rl}_{f_K}(Q) = \mathbf{Adv}^{\text{qPRF}}_{f_K}(Q) \le O\left(Q^2/2^n\right)$.[1]

If we assume this, from (6.4) we obtain

$$\mathbf{Adv}^{\text{qPRF}}_{\mathsf{NMAC}^f_{K_1,K_2}}(\mathcal{A}) \le O\left(\sqrt{\frac{\ell^2 \cdot Q^5}{2^n}}\right) \tag{6.8}$$

instead of (6.7). When $\ell = O(1)$, the inequality (6.8) guarantees the security of NMAC only up to $O(2^{n/5})$ queries.

[1] This bound matches the bound by the Grover search.

6.2 Technical Overview

Let $h : \{0,1\}^{m+n} \to \{0,1\}^n$ be a quantum random oracle. The technically hardest part to prove the security bound of HMAC and NMAC is to show the indistinguishability of the function $F_1^h(u,v) := h(v, f(u))$ from a random function, where $u \in \{0,1\}^n$, $v \in \{0,1\}^m$, and $f : \{0,1\}^n \to \{0,1\}^n$ is a random function that is independent of h. (Adversaries have a direct oracle access to the quantum random oracle h, but only indirect access to f. That is, adversaries can query to f only through queries to F_1^h, and cannot observe the output values of f. See also Fig. 6.1.) Once we show the indistinguishability of F_1^h, the remaining proofs can be done with simpler proof techniques. It turns out that previous

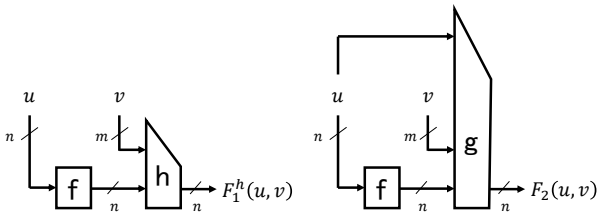


Figure 6.1: F_1^h and F_2. h is a quantum random oracle that adversaries can directly access. f and g are random functions that are independent from h.

techniques cannot be directly used to prove the indistinguishability of F_1^h. Thus we introduce a technique which we call *equivalent databases*.

Recall that we denote the distinguishing advantage of an adversary $\mathcal{A}$ between (pair of) oracles (O_1^h, h) and (O_2, h) by $\mathbf{Adv}^{\mathrm{dist}}_{(O_1^h,h),(O_2,h)}(\mathcal{A})$, where h is a quantum random oracle and O_1^h depends on h. Let RF be a random function that is independent of h. As we described above, the technically hardest part to show the tight security bound of HMAC and NMAC is to show the following proposition.

Proposition 19 (Technically hardest proposition to show, informal)**.** *If $\mathcal{A}$ makes at most q queries to each oracle,* $\mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(\mathsf{RF},h)} \leq O(\sqrt{q^3/2^n})$ *holds.*

Let F_2 be the function defined by $F_2(u,v) := g(u,v,f(u))$, where $g : \{0,1\}^n \times \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ is another random function (see also Fig. 6.1). Then, since g is a random function, $\mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(\mathsf{RF},h)}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(F_2,h)}(\mathcal{A})$ holds. In what follows, we present an overview of how we show

$$\mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(F_2,h)}(\mathcal{A}) \leq O\left(\sqrt{q^3/2^n}\right), \tag{6.9}$$

instead of directly showing Proposition 19. [2] For bit strings x and y, we identify the concatenation $x||y$ and the pair (x,y).

Following usual terminology on provable security in symmetric-key cryptology, we call (direct) queries to h *offline queries* because h is an ideal model of a public function that adversaries can compute offline. In addition, we call queries to F_1^h and F_2 *online queries* because the oracles of F_1^h and F_2 model the keyed functions that adversaries can compute only by making online queries.

6.2.1 Classical Proof Intuitions

If our goal were to show the indistinguishability of F_1^h and F_2 in the *classical* setting, we could show it based on the following idea by using the *lazy sampling* technique to f, g, and h:

> *If $\mathcal{A}$ cannot guess outputs of f, and outputs of f do not collide, then the outputs of F_1^h and F_2 seem completely random and indistinguishable.*

More precisely, a (classical) adversary $\mathcal{A}$ cannot distinguish F_1^h and F_2 as long as the following two bad events hit and coll do not happen.[3]

[2] We consider F_2 instead of RF so that there exists a useful correspondence between "good" databases for F_1^h and those for F_2, which we will elaborate later.

[3] We use the symbols u and ζ to denote n-bit strings and v to denote an m-bit string.

hit: $\mathcal{A}$ succeeds in guessing a previous output of f and queries it to h. That is, $\mathcal{A}$ has queried $u||v'$ to the online keyed oracle (F_1^h or F_2) before, and now $\mathcal{A}$ queries $v||f(u)$ to h (for some $v \in \{0,1\}^m$).

coll: A new output of f (which is sampled during an online query) happens to collide with either of (a) a previous output of f, or (b) the least significant n-bit ζ of a previous offline query $v||\zeta$ to h.

Our proof for the *classical* indistinguishability would be as follows: First, we show that F_1^h and F_2 are completely indistinguishable as long as hit and coll do not happen. Second, we show that Pr[hit] and Pr[coll] are small. Let coll_i denote the event that coll happens at the i-th query. Then, by using the randomness of outputs of f, we can show $\Pr[\mathsf{coll}_i] \leq O(i/2^n)$ for each i, which implies that $\Pr[\mathsf{coll}] \leq \sum_{1\leq i\leq q} \Pr[\mathsf{coll}_i] \leq \sum_{1\leq i\leq q} O(i/2^n) = O(q^2/2^n)$. Similarly, $\Pr[\mathsf{hit}] \leq O(q^2/2^n)$ can be shown. (Actually there exists a qualitative difference between the proof for $\Pr[\mathsf{coll}] \leq O(q^2/2^n)$ and that for $\Pr[\mathsf{hit}] \leq O(q^2/2^n)$, which will be explained later). Hence we can show $\mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(F_2,h)}(\mathcal{A}) \leq \Pr[\mathsf{coll}] + \Pr[\mathsf{hit}] \leq O(q^2/2^n)$ in the classical setting.

6.2.2 How to Show Quantum Indistinguishability?

When we show the *quantum* indistinguishability of F_1^h and F_2, it is natural to combine the above *classical* idea with some quantum proof techniques developed in previous works. Indeed, our first idea toward a quantum proof is to combine the above classical idea with a quantum technique used in Chapter 4 and Chapter 5. [4] However, actually it turns out that they cannot be simply combined. The issue is attributed to our situation where we have to deal with the bad event hit that "$\mathcal{A}$'s *offline* query to h collides with a previous output of f in the *online* oracle".

Below, we explain (1) an overview of the quantum proof technique in Chapter 4 and Chapter 5, (2) what kind of issue arises if we combine the above classical idea with the previous quantum technique, and that (3) we can solve the issue by introducing a new proof technique which we name *equivalent databases*.

6.2.3 Proof Technique in Chapter 4 and Chapter 5

Roughly speaking, we showed quantum oracle indistinguishability of certain two oracles in Chapter 4 and Chapter 5 as follows.

1. Suppose that random functions from which the oracles are built (in our case, f, g, and h) are implemented by using RstOE so that we can use intuitions of classical lazy sampling in quantum proofs to some extent (let D_f, D_g, and D_h denote *databases* associated with RstOE for f, g, and h, respectively, which correspond to transcripts of queries in the classical setting).

2. Based on classical proof ideas of using good and bad events, define the notion of *good* and *bad* for tuples of databases (in our case, (D_f, D_h) for F_1^h and (D_f, D_g, D_h) for F_2) in such a way that

   (a) There exists a one-to-one correspondence between good databases for one oracle (in our case, good databases (D_f, D_h) for F_1^h) and good databases for the other oracle (in our case, good databases (D_f, D_g, D_h) for F_2).

   (b) The behavior of one oracle (in our case, F_1^h) on a good database is the same as that of the other oracle (in our case, F_2) on the corresponding good database.

3. By using (a) and (b), show that the oracles (in our case, the pairs of the oracles (F_1^h, h) and (F_2, h)) are completely indistinguishable as long as databases are good.

4. Show that the probability (in some sense) that good databases change to bad databases is very small at each query.

Note that, unlike the classical setting, even if the record "x has been queried to f and responded with y" is stored in a database D_f for f, there is a possibility that the record will be overwritten as "x has not been queried to f before", or "x has been queried to f and responded with y'" for some y' such that $y \neq y'$. Hence it is not necessarily trivial how to define good and bad databases in such a way that we can formally prove both of (a) and (b) hold.

Next, we explain what kind of issue happens when we apply the above idea to our situation. In short, the issue lies in the last one of the above four steps.

[4] In Zhandry's paper that introduced the compressed oracle technique, quantum indifferentiability of the *fixed-input-length* Merkle-Damgård construction is proved [Zha19]. Note that the *variable-input-length* Merkle-Damgård construction that is used in HMAC and NMAC is not indifferentiable in the random oracle model even in the classical setting [CDMP05]. In addition, the security bound of the indifferentiability is proved up to $O(2^{n/4})$ (but not $O(2^{n/3})$) quantum queries in [Zha19]. Thus, we start from the proof technique used in Chapter 4 and Chapter 5 instead of [Zha19].

6.2.4 An Issue with Our Situation

In Chapter 4 and Chapter 5, each adversary can access to only a single *keyed* oracle. Roughly speaking, a good database changes to bad only when a fresh value x is (indirectly) queried to a random function RF, and the newly sampled value $y := \mathsf{RF}(x)$ happens to collide with an existing record in a database (i.e., a bad event that correspond to coll in our situation).

On the other hand, in our situation, a good database also changes to bad when *an adversary succeeds to query $v||\zeta$ to h such that ζ collides with a previous output of f* (i.e., hit occurs).

This difference causes an issue to prove that the "bad" probability is small. Unlike the lazy sampling that always chooses values uniformly at random, (quantum) adversaries can choose offline (quantum) queries to h arbitrarily and *adaptively*. Thus, an adversary may have strong ability to succeed to cause hit, even if the probability of coll is small.

Note that how to deal with adaptive queries to offline queries is not an easy issue even in the classical setting. To reduce the arguments on adaptive queries into those on non-adaptive arguments, sophisticated proof techniques such as the coefficients H technique [Pat08] are usually used.

6.2.5 How to Solve the Issue

Our key intuition to solve the issue is, for arbitrary good database (D_f, D_h) for F_1^h that an adversary $\mathcal{A}$ is trying to change to be bad, there would be sufficiently many good databases (D'_f, D'_h) that $\mathcal{A}$ cannot distinguish from (D_f, D_h).

Suppose that (I) $\mathcal{A}$ is running relative to F_1^h and h, and has made $(i-1)$ queries in total, (II) both of the bad events coll and hit have not happened, and (III) now $\mathcal{A}$ chooses a bit string $\tilde{v}||\tilde{\zeta}$ to query to h, trying to cause hit at the i-th query.

Let D_f and D_h be the current databases for f and h (before the i-th query). Then there exist $u_1, \ldots, u_s, \alpha_1, \ldots, \alpha_s \in \{0,1\}^n$ $(s \leq i-1)$ such that $D_f = ((u_1, \alpha_1), \ldots, (u_s, \alpha_s))$. Intuitively, α_j is equal to $f(u_j)$. Since bad events have not happened yet, D_f does not contain any collision (i.e., $\alpha_i \neq \alpha_j$ for $i \neq j$).

Let hit_i denote the event that hit occurs at the i-th query (to h). Then, hit_i occurs when $\mathcal{A}$ successfully chooses a value $\tilde{v}||\tilde{\zeta}$ such that $\tilde{\zeta} = \alpha_j$ holds for some j. Our current goal is to prove that $\Pr[\mathsf{hit}_i]$ is very small.

To achieve this goal, we show that $\Pr\left[\mathsf{hit}_i \middle| \mathcal{A} \text{ chooses } \tilde{v}||\tilde{\zeta}\right]$ is very small for *arbitrary* $\tilde{v}||\tilde{\zeta}$, by focusing on the freedom of the choices of the values $f(u_1) = \alpha_1, \ldots, f(u_s) = \alpha_s$. Intuitively, even if the value $\alpha_j (= f(u_j))$ in the element $(u_j, \alpha_j) \in D_f$ is replaced with another value α'_j, $\mathcal{A}$ does not notice since $\mathcal{A}$ does not observe output values of f. This means that the choices of the values $f(u_1) = \alpha_1, \ldots, f(u) = \alpha_s$ have some degree of freedom, even after $\mathcal{A}$ has chosen which value $\tilde{v}||\tilde{\zeta}$ to query to h. We use this degree of freedom to bound the probability $\Pr\left[\mathsf{hit}_i \middle| \mathcal{A} \text{ chooses } \tilde{v}||\tilde{\zeta}\right]$ (actually we will show a stronger result).

To provide a proof based on the above intuition, we introduce the notion of *equivalent databases* as follows.

Definition 3 (Equivalent database, informal)**.** *A (good) database (D'_f, D'_h) is said to be equivalent to (D_f, D_h) if $|D'_f| = |D_f|$, $|D'_h| = |D_h|$, and (D'_f, D'_h) is equal to (D_f, D_h) except for the choices of the output values of f.*

We present an example to illustrate the intuition on equivalent databases. Let $D_f := ((u_1, \alpha_1), (u_2, \alpha_2))$ and $D_h := ((v_1||\alpha_1, w_1), (v_2^{(1)}||\alpha_2, w_2^{(1)}), (v_2^{(2)}||\alpha_2, w_2^{(2)}), (v_3||\zeta_3, w_3))$. This corresponds to the situation where $u_1||v_1$, $u_2||v_2^{(1)}$, $u_2||v_2^{(2)}$ have been queried to F_1^h, and $v_3||\zeta_3$ has been queried to h. See also Fig. 6.2. The adversary observes that $F_1^h(u_1||v_1) = w_1$, $F_1^h(u_2||v_2^{(1)}) = w_2^{(1)}$, $F_1^h(u_2||v_2^{(2)}) = w_2^{(2)}$, and $h(v_3||\zeta_3) = w_3$, but does not know the values $\alpha_1 = f(u_1)$ and $\alpha_2 = f(u_2)$. Suppose $\alpha_1, \alpha_2, \zeta_3$ are distinct, which implies that (D_f, D_h) is a good database. Then, another good database (D'_f, D'_h) is equivalent to (D_f, D_h) if and only if there exist α'_1 and α'_2 such that $\alpha'_1, \alpha'_2, \zeta_3$ are distinct, $D'_f = ((u_1, \alpha'_1), (u_2, \alpha'_2))$, and $D'_h = ((v_1||\alpha'_1, w_1), (v_2^{(1)}||\alpha'_2, w_2^{(1)}), (v_2^{(2)}||\alpha'_2, w_2^{(2)}), (v_3||\zeta_3, w_3))$.

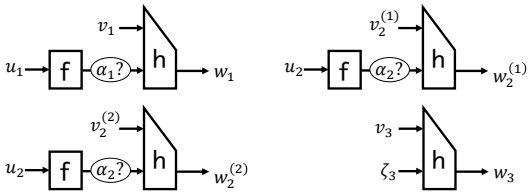


Figure 6.2: The situation that corresponds to the good database (D_f, D_h). The adversary has no information on α_1 and α_2 expect that $\alpha_1, \alpha_2, \zeta_3$ are distinct. We say that another good database (D'_f, D'_h) is equivalent to (D'_f, D'_h) if and only if (D_f, D_h) is equal to (D_f, D_h) except for the choice of the values for α_1 and α_2.

Let $\mathsf{Equiv}(D_f, D_h)$ be the set of good databases that are equivalent to (D_f, D_h). Then, intuitively, the following properties hold:

1. The probability that a database happens to become (D_f, D_h) (after $\mathcal{A}$ made $(i-1)$ queries) is equal to the probability that the database happens to become (D'_f, D'_h), for any $(D'_f, D'_h) \in \mathsf{Equiv}(D_f, D_h)$.

2. The ratio between (I) the number of $(D'_f, D'_h) \in \mathsf{Equiv}(D_f, D_h)$ that leads to the bad event hit_i (i.e., $\alpha_j = \tilde{\zeta}$ for some j) and (II) the size of the entire set $\mathsf{Equiv}(D_f, D_h)$ is at most about $\approx |D_f|/2^n \leq O(i/2^n)$. [5]

From the above two properties it follows that, for arbitrary $\tilde{v}||\tilde{\zeta}$ *and arbitrary good* (D_f, D_h),

$$\Pr\left[\mathsf{hit}_i \middle| \mathcal{A} \text{ chooses } \tilde{v}||\tilde{\zeta} \wedge \text{ database is equivalent to } (D_f, D_h)\right] \leq O\left(i/2^n\right)$$

holds. This implies that $\Pr[\mathsf{hit}_i] \leq O(i/2^n)$.

The above explanations are in fact based on classical intuitions. To show they also work in the quantum setting, we carefully analyze quantum amplitude (complex coefficients) of state vectors.

6.2.6 Finishing the Proof

Now we have $\Pr[\mathsf{hit}_i] \leq O(\frac{i}{2^n})$ in the quantum setting. We can also show $\Pr[\mathsf{coll}_i] \leq O(\frac{i}{2^n})$ with the technique in Chapter 4 and Chapter 5.

In the classical setting, the distinguishing advantage is upper bounded by $\mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(F_2,h)}(\mathcal{A}) \leq \Pr[\mathsf{hit}] + \Pr[\mathsf{coll}] \leq \sum_{1\leq i\leq q}\Pr[\mathsf{hit}_i] + \sum_{1\leq i\leq q}\Pr[\mathsf{coll}_i]$. On the other hand, roughly speaking, the quantum distinguishing advantage is upper bounded by $\mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(F_2,h)}(\mathcal{A}) \leq \sum_{1\leq i\leq q}\sqrt{\Pr[\mathsf{hit}_i]} + \sum_{1\leq i\leq q}\sqrt{\Pr[\mathsf{coll}_i]}$. Therefore, we obtain the bound as $\mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(F_2,h)}(\mathcal{A}) \leq \sum_{1\leq i\leq q} O\left(\sqrt{i/2^n}\right) + \sum_{1\leq i\leq q} O\left(\sqrt{i/2^n}\right) \leq O\left(\sqrt{q^3/2^n}\right)$ in the quantum setting, instead of the classical bound $O(q^2/2^n)$.

The intuition behind the notion of equivalent databases might seem simple or even trivial, though, the important point is that we can provide a rigorous proof that the intuition actually works in the quantum setting through RstOE. (Recall that it was unclear how to record quantum queries before the development of the compressed oracle technique.)

As we mentioned before, it is quite important to show the tight security bound in symmetric cryptology because even the improvement from $O(2^{n/5})$ (or $O(2^{n/8})$) to $O(2^{n/3})$ has significant importance in the real world. Bad events like hit that an adversary succeeds to guess an output of a random function often appear in classical provable security for symmetric-key cryptosystems. To deal with such bad events when showing quantum tight security bounds, proof techniques like our equivalent databases seem indispensable. We believe that our technique broadens the applicability of quantum provable security in symmetric-key cryptology.

6.3 Some Technical Lemmas

Here we introduce two technical lemmas for later use.

Lemma 13 (Lemma 2.2 of [SXY18])**.** *Let $h : \{0,1\}^{m+n} \to \{0,1\}^n$ be a quantum random oracle. For a random key $K \in \{0,1\}^k$ $(k < m+n)$, define $F_K^h : \{0,1\}^{m+n-k} \to \{0,1\}^n$ by $F_K^h(x) = h(x||K)$. Then, for each quantum adversary $\mathcal{A}$ that makes at most q_h quantum queries to h, $\mathbf{Adv}^{\mathrm{qPRF}}_{F_K^h}(\mathcal{A}) \leq O\left(q_h/2^{k/2}\right)$ holds.*

Lemma 14. *Let $h : \{0,1\}^{m+n} \to \{0,1\}^n$ be a quantum random oracle, and $k \leq m$. Let $\Delta \in \{0,1\}^m$ and $IV \in \{0,1\}^n$ be public constants such that $\Delta \neq 0^m$. Define $\rho^h : \{0,1\}^k \to \{0,1\}^{2n}$ by $\rho^h(K) = h(K||0^{m-k}||IV)||h((K||0^{m-k} \oplus \Delta)||IV)$. Then, for any quantum adversary $\mathcal{A}$ that makes at most q_h quantum queries to h, $\mathbf{Adv}^{\mathrm{qPRG}}_{\rho^h}(\mathcal{A}) \leq O\left(q_h/2^{k/2}\right)$ holds.*

Lemma 14 can easily be shown by slightly modifying the proof of Lemma 13 (Lemma 2.2 in [SXY18]), but we give a proof below for completeness.

[5] This holds due to the following reasoning. For simplicity, assume that nothing has been *directly* queried to h before, and D_f has $(i-1)$ entries $(u_1, \alpha_1), \ldots, (u_{i-1}, \alpha_{i-1})$ (other cases can be shown similarly). Then $|\mathsf{Equiv}(D_f, D_h)|$ is equal to the number of choices of the tuple $(\alpha_1, \ldots, \alpha_{i-1})$ such that $\alpha_j \neq \alpha_k$ for $j \neq k$. Hence $|\mathsf{Equiv}(D_f, D_h)| = \binom{2^n}{i-1}$. In addition, the number of $(D'_f, D'_h) \in \mathsf{Equiv}(D_f, D_h)$ such that $\alpha_j = \tilde{\zeta}$ for some j is $(i-1)\cdot\binom{2^n}{i-2}$. Thus the ratio is $(i-1)\cdot\binom{2^n}{i-2}/\binom{2^n}{i-1} = \frac{(i-1)}{(2^n-i+2)} \leq O(i/2^n)$.

6.3.1 Proof of Lemma 14

To show Lemma 14, we use the following lemma.

Lemma 15 (Lemma C.1 in [SY17])**.** *For a bit string $K \in \{0,1\}^k$ that is uniformly chosen at random, let $\tilde{g}_K : \{0,1\}^k \to \{0,1\}$ be the function such that $\tilde{g}_K(x) = 1$ if and only if $x = K$. In addition, let $\tilde{g}_\perp : \{0,1\}^k \to \{0,1\}$ be the function such that $\tilde{g}_\perp(x) = 0$ for all x. Then, for a quantum adversary $\mathcal{A}$ that makes at most q quantum queries to $\tilde{g}_K$ or $\tilde{g}_\perp$,*

$$\mathbf{Adv}^{\mathrm{dist}}_{g_K, g_\perp}(\mathcal{A}) \leq O\left(\frac{q}{2^{k/2}}\right) \tag{6.10}$$

holds.

First, we show that the lemma below follows from Lemma 15.

Lemma 16. *Let $\Delta \in \{0,1\}^m$ be a public constant such that $\Delta \neq 0^m$ and suppose that $k \leq m$. Let $g_K^{\mathsf{rel}(\Delta)} : \{0,1\}^m \to \{0,1\}$ be the function such that $g_K^{\mathsf{rel}(\Delta)}(x) = 1$ if and only if $x = K||0^{m-k}$ or $x = (K||0^{m-k}) \oplus \Delta$ ($K \in \{0,1\}^k$ is chosen uniformly at random). In addition, let $g_\perp : \{0,1\}^m \to \{0,1\}$ be the function such that $g_\perp(x) = 0$ for all x. Then, for any quantum adversary $\mathcal{A}$ that makes at most q quantum queries to $g_K^{\mathsf{rel}(\Delta)}$ or $g_\perp$,*

$$\mathbf{Adv}^{\mathrm{dist}}_{g_K^{\mathsf{rel}(\Delta)}, g_\perp}(\mathcal{A}) \leq O\left(\frac{q}{2^{k/2}}\right) \tag{6.11}$$

holds.

Proof. We construct an adversary $\mathcal{B}$ to distinguish $\tilde{g}_K$ and $\tilde{g}_\perp$ that makes at most $O(q)$ queries from the adversary $\mathcal{A}$ to distinguish $g_K^{\mathsf{rel}(\Delta)}$ and $g_\perp$ as follows: $\mathcal{B}$ is given access to the quantum oracle of a Boolean function G ($G = \tilde{g}_K$ or $\tilde{g}_\perp$). First, $\mathcal{B}$ runs $\mathcal{A}$. When $\mathcal{A}$ queries x to its oracle, $\mathcal{B}$ performs the following procedure and responds to $\mathcal{A}$:

1. If $k < m$, and both of the least significant $(m-k)$ bits of x (which we denote by $[x]_{\mathrm{lsb}(m-k)}$) and $x \oplus \Delta$ (which we denote by $[x \oplus \Delta]_{\mathrm{lsb}(m-k)}$) are not equal to 0^{m-k}, respond to $\mathcal{A}$ with 0.
2. If $k = m$, or $[x]_{\mathrm{lsb}(m-k)} = 0^{m-k}$, or $[x \oplus \Delta]_{\mathrm{lsb}(m-k)} = 0^{m-k}$, then:
   (a) Set $b_1 \leftarrow 0$ and $b_2 \leftarrow 0$.
   (b) If $k = m$ or $[x]_{\mathrm{lsb}(m-k)} = 0^{m-k}$, query the most significant k bits of x (which we denote by $[x]_{\mathrm{msb}(k)}$) to G, and set $b_1 \leftarrow G([x]_{\mathrm{msb}(k)})$.
   (c) If $k = m$ or $[x \oplus \Delta]_{\mathrm{lsb}(m-k)} = 0^{m-k}$, query the first k bits of $x \oplus \Delta$ (which we denote by $[x \oplus \Delta]_{\mathrm{msb}(k)}$) to G, and set $b_2 \leftarrow G([x \oplus \Delta]_{\mathrm{msb}(k)})$.
   (d) Respond to $\mathcal{A}$ with $b_1 \vee b_2$.

Finally $\mathcal{B}$ returns $\mathcal{A}$'s last output as its own output.

Then, $\mathcal{B}$ perfectly simulates $g_K^{\mathsf{rel}(\Delta)}$ or $g_\perp$ depending on whether $G = \tilde{g}_K$ or $\tilde{g}_\perp$, and $\mathcal{B}$ makes at most $O(q)$ quantum queries. Thus

$$\mathbf{Adv}^{\mathrm{dist}}_{g_K^{\mathsf{rel}(\Delta)}, g_\perp}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{dist}}_{\tilde{g}_K, \tilde{g}_\perp}(\mathcal{B}) \leq O\left(\frac{q}{2^{k/2}}\right) \tag{6.12}$$

follows from Lemma 15. □

Next we show the following lemma.

Lemma 17. *Let $h : \{0,1\}^{n+m} \to \{0,1\}^n$ be a quantum random oracle, and let $k \leq m$. For a randomly chosen key $K \in \{0,1\}^k$ and a public constant $\Delta \in \{0,1\}^m$ such that $\Delta \neq 0^m$, define a keyed function $F_K^h : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$ by, for each $b \in \{0,1\}$ and $x \in \{0,1\}^n$,*

$$F_K^h(b,x) := \begin{cases} h(K||0^{m-k}||x) & \text{if } b = 0, \\ h((K||0^{m-k}) \oplus \Delta)||x) & \text{if } b = 1. \end{cases} \tag{6.13}$$

Then, for any quantum algorithm $\mathcal{A}$ that makes at most q_h quantum queries to h,

$$\mathbf{Adv}^{\mathrm{qPRF}}_{F_K^h}(\mathcal{A}) \leq O\left(\frac{q_h}{2^{k/2}}\right) \tag{6.14}$$

holds.

Proof. Let $H_0 : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$ be a random function that is independent of h. In addition, let $H_1^{h,H_0} : \{0,1\}^{m+n} \to \{0,1\}^n$ be a function defined by, for each $\alpha \in \{0,1\}^m$ and $x \in \{0,1\}^n$,

$$H_1^{h,H_0}(\alpha||x) := \begin{cases} h(\alpha||x) & \text{if } \alpha \neq K||0^{m-k} \text{ and } \alpha \neq K||0^{m-k} \oplus \Delta, \\ H_0(0,x) & \text{if } \alpha = K||0^{m-k}, \\ H_0(1,x) & \text{if } \alpha = K||0^{m-k} \oplus \Delta. \end{cases} \tag{6.15}$$

Then the distribution of the functions (F_K^h, h) and the distribution of the functions (H_0, H_1^{h,H_0}) are the same. Thus

$$\begin{aligned} \mathbf{Adv}^{\mathrm{qPRF}}_{F_K^h}(\mathcal{A}) &= \mathbf{Adv}^{\mathrm{dist}}_{(F_K^h,h),(H_0,h)}(\mathcal{A}) \\ &\leq \mathbf{Adv}^{\mathrm{dist}}_{(F_K^h,h),(H_0,H_1^{h,H_0})}(\mathcal{A}) + \mathbf{Adv}^{\mathrm{dist}}_{(H_0,H_1^{h,H_0}),(H_0,h)}(\mathcal{A}) \\ &= \mathbf{Adv}^{\mathrm{dist}}_{(H_0,H_1^{h,H_0}),(H_0,h)}(\mathcal{A}) \end{aligned} \tag{6.16}$$

holds.

We construct an adversary $\mathcal{B}$ to distinguish $g_K^{\mathsf{rel}(\Delta)}$ and $g_\perp$ from the adversary $\mathcal{A}$ to distinguish (H_0, H_1^{h,H_0}) and (H_0, h) as follows: $\mathcal{B}$ is given access to the quantum random oracle of a Boolean function G ($G = g_K^{\mathsf{rel}(\Delta)}$ or $g_\perp$). $\mathcal{B}$ first samples random functions $h' : \{0,1\}^{m+n} \to \{0,1\}^n$ and $H_0' : \{0,1\} \times \{0,1\}^n \to \{0,1\}^n$, and runs $\mathcal{A}$. When $\mathcal{A}$ makes a query to the first oracle (which is supposed to be H_0), $\mathcal{B}$ responds by using H_0'. When $\mathcal{A}$ makes a query $\alpha||x$ ($\alpha \in \{0,1\}^m$ and $x \in \{0,1\}^n$) to the second oracle (which is supposed to be H_1^{h,H_0} or h), $\mathcal{B}$ runs the following procedure and respond to $\mathcal{A}$:

1. Query α to G.
2. If $G(\alpha) = 0$, $\mathcal{B}$ responds to $\mathcal{A}$ with $h'(\alpha||x)$.
3. If $G(\alpha) = 1$ and $[\Delta]_{\mathrm{lsb}(m-k)} \neq 0^{m-k}$, then
   (a) If $[\alpha]_{\mathrm{lsb}(m-k)} = 0^{m-k}$, $\mathcal{B}$ responds to $\mathcal{A}$ with $H_0'(0,x)$.
   (b) If $[\alpha]_{\mathrm{lsb}(m-k)} \neq 0^{m-k}$, $\mathcal{B}$ responds to $\mathcal{A}$ with $H_0'(1,x)$.
4. If $G(\alpha) = 1$ and $[\Delta]_{\mathrm{lsb}(m-k)} = 0^{m-k}$, then
   (a) If $\alpha < \alpha \oplus \Delta$ (here we regard α and $\alpha \oplus \Delta$ as integers in $\{0, \ldots, 2^k - 1\}$), $\mathcal{B}$ responds to $\mathcal{A}$ with $H_0'(0,x)$.
   (b) If $\alpha > \alpha \oplus \Delta$, $\mathcal{B}$ responds to $\mathcal{A}$ with $H_0'(1,x)$.

Finally $\mathcal{B}$ returns $\mathcal{A}$'s last output as its own output.

Then, $\mathcal{B}$ perfectly simulates (H_0, H_1^{h,H_0}) and (H_0, h) depending on whether G is $g_K^{\mathsf{rel}(\Delta)}$ or $g_\perp$, and $\mathcal{B}$ makes at most $O(q_h)$ quantum queries. Thus

$$\mathbf{Adv}^{\mathrm{dist}}_{(H_0,H_1^{h,H_0}),(H_0,h)}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{dist}}_{g_K^{\mathsf{rel}(\Delta)},g_\perp}(\mathcal{B}) \leq O\left(\frac{q_h}{2^{k/2}}\right) \tag{6.17}$$

follows from Lemma 16, which completes the proof. □

Now we show Lemma 14.

Proof of Lemma 14. Lemma 14 immediately follows from Lemma 17, since adversaries to distinguish $\rho^h(K)$ and a random $2n$-bit string can be regarded as special adversaries to distinguish F_K^h and a random function that query only $(0, IV)$ and $(1, IV)$ to F_K^h (or the random function). □

6.4 Main Technical Proposition

The goal of this section is to show the following proposition, which is the technically hardest part to show quantum security of HMAC and NMAC. Note that the proposition is a formal restatement of Proposition 19 in Section 6.2.

Proposition 20. *Let $h : \{0,1\}^{m+n} \to \{0,1\}^n$ be a quantum random oracle. Let $f : \{0,1\}^{n+m'} \to \{0,1\}^n$ be a random function, and $F_1^h : \{0,1\}^{n+m'} \times \{0,1\}^m \to \{0,1\}^n$ be the function defined by $F_1^h(u,v) := h(v, f(u))$. Let $\mathcal{A}$ be an algorithm that runs relative to the quantum oracle of F_1^h and the quantum random oracle h, or the quantum oracle of a random function* RF *and the quantum random oracle h. Suppose that $\mathcal{A}$ makes at most q_h quantum queries to h and Q quantum queries to F_1^h or* RF*. Let $q := \max\{Q, q_h\}$, and suppose that q is in $o(2^{n/3})$. Then*

$$\mathbf{Adv}^{\mathrm{qPRF}}_{F_1^h}(\mathcal{A}) \leq O\left(\sqrt{q^3/2^n}\right) \tag{6.18}$$

holds.

Recall that F_2 is the function defined by $F_2(u,v) := g(u,v,f(u))$, where $g : \{0,1\}^{n+m'} \times \{0,1\}^m \times \{0,1\}^n \to \{0,1\}^n$ is another random function (see Fig. 6.1). Then, since g is a random function, $\mathbf{Adv}^{\mathrm{qPRF}}_{F_1^h}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(F_2,h)}(\mathcal{A})$ holds. To simplify proofs, instead of directly showing (6.18), we show that $\mathbf{Adv}^{\mathrm{dist}}_{(F_1^h,h),(F_2,h)}(\mathcal{A}) \leq O\left(\sqrt{q^3/2^n}\right)$ holds. In addition, we give a proof for the case $m' = 0$. The claims for $m' > 0$ can be shown in the same way. We assume that $\mathcal{A}$ makes queries to F_1^h and h (or, F_2 and h) in a sequential order and model the adversary and oracles as in Section 2.4.2. In particular, by convention we assume that $\mathcal{A}$'s $(2i-1)$-th query is made to F_1^h (or F_2) and $2i$-th query is made to h for $1 \leq i \leq q$. (For instance, $\mathcal{A}$ first queries to F_1^h (or F_2) and second queries to h.) We call queries to F_1^h and F_2 *online queries* and queries to h *offline queries* since, in practical settings, computations of h are done offline on adversaries' (quantum) computers.

We assume that the unitary operators to process queries to F_1^h and F_2 are implemented as follows:
Quantum oracle of F_1^h.

1. Take $|u,v\rangle|y\rangle$ as an input, where $u, y \in \{0,1\}^n$ and $v \in \{0,1\}^m$.
2. Query u to f and obtain
$$|u,v\rangle|y\rangle \otimes |f(u)\rangle. \tag{6.19}$$
3. Query $(v, f(u))$ to h and add the answer into the y register to obtain
$$|u,v\rangle|y \oplus F_1^h(u,v)\rangle \otimes |f(u)\rangle. \tag{6.20}$$
4. Uncompute Step 2 to obtain $|u,v\rangle|y \oplus F_1^h(u,v)\rangle$.

We assume that the quantum oracle of F_2 is implemented in the same way as F_1^h, except that the query $(v, f(u))$ to h in Step 3 is replaced with the query $(u, v, f(u))$ to g. See also Fig. 6.3.

We show the hardness of distinguishing F_1^h and F_2 by using the recording standard oracle with errors (RstOE): We assume that the quantum oracles of f, g, and h are implemented by using RstOE (quantum queries are processed with RstOE). Let RstOE_f, RstOE_g, and RstOE_h be the recording standard oracle with errors for f, g, and h, respectively. We use the symbols D_f, D_g, and D_h to denote databases for f, g, and h, respectively. Then the unitary operator $O_{F_1^h}$ (resp., O_{F_2}) to process queries to F_1^h (resp., F_2) can be decomposed as $O_{F_1^h} = \mathsf{RstOE}_f^* \cdot \mathsf{RstOE}_h \cdot \mathsf{RstOE}_f$ (resp., $O_{F_2} = \mathsf{RstOE}_f^* \cdot \mathsf{RstOE}_g \cdot \mathsf{RstOE}_f$). See also Fig. 6.3 for the intuition about which registers the different RstOEs act.

6.4.1 Good and Bad Databases

Here we introduce the notion of good and bad databases for F_1^h and F_2. When we use the symbols u, ζ, v, w, we assume that $u, \zeta, w \in \{0,1\}^n$ and $v \in \{0,1\}^m$.

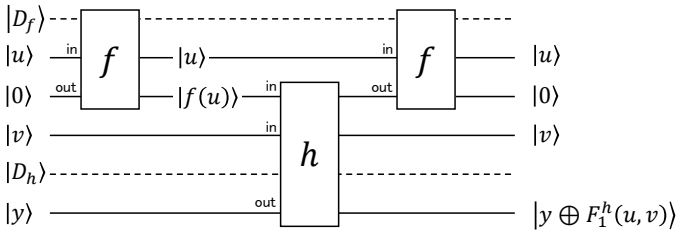
We say that a (pair of) valid databases (D_f, D_h) for F_1^h is *good* if and only if it satisfies the following property.

1. For each $(u,\zeta) \in D_f$, there exist $v \in \{0,1\}^m$ and $w \in \{0,1\}^n$ such that $((v,\zeta),w) \in D_h$.
2. For (u,ζ) and (u',ζ') in D_f such that $u \neq u'$, $\zeta \neq \zeta'$ holds (there is no collision for f).

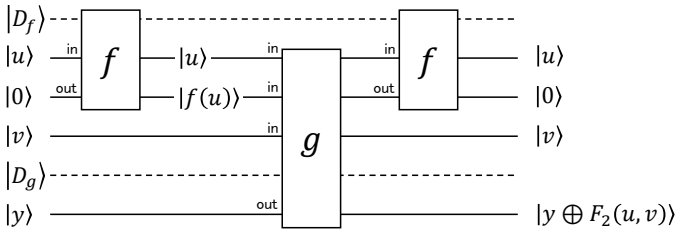
We say that (D_f, D_h) is *bad* if it is not good.

Similarly, we say that a (tuple of) valid databases (D_f, D_g, D_h) for F_2 is *good* if and only if it satisfies the following properties.

1. For each $(u,\zeta) \in D_f$, there exist $v \in \{0,1\}^m$ and $w \in \{0,1\}^n$ such that $((u,v,\zeta),w) \in D_g$.



(a) Implementation of F_1^h.



(b) Implementation of F_2.

Figure 6.3: Implementations of F_1^h and F_2. "in" and "out" denote the registers to send queries and receive answers, respectively. The dotted lines (and $|D_f\rangle, |D_h\rangle, |D_g\rangle$) appear only when f, h, g are implemented with RstOE, which correspond to the database registers.

2. For each $((u, v, \zeta), w) \in D_g$, $(u, \zeta) \in D_f$.
3. For (u, ζ) and (u', ζ') in D_f such that $u \neq u'$, $\zeta \neq \zeta'$ holds (i.e., there is no collision for f).
4. For each $((v, \zeta), w) \in D_h$ and $(u', \zeta') \in D_f$, $\zeta \neq \zeta'$ holds (i.e., the most significant n bits of inputs to h and the outputs of f do not collide).

We say that (D_f, D_g, D_h) is *bad* if it is not good.

Intuition Behind Good Databases. Intuitively, a database (D_f, D_h) for F_1^h is defined to be good if and only if D_f does not contain collisions (the second condition on F_1^h). The first condition on F_1^h is included so that a weird situation such as "u has been queried to f, but $(v, f(u))$ has not been queried to h for any v" will not happen for good databases. Similarly, a database (D_f, D_g, D_h) for F_2 is defined to be good if and only if D_f does not contain collisions (the third condition condition on F_2) and the least significant n bits of inputs to h do not collide with outputs of f (the fourth condition on F_2). The first and second conditions on F_2 is included so that weird situations such as "u has been queried to f, but $(u, v, f(u))$ has not been queried to g for any v" or "(u, v, ζ) has been queried to g, but u has not been queried to f" will not happen for good databases.

6.4.2 One-to-One Correspondence for Good Databases

For a good database (D_f, D_g, D_h) for F_2, let $D_g \star D_h$ be the valid database for h such that $((v, \zeta), w) \in D_g \star D_h$ if and only if $((v, \zeta), w) \in D_h$ or $((u, v, \zeta), w) \in D_g$ for some u. Then $(D_f, D_g \star D_h)$ becomes a good database for F_1^h. Let us denote $(D_f, D_g \star D_h)$ by $[(D_f, D_g, D_h)]_1$. Then, it can easily be shown that the map $[\cdot]_1 : (D_f, D_g, D_h) \mapsto [(D_f, D_g, D_h)]_1 = (D_f, D_g \star D_h)$ is a bijection between the set of good databases for F_2 and that for F_1^h. Let $[\cdot]_2$ denote the inverse map of $[\cdot]_1$.

The bijections extend to (partially defined) isometries between the state spaces. Let $\mathcal{H}_{\mathcal{A}}$ be the state space of the adversary, and $\mathcal{H}_{D_f D_h}$ (resp., $\mathcal{H}_{D_f D_g D_h}$) be the state space of the databases for F_1^h (resp., F_2^h). In addition, let $V_{\mathsf{good}}^{(1)} \subset \mathcal{H}_{D_f D_h}$ (resp., $V_{\mathsf{good}}^{(2)} \subset \mathcal{H}_{D_f D_g D_h}$) be the subspace spanned by good databases. Then, the linear map from $\mathcal{H}_{\mathcal{A}} \otimes V_{\mathsf{good}}^{(1)}$ to $\mathcal{H}_{\mathcal{A}} \otimes V_{\mathsf{good}}^{(2)}$ that maps $|\eta\rangle \otimes |D_f, D_h\rangle$ to $|\eta\rangle \otimes |[D_f, D_h]_2\rangle$ for $|\eta\rangle \in \mathcal{H}_{\mathcal{A}}$ and a good database (D_f, D_h) becomes an isometry. We denote this isometry and its inverse also by $[\cdot]_2$ and $[\cdot]_1$, respectively.

6.4.3 Equivalent Good Databases

Next, we define the notion of *equivalent databases*. First, we define the notion for equivalent good databases for F_1^h. Let (D_f, D_h) be a good database for F_1^h, and let

$$S := \left\{ \zeta \in \{0,1\}^n \middle| \exists v, w \text{ s.t. } ((v,\zeta),w) \in D_h \text{ and } (u,\zeta) \notin D_f \text{ for all } u \right\}.$$

We say that another good database (D'_f, D'_h) is equivalent to (D_f, D_h) if and only if they are the same except for the output values of f, i.e., there exists a permutation π on $\{0,1\}^n$ such that

1. $\pi(\zeta) = \zeta$ for all $\zeta \in S$,
2. $(u,\zeta) \in D_f$ if and only if $(u, \pi(\zeta)) \in D'_f$, and
3. $((v,\zeta),w) \in D_h$ if and only if $((v,\pi(\zeta)),w) \in D'_h$ holds.

We define that a good database (D'_f, D'_g, D'_h) for F_2 is equivalent to another good database (D_f, D_g, D_h) in the same way, except that S is defined as $S := \{\zeta \in \{0,1\}^n | \exists v, w \text{ s.t. } ((v,\zeta),w) \in D_h\}$ and the following condition is additionally imposed.

3^+. $((u,v,\zeta),w) \in D_g$ if and only if $((u,v,\pi(\zeta)),w) \in D'_g$ hold.

Remark 17. *As explained in Section 6.2, intuitively, two good databases are defined to be equivalent if and only if any adversary cannot distinguish them.*

Remark 18. *By definition of equivalent databases, if a good database (D_f, D_g, D_h) for F_2 is equivalent to another good database (D'_f, D'_g, D'_h), then $D'_h = D_h$ holds.*

6.4.4 Notations for State Vectors

Let $|\phi_{2i-1}\rangle$ be the whole quantum state just before $\mathcal{A}$'s i-th query to F_1^h when $\mathcal{A}$ runs relative to F_1^h and h. In addition, let $|\phi_{2i}\rangle$ be the whole quantum state just before $\mathcal{A}$'s i-th query to h when $\mathcal{A}$ runs relative to F_1^h and h. Define $|\psi_{2i-1}\rangle$ and $|\psi_{2i}\rangle$ similarly when $\mathcal{A}$ runs relative to F_2 and h. For ease of notation, let $|\phi_{2q+1}\rangle$ and $|\psi_{2q+1}\rangle$ be the quantum states just before the final measurement when $\mathcal{A}$ runs relative to (F_1^h, h) and (F_2, h), respectively.

6.4.5 The Technically Hardest Part

The following proposition is the technically hardest part to show Proposition 20.

Proposition 21. *For each $j = 1, \ldots, 2q+1$, there exist $|\phi_j^{\mathsf{good}}\rangle$, $|\phi_j^{\mathsf{bad}}\rangle$, $|\psi_j^{\mathsf{good}}\rangle$, and $|\psi_j^{\mathsf{bad}}\rangle$ that satisfy the following properties:*

1. *$|\phi_j\rangle = |\phi_j^{\mathsf{good}}\rangle + |\phi_j^{\mathsf{bad}}\rangle$ and $|\psi_j\rangle = |\psi_j^{\mathsf{good}}\rangle + |\psi_j^{\mathsf{bad}}\rangle$.*
2. *$|\phi_j^{\mathsf{good}}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V_{\mathsf{good}}^{(1)}$ and $|\psi_j^{\mathsf{good}}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V_{\mathsf{good}}^{(2)}$.*
3. *$|\phi_j^{\mathsf{good}}\rangle = \left[|\psi_j^{\mathsf{good}}\rangle\right]_1$.*
4. *There exists a complex number $a^{(j)}_{uvyzD_fD_gD_h}$ such that*

$$|\psi_j^{\mathsf{good}}\rangle = \sum_{\substack{u,v,y,z,D_f,D_g,D_h; \\ (D_f,D_g,D_h):good}} a^{(j)}_{uvyzD_fD_gD_h} |u,v\rangle |y\rangle |z\rangle \otimes |D_f, D_g, D_h\rangle \tag{6.21}$$

and $a^{(j)}_{uvyzD_fD_gD_h} = a^{(j)}_{uvyzD'_fD'_gD'_h}$ if (D_f, D_g, D_h) and (D'_f, D'_g, D'_h) are equivalent, where (u,v), y, and z correspond to $\mathcal{A}$'s register to send queries, register to receive answers from oracles, and register for offline computations, respectively.[6]

[6]To be precise we have to use the symbol (v,ζ) instead of (u,v) when $j = 2i$ because we always use the symbol $v||\zeta$ to denote an input to h. However, here we use (u,v) to simplify notations. In the proof we use the symbol $a^{(2i)}_{v\zeta yzD_fD_gD_h}$ instead of $a^{(2i)}_{uvyzD_fD_gD_h}$.

5. *For a good database* (D_f, D_g, D_h) *with non-zero coefficient in* $|\psi_{2i-1}^{\mathsf{good}}\rangle$ *(resp., in* $|\psi_{2i}^{\mathsf{good}}\rangle$*),* $|D_g| \leq i-1$*,* $|D_f| \leq 2(i-1)$*, and* $|D_h| \leq i-1$ *hold (resp.,* $|D_g| \leq i$*,* $|D_f| \leq 2i$*, and* $|D_h| \leq i-1$ *hold).*

6. $\| |\phi_j^{\mathsf{bad}}\rangle \| \leq \| |\phi_{j-1}^{\mathsf{bad}}\rangle \| + O\left(\sqrt{j/2^n}\right)$ *and* $\| |\psi_j^{\mathsf{bad}}\rangle \| \leq \| |\psi_{j-1}^{\mathsf{bad}}\rangle \| + O\left(\sqrt{j/2^n}\right)$ *hold (we regard that* $\| |\phi_0^{\mathsf{bad}}\rangle \| = \| |\psi_0^{\mathsf{bad}}\rangle \| = 0$*).*

Intuitive Interpretation of Proposition 21. The first and second properties show that $|\phi_j\rangle$ and $|\psi_j\rangle$ are divided into good and bad components. The third property shows that the good component of $|\phi_j\rangle$ matches to that of $|\psi_j\rangle$ through the isometry $[\cdot]_1$, which intuitively means that $\mathcal{A}$ cannot distinguish the two oracles as long as databases are good. The fourth property shows that the coefficients of equivalent databases are perfectly equal, which intuitively means that $\mathcal{A}$ cannot distinguish equivalent good databases. The fifth property shows the upper bound of the size of databases. The sixth property shows that the chance for good databases change to bad is very small at each query.

Overview of the Proof of Proposition 21. The proposition is shown by induction on j. The claim for $j = 1$ obviously holds by setting $|\phi_1^{\mathsf{bad}}\rangle = |\psi_1^{\mathsf{bad}}\rangle = 0$. Inductive steps are separated into two cases.

(Online queries): If the claim for $j = 2i-1$ (i.e., before the i-th query to F_1^h or F_2) holds, then the claim for $j = 2i$ (i.e., after the query) holds.

(Offline queries): If the claim for $j = 2i$ (i.e., before the i-th query to h) holds, then the claim for $j = 2i+1$ (i.e., after the query) holds.

Proof for online queries. Recall that $O_{F_1^h}$ (resp., O_{F_2}) are decomposed as $O_{F_1^h} = \mathsf{RstOE}_f^* \cdot \mathsf{RstOE}_h \cdot \mathsf{RstOE}_f$ (resp., $O_{F_2} = \mathsf{RstOE}_f^* \cdot \mathsf{RstOE}_g \cdot \mathsf{RstOE}_f$). We show that Properties 1–6 listed in Proposition 21 hold at each action of RstOE_f, RstOE_h (resp., RstOE_g), and RstOE_f^*. A state vector after an action of RstOE can be decomposed into three components.[7]

(i) The one that was (pre-)good before the action and still remains (pre-)good.

(ii) The one that was (pre-)good before the action but changed to bad.

(iii) The one that was already bad before the action.

Roughly speaking, we define (i) to be a new good vector, and the sum of (ii) and (iii) to be a new bad vector.[8] Then Properties 1 and 4 of Proposition 21 can easily be shown.

To show that Properties 3 and 4 still hold for the new good vector, we keep track of how the coefficients of basis vectors change by using Proposition 3. We also utilize symmetry of equivalent databases to show Property 4.

Property 6 is proven by showing the norm of the component (iii) is in $O(\sqrt{i/2^n})$. Intuitively, this corresponds to showing the probability that the event coll in Section 6.2 happens at the query is $O(i/2^n)$. We carefully prove it by using Proposition 3, taking into account that records in databases may be deleted or overwritten.

Proof for offline queries. The proof for offline queries are similar[9], except that showing $\|(\text{iii})\| \leq O(\sqrt{i/2^n})$ corresponds to showing $\Pr[\mathsf{hit}_i] \leq O(i/2^n)$ in Section 6.2. To formally prove the bound, we use the inductive hypothesis that Property 4 holds for $j = 2i$.

Before proving Proposition 21, we show that Proposition 20 follows from Proposition 21.

Proof of Proposition 20. Let tr_{D1} (resp., tr_{D2}) denote the partial trace operations over the quantum states of the databases for (F_1^h, h) (resp., (F_2, h)). Then

$$\begin{aligned}
\mathbf{Adv}^{\mathrm{dist}}_{F_1^h, F_2}(\mathcal{A}) &\leq \mathsf{td}\left(\mathsf{tr}_{D1}(|\phi_{2q+1}\rangle\langle\phi_{2q+1}|), \mathsf{tr}_{D2}(|\psi_{2q+1}\rangle\langle\psi_{2q+1}|)\right) \\
&\leq \mathsf{td}\left(\mathsf{tr}_{D1}(|\phi_{2q+1}^{\mathsf{good}}\rangle\langle\phi_{2q+1}^{\mathsf{good}}|), \mathsf{tr}_{D2}(|\psi_{2q+1}^{\mathsf{good}}\rangle\langle\psi_{2q+1}^{\mathsf{good}}|)\right) && (6.22) \\
&\quad + \left\||\phi_{2q+1}^{\mathsf{bad}}\rangle\right\| + \left\||\psi_{2q+1}^{\mathsf{bad}}\rangle\right\| && (6.23)
\end{aligned}$$

[7] Pre-good databases are defined in a complete proof of Proposition 21 presented in Section 6.4.6 in the supplementary materials.

[8] To be more precise, we sometimes include small "good" terms into the new bad vector so that the analysis will be easier.

[9] Actually the proof for offline queries are even simpler because the offline oracle is just a single random oracle h while the online oracles consist of two random functions.

holds. By Property 3 of Proposition 21, the term (6.22) is equal to zero. In addition,

$$(6.23) \leq \sum_{1 \leq j \leq 2q+1} O\left(\sqrt{j/2^n}\right) + \sum_{1 \leq j \leq 2q+1} O\left(\sqrt{j/2^n}\right) \leq O\left(\sqrt{q^3/2^n}\right)$$

follows from Property 6 of Proposition 21. Hence Proposition 20 follows. □

6.4.6 Proof of Proposition 21

As mentioned before, we show the proposition by induction on j. The claim for $j = 1$ obviously holds by setting $|\phi_1^{\mathsf{bad}}\rangle = |\psi_1^{\mathsf{bad}}\rangle = 0$. Inductive steps are separated into the proof for online queries (i.e., the proof for $j = 2i$ under the hypothesis on $j = 2i - 1$) and the one for offline queries (i.e., the proof for $j = 2i + 1$ under the hypothesis on $j = 2i$).

First we prove the former by decomposing $O_{F_1^h}$ (resp., O_{F_2}) as $O_{F_1^h} = \mathsf{RstOE}_f^* \cdot \mathsf{RstOE}_h \cdot \mathsf{RstOE}_f$ (resp., $O_{F_2} = \mathsf{RstOE}_f^* \cdot \mathsf{RstOE}_g \cdot \mathsf{RstOE}_f$), and showing Properties 1–6 in the proposition hold at each action of RstOE_f, RstOE_h (resp., RstOE_g), and RstOE_f^*. (See also Fig. 6.3 about the decompositions.)

Before providing the proof, we define pre-good and pre-bad databases in addition to good and bad databases, and see that the one-to-one correspondence between good databases and the notions on equivalent databases are naturally extended to pre-good databases.

6.4.6.1 Pre-Good and Pre-Bad Databases

We say that a (pair of) valid database (D_f, D_h) for F_1^h is *pre-good* if and only if it satisfies the following properties:

1. (D_f, D_h) is good, or
2. There exists an element $(u, \zeta) \in D_f$ such that $(D_f \setminus (u, \zeta), D_h)$ is good and $((\zeta, v), w) \notin D_h$ for all v and w, and $(u', \zeta) \notin D_f$ for all $u' \neq u$.

We say that (D_f, D_h) is *pre-bad* if it is not pre-good.

Similarly, we say that a (tuple of) valid database (D_f, D_g, D_h) for F_2 is *pre-good* if and only if it satisfies the following properties:

1. (D_f, D_g, D_h) is good, or
2. There exists an element $(u, \zeta) \in D_f$ such that $(D_f \setminus (u, \zeta), D_g, D_h)$ is good and $((v, \zeta), w) \notin D_h \wedge ((u, v, \zeta), w) \notin D_g$ holds for all v and w, and $(u', \zeta) \notin D_f$ for all $u' \neq u$.

We say that (D_f, D_g, D_h) is *pre-bad* if it is not pre-good.

Intuition Behind Pre-Good Databases. Intuitively, a database is pre-good if and only if one of the following conditions hold: (i) It is just good, or (ii) $\mathcal{A}$ queried some value (u, v) to F_1^h (resp., F_2), the query u to f has already been processed inside F_1^h (resp., F_2) and a new output value $f(u)$ is sampled but the query $(v, f(u))$ to h (resp., $(u, v, f(u))$ to g) has not been processed yet, and the database is likely to become good.

6.4.6.2 One-to-one Correspondence for Pre-Good Databases

Here we re-define the one-to-one correspondence and the isometries $[\cdot]_1$ and $[\cdot]_2$ so that they are defined not only on good databases but also on pre-good databases.

For a pre-good database (D_f, D_g, D_h) for F_2, let $D_g \star D_h$ be the valid database for h such that $((v, \zeta), w) \in D_g \star D_h$ if and only if $((v, \zeta), w) \in D_h$ or $((u, v, \zeta), w) \in D_g$ for some u. Then $(D_f, D_g \star D_h)$ becomes a pre-good database for F_1^h. Let us denote $(D_f, D_g \star D_h)$ by $[(D_f, D_g, D_h)]_1$. Then, it can easily be shown that the map $[\cdot]_1 : (D_f, D_g, D_h) \mapsto [(D_f, D_g, D_h)]_1 = (D_f, D_g \star D_h)$ is a bijection between the set of pre-good databases for F_2 and the set of pre-good databases for F_1^h. Let $[\cdot]_2$ denote the inverse map of $[\cdot]_1$.

The bijections extend to (partially defined) isometries between the state spaces. Again, let $\mathcal{H}_{\mathcal{A}}$ denote the state space of the adversary, and $\mathcal{H}_{D_f D_h}$ (resp., $\mathcal{H}_{D_f D_g D_h}$) denote the state space of the databases for F_1^h (resp., F_2^h). In addition, let $V^{(1)}_{\mathsf{pre\text{-}good}} \subset \mathcal{H}_{D_f D_h}$ (resp., $V^{(2)}_{\mathsf{pre\text{-}good}} \subset \mathcal{H}_{D_f D_g D_h}$) be the subspace spanned by pre-good databases. Let $\mathcal{H}_{\mathrm{aux}}$ be the state space that corresponds to the auxiliary qubits used by the oracles (see (6.19) and (6.20)). Then, the linear map from $\mathcal{H}_{\mathcal{A}} \otimes V^{(1)}_{\mathsf{pre\text{-}good}} \otimes \mathcal{H}_{\mathrm{aux}}$ to $\mathcal{H}_{\mathcal{A}} \otimes V^{(2)}_{\mathsf{pre\text{-}good}} \otimes \mathcal{H}_{\mathrm{aux}}$ that maps $|\eta\rangle \otimes |D_f, D_h\rangle \otimes |\xi\rangle$ to $|\eta\rangle \otimes |[D_f, D_h]_2\rangle \otimes |\xi\rangle$

for $|\eta\rangle \in \mathcal{H}_{\mathcal{A}}$, $|\xi\rangle \in \mathcal{H}_{\mathrm{aux}}$, and a pre-good database (D_f, D_h) becomes an isometry. We denote this isometry and its inverse also by $[\cdot]_2$ and $[\cdot]_1$, respectively.

The above mappings $[\cdot]_1$ and $[\cdot]_2$ are generalizations of those on good databases define in Section 6.4. Note that $[(D_f, D_g, D_h)]_1$ is good if and only if (D_f, D_g, D_h) is good.

6.4.6.3 Equivalent Pre-Good Databases

Let (D_f, D_h) be a good database for F_1^h. Recall that another good database (D'_f, D'_h) is equivalent to (D_f, D_h) if and only if they are the same except the output values of f, i.e., there exists a permutation π on $\{0,1\}^n$ such that

1. $\pi(\zeta) = \zeta$ for all $\zeta \in S$,
2. $(u, \zeta) \in D_f$ if and only if $(u, \pi(\zeta)) \in D'_f$, and
3. $((v, \zeta), w) \in D_h$ if and only if $((v, \pi(\zeta)), w) \in D'_h$ hold,

where

$$S := \left\{ \zeta \in \{0,1\}^n \middle| \exists v, w \text{ s.t. } ((v,\zeta),w) \in D_h \text{ and } (u,\zeta) \notin D_f \text{ for all } u \right\}.$$

Next, we extend the notion for pre-good databases for F_1^h. By definition, arbitrary pre-good database has the form $(D_f \cup (u, \zeta), D_h)$ such that (D_f, D_h) is good. Let $(D'_f \cup (u', \zeta'), D'_h)$ be another pre-good database such that (D'_f, D'_h) is good. We say that $(D_f \cup (u, \zeta), D_h)$ is equivalent to $(D'_f \cup (u', \zeta'), D'_h)$ if and only if

4. (D_f, D_h) is equivalent to (D'_f, D'_h) in the above sense, and
5. $u = u' \wedge \zeta' = \pi(\zeta)$, where π is the permutation defined above for (D_f, D_h).

We define that a pre-good database (D'_f, D'_g, D'_h) for F_2 is equivalent to another pre-good database (D_f, D_g, D_h) in the same way, except that S is defined as $S := \{\zeta \in \{0,1\}^n | \exists v, w \text{ s.t. } ((v,\zeta),w) \in D_h\}$ and the following condition is additionally imposed.

3^+. $((u, v, \zeta), w) \in D_g$ if and only if $((u, v, \pi(\zeta)), w) \in D'_g$ hold.

6.4.6.4 Regular and Irregular States

Let $|\phi\rangle$ be a joint quantum state of $\mathcal{A}$ and the oracle ((F_1^h, h) or (F_2, h)) that is not in superposition[10]. We say that the state $|\phi\rangle$ is *irregular* when the database in $|\phi\rangle$ is invalid, or the auxiliary n qubits that are temporarily used in the oracle (the rightmost register $|f(u)\rangle$ in (6.19) and (6.20)) is not $|0^n\rangle$. We say that $|\phi\rangle$ is *regular* if it is not irregular.

6.4.6.5 Remarks on Other Notations

In what follows, to simplify notations on summations, we denote the sum over variables $x_1, \ldots, x_s$ that satisfies predicates $P_1(x_1, \ldots, x_s), \ldots, P_t(x_1, \ldots, x_s)$ by $\sum_{x_1,\ldots,x_s; P(x_1,\ldots,x_s),\ldots,P_t(x_1,\ldots,x_s)}$. That is, we separate the symbols of variables over which the summation is taken and the conditions that the variables satisfy by ";". For example, the summation over $\alpha, \beta, \gamma \in \{0,1\}^n$ that satisfy $\alpha \oplus \beta = 0^n$ and $\beta \oplus \gamma = 0^n$ is denoted by $\sum_{\alpha,\beta,\gamma;\alpha\oplus\beta=0^n,\beta\oplus\gamma=0^n}$.

Let Π_{valid} and Π_{invalid} denote the orthogonal projections onto the vector space spanned by valid and invalid databases, respectively. Let Π_{good} and Π_{bad} denote the orthogonal projections onto the vector space spanned by good and bad databases, respectively. Let $\Pi_{\mathsf{pre\text{-}good}}$ and $\Pi_{\mathsf{pre\text{-}bad}}$ denote the orthogonal projections onto the vector space spanned by pre-good and pre-bad databases, respectively. Let Π_{reg} and Π_{irreg} denote the orthogonal projections onto the vector space spanned by regular and irregular databases, respectively.

Remark 19. *Note that a good database can be pre-good and* bad *because the set of pre-good databases is wider than that of good databases, and we say that a database is bad if it is not good. In the proofs below, we sometimes use the fact that* $\Pi_{\mathsf{bad}} |D_f, D_g, D_h\rangle = |D_f, D_g, D_h\rangle$ *(resp.,* $\Pi_{\mathsf{bad}} |D_f, D_h\rangle = |D_f, D_h\rangle$*) holds for a database* (D_f, D_g, D_h) *(resp.,* (D_f, D_h)*) that is* pre-good and bad*, without any notice.*

Next we prove the following lemma, which shows how the quantum states $|\phi_{2i-1}^{\mathsf{good}}\rangle$ and $|\psi_{2i-1}^{\mathsf{good}}\rangle$ change when RstOE_f acts on them.

[10] That is, even if we measure $|\phi\rangle$ with computational basis, $|\phi\rangle$ does not change.

Lemma 18 (Action of RstOE_f)**.** *Suppose that there exist $|\phi_{2i-1}^{\mathsf{good}}\rangle$, $|\phi_{2i-1}^{\mathsf{bad}}\rangle$, $|\psi_{2i-1}^{\mathsf{good}}\rangle$, and $|\psi_{2i-1}^{\mathsf{bad}}\rangle$ that satisfy the properties of Proposition 21. Then there exist $|\phi_{2i-1}^{\mathsf{good},1}\rangle$, $|\phi_{2i-1}^{\mathsf{bad},1}\rangle$, $|\psi_{2i-1}^{\mathsf{good},1}\rangle$, and $|\psi_{2i-1}^{\mathsf{bad},1}\rangle$ that satisfy the following properties:*

1. $\mathsf{RstOE}_f\,|\psi_{2i-1}\rangle = |\psi_{2i-1}^{\mathsf{good},1}\rangle + |\psi_{2i-1}^{\mathsf{bad},1}\rangle$ *and* $\mathsf{RstOE}_f\,|\phi_{2i-1}\rangle = |\phi_{2i-1}^{\mathsf{good},1}\rangle + |\phi_{2i-1}^{\mathsf{bad},1}\rangle$.
2. $|\phi_{2i-1}^{\mathsf{good},1}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V_{\mathsf{pre\text{-}good}}^{(1)} \otimes \mathcal{H}_{\mathrm{aux}}$ *and* $|\psi_{2i-1}^{\mathsf{good},1}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V_{\mathsf{pre\text{-}good}}^{(2)} \otimes \mathcal{H}_{\mathrm{aux}}$.
3. $|\phi_{2i-1}^{\mathsf{good},1}\rangle = \left[|\psi_{2i-1}^{\mathsf{good},1}\rangle\right]_1$.
4. *There exists complex number $a_{uvyzD_fD_gD_h}^{(2i-1),1}$ such that the following properties (a) and (b) hold:*
   (a) *It holds that*
   $$|\psi_{2i-1}^{\mathsf{good},1}\rangle = \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h):\,\textit{pre-good}\\ D_f(u)\neq\perp}} a_{uvyzD_fD_gD_h}^{(2i-1),1}\,|u,v\rangle\,|y\rangle\,|z\rangle \otimes |D_f,D_g,D_h\rangle \otimes |D_f(u)\rangle,$$
   where (u,v), y, and z correspond to $\mathcal{A}$'s register to send queries, register to receive answers from oracles, and register for offline computations, respectively. (The rightmost register $|D_f(u)\rangle$ corresponds to the auxiliary qubits used in the oracle. See (6.19) *and* (6.20)*.)*
   (b) $a_{uvyzD_fD_gD_h}^{(2i-1),1} = a_{uvyzD_f'D_g'D_h'}^{(2i-1),1}$ *if (D_f,D_g,D_h) and (D_f',D_g',D_h') are equivalent.*
5. *For a pre-good database (D_f,D_g,D_h) with non-zero coefficient in $|\psi_{2i-1}^{\mathsf{good},1}\rangle$, $|D_g| \le i-1$, $|D_f| \le 2(i-1)+1$, and $|D_h| \le i-1$ hold.*
6. $\| \,|\phi_{2i-1}^{\mathsf{bad},1}\rangle\,\| \le \| \,|\phi_{2i-1}^{\mathsf{bad}}\rangle\,\| + O\left(\sqrt{i/2^n}\right)$ *and* $\| \,|\psi_{2i-1}^{\mathsf{bad},1}\rangle\,\| \le \| \,|\psi_{2i-1}^{\mathsf{bad}}\rangle\,\| + O\left(\sqrt{i/2^n}\right)$ *hold.*

Remark 20. *Intuitive interpretation of the lemma is almost the same as that for Proposition 21 (see the explanation below Proposition 21 for details) except that the fourth property is divided into 4-(a) and 4-(b) in the above lemma, where 4-(a) says that there is an auxiliary register $D_f(u)$ and the coefficient $a_{uvyzD_fD_gD_h}^{(2i-1),1}$ in $|\psi_{2i-1}^{\mathsf{good},1}\rangle$ is non-zero only if $D_f(u) \neq \perp$.*

Proof. First, note that property 3 and 4 of Proposition 21 imply that

$$|\phi_{2i-1}^{\mathsf{good}}\rangle = \left[|\psi_{2i-1}^{\mathsf{good}}\rangle\right]_1 = \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h):\mathsf{good}}} a_{uvyzD_fD_gD_h}^{(2i-1)}\,|u,v\rangle\,|y\rangle\,|z\rangle \otimes |D_f, D_g \star D_h\rangle \tag{6.24}$$

holds.

Let $\Pi_\perp$ and $\Pi_{\not\perp}$ be the orthogonal projections onto the spaces spanned by the vectors $|u,v\rangle\,|y\rangle\,|z\rangle \otimes |D_f,D_g,D_h\rangle$ (or, $|u,v\rangle\,|y\rangle\,|z\rangle \otimes |D_f,D_h\rangle$) such that $D_f(u) = \perp$ and $D_f(u) \neq \perp$, respectively.

Recall that $|\psi_{2i-1}^{\mathsf{good}}\rangle$ is represented as in (6.21). By applying the first property in Proposition 3 in a straightforward

manner, we have

$$\Pi_{\mathsf{valid}}\mathsf{RstOE}_f\Pi_{\not\perp}\left|\psi_{2i-1}^{\mathsf{good}}\right\rangle = \Pi_{\mathsf{valid}}\mathsf{RstOE}_f \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\(D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes \left|D_f\cup(u,\alpha),D_g,D_h\right\rangle$$

$$= \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\(D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes \left|D_f\cup(u,\alpha),D_g,D_h\right\rangle\otimes\left|\alpha\right\rangle \tag{6.25}$$

$$+ \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\(D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\D_f(u)=\perp}} \frac{1}{\sqrt{2^n}}a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes\left(\left|D_f\right\rangle-\sum_\gamma\frac{1}{\sqrt{2^n}}\left|D_f\cup(u,\gamma)\right\rangle\right)\left|D_g,D_h\right\rangle\otimes\left|\alpha\right\rangle \tag{6.26}$$

$$- \sum_{\substack{u,v,y,z,\alpha,\gamma,D_f,D_g,D_h;\\(D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\D_f(u)=\perp}} \frac{1}{2^n}a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes \left|D_f\cup(u,\gamma),D_g,D_h\right\rangle\otimes\left|\gamma\right\rangle \tag{6.27}$$

$$+ \frac{1}{2^n}\sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\(D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes\left(2\sum_\gamma\frac{1}{\sqrt{2^n}}\left|D_f\cup(u,\gamma)\right\rangle-\left|D_f\right\rangle\right)\left|D_g,D_h\right\rangle\otimes\left|\widehat{0^n}\right\rangle, \tag{6.28}$$

where the terms (6.25)-(6.28) correspond to (3.12)-(3.15), respectively. Similarly, by applying the second property in Proposition 3 we have

$$\Pi_{\mathsf{valid}}\mathsf{RstOE}_f\Pi_{\perp}\left|\psi_{2i-1}^{\mathsf{good}}\right\rangle = \Pi_{\mathsf{valid}}\mathsf{RstOE}_f \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\(D_f,D_g,D_h)\text{: good}\\D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_fD_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle\otimes\left|D_f,D_g,D_h\right\rangle$$

$$= \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\(D_f,D_g,D_h)\text{: good}\\D_f(u)=\perp}} \frac{1}{\sqrt{2^n}}a^{(2i-1)}_{uvyzD_fD_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes\left|D_f\cup(u,\alpha),D_g,D_h\right\rangle\otimes\left|\alpha\right\rangle \tag{6.29}$$

$$+ \frac{1}{\sqrt{2^n}}\sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\(D_f,D_g,D_h)\text{: good}\\D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes\left(\left|D_f\right\rangle-\sum_\gamma\frac{1}{\sqrt{2^n}}\left|D_f\cup(u,\gamma)\right\rangle\right)\left|D_g,D_h\right\rangle\otimes\left|\widehat{0^n}\right\rangle, \tag{6.30}$$

where the terms (6.29) and (6.30) correspond to (3.16) and (3.17), respectively. Since (6.24) holds, in the same way we have

$$\Pi_{\mathsf{valid}}\mathsf{RstOE}_f\Pi_{\not\perp}\left|\phi_{2i-1}^{\mathsf{good}}\right\rangle = \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\(D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes\left|D_f\cup(u,\alpha),D_g\star D_h\right\rangle\otimes\left|\alpha\right\rangle \tag{6.31}$$

$$+ \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\(D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\D_f(u)=\perp}} \frac{1}{\sqrt{2^n}}a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes\left(\left|D_f\right\rangle-\sum_\gamma\left|D_f\cup(u,\gamma)\right\rangle\right)\left|D_g\star D_h\right\rangle\otimes\left|\alpha\right\rangle \tag{6.32}$$

$$- \sum_{\substack{u,v,y,z,\alpha,\gamma,D_f,D_g,D_h;\\(D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\D_f(u)=\perp}} \frac{1}{2^n}a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\left|u,v\right\rangle\left|y\right\rangle\left|z\right\rangle \otimes\left|D_f\cup(u,\gamma),D_g\star D_h\right\rangle\otimes\left|\gamma\right\rangle \tag{6.33}$$

$$+\frac{1}{2^n}\sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\(D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\,|u,v\rangle\,|y\rangle\,|z\rangle \otimes\left(2\sum_\gamma\frac{1}{\sqrt{2^n}}\,|D_f\cup(u,\gamma)\rangle-|D_f\rangle\right)|D_g\star D_h\rangle\otimes|\widehat{0^n}\rangle \tag{6.34}$$

and

$$\Pi_{\mathsf{valid}}\mathsf{RstOE}_f\Pi_\perp\,|\phi^{\mathsf{good}}_{2i-1}\rangle = \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\(D_f,D_g,D_h)\text{: good}\\D_f(u)=\perp}}\frac{1}{\sqrt{2^n}}\,a^{(2i-1)}_{uvyzD_fD_gD_h}\,|u,v\rangle\,|y\rangle\,|z\rangle \otimes|D_f\cup(u,\alpha),D_g\star D_h\rangle\otimes|\alpha\rangle \tag{6.35}$$

$$+\frac{1}{\sqrt{2^n}}\sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\(D_f,D_g,D_h)\text{: good}\\D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_fD_gD_h}\,|u,v\rangle\,|y\rangle\,|z\rangle \otimes\left(|D_f\rangle-\sum_\gamma\frac{1}{\sqrt{2^n}}\,|D_f\cup(u,\gamma)\rangle\right)|D_g\star D_h\rangle\otimes|\widehat{0^n}\rangle\,. \tag{6.36}$$

Define $|\psi^{\mathsf{good},1}_{2i-1}\rangle$, $|\psi^{\mathsf{bad},1}_{2i-1}\rangle$, $|\phi^{\mathsf{good},1}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad},1}_{2i-1}\rangle$ by

$$|\psi^{\mathsf{good},1}_{2i-1}\rangle := |(6.25)\rangle+\Pi_{\text{pre-good}}\,|(6.29)\rangle,\quad |\psi^{\mathsf{bad},1}_{2i-1}\rangle := \mathsf{RstOE}_f\,|\psi_{2i-1}\rangle-|\psi^{\mathsf{good},1}_{2i-1}\rangle,$$
$$|\phi^{\mathsf{good},1}_{2i-1}\rangle := |(6.31)\rangle+\Pi_{\text{pre-good}}\,|(6.35)\rangle,\quad |\phi^{\mathsf{bad},1}_{2i-1}\rangle := \mathsf{RstOE}_f\,|\phi_{2i-1}\rangle-|\phi^{\mathsf{good},1}_{2i-1}\rangle\,.$$

Remark 21. *The intuition behind the definitions of $|\psi^{\mathsf{good},1}_{2i-1}\rangle$ is as follows. Roughly speaking, the two terms $|(6.25)\rangle$ and $|(6.29)\rangle$ reflect classical intuition of lazy sampling, and other terms represent the difference between classical behavior and quantum-specific behavior of oracle. Since now the output of f is written into the auxiliary register that is set to be 0, the behavior of the RstOE_f is very close to that of the classical random oracle, and the effect of quantum-specific behavior of the oracle is very small. Therefore we define $|\psi^{\mathsf{good},1}_{2i-1}\rangle$ to be the pre-good components of $|(6.25)\rangle$ and $|(6.29)\rangle$ (note that all the databases in $|(6.25)\rangle$ are good and $\Pi_{\text{pre-good}}\,|(6.25)\rangle = |(6.25)\rangle$ holds). $|\psi^{\mathsf{bad},1}_{2i-1}\rangle$ is defined in such a way that property 1 of the lemma holds. The intuition behind $|\phi^{\mathsf{good},1}_{2i-1}\rangle$ and $|\phi^{\mathsf{good},1}_{2i-1}\rangle$ is the same.*

Property 1, 4-(a), 5 of the lemma immediately follow from the definition of $|\psi^{\mathsf{good},1}_{2i-1}\rangle$, $|\psi^{\mathsf{bad},1}_{2i-1}\rangle$, $|\phi^{\mathsf{good},1}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad},1}_{2i-1}\rangle$.

Property 2 of the lemma holds since all the databases in $|(6.25)\rangle$ and $|(6.31)\rangle$ are good, and those in $\Pi_{\text{pre-good}}\,|(6.29)\rangle$ and $\Pi_{\text{pre-good}}\,|(6.35)\rangle$ are pre-good.

Property 3 of the lemma holds because, for each basis vector $|\tilde{u},\tilde{v}\rangle\,|\tilde{y}\rangle\,|\tilde{z}\rangle\otimes|\tilde{D}_f,\tilde{D}_g,\tilde{D}_h\rangle\otimes|\tilde{\gamma}\rangle$ in $|(6.25)\rangle$ (resp., in $\Pi_{\text{pre-good}}\,|(6.29)\rangle$), its coefficient is equal to the coefficient of $[|\tilde{u},\tilde{v}\rangle\,|\tilde{y}\rangle\,|\tilde{z}\rangle\otimes|\tilde{D}_f,\tilde{D}_g,\tilde{D}_h\rangle\otimes|\tilde{\gamma}\rangle]_1 = |\tilde{u},\tilde{v}\rangle\,|\tilde{y}\rangle\,|\tilde{z}\rangle\otimes|\tilde{D}_f,\tilde{D}_g\star\tilde{D}_h\rangle\otimes|\tilde{\gamma}\rangle$ in $|(6.31)\rangle$ (resp., in $\Pi_{\text{pre-good}}\,|(6.35)\rangle$).

For property 4-(b), note that all the databases in $|(6.25)\rangle$ are good while those in $\Pi_{\text{pre-good}}\,|(6.29)\rangle$ are pre-good and bad. In particular, it can be checked that the coefficient $a^{(2i-1),1}_{uvyzD_fD_gD_h}$ in $|\psi^{\mathsf{good},1}_{2i-1}\rangle$ can be represented as

$$a^{(2i-1),1}_{uvyzD_fD_gD_h} = a^{(2i-1)}_{uvyzD_fD_gD_h}\text{ if }(D_f,D_g,D_h)\text{ is good,}$$

and

$$a^{(2i-1),1}_{uvyzD_fD_gD_h} = \frac{1}{\sqrt{2^n}}a^{(2i-1)}_{uvyz(D_f\setminus(u,D_f(u)))D_gD_h}\text{ if }(D_f,D_g,D_h)\text{ is pre-good and bad,}$$

and $(D_f\setminus(u,D_f),D_g,D_h)$ is a good database in the latter equation. Therefore property 4-(b) follows from property 4 of Proposition 21.

Below we prove that property 6 of the lemma holds for $|\phi^{\mathsf{bad},1}_{2i-1}\rangle$ by showing the norms of the terms $|(6.32)\rangle$ - $|(6.34)\rangle$, $\Pi_{\text{pre-good}}\,|(6.35)\rangle$, and $|(6.36)\rangle$ are small. [11]

[11]The term $\Pi_{\text{pre-good}}\,|(6.35)\rangle$ corresponds to the classical situation where a fresh value of f is sampled and causes a bad event. Other terms correspond to the difference between classical behavior and quantum-specific behavior of the oracle.

Upper bounding the norm of $|(6.32)\rangle$.
Summands of the term (6.32) are orthogonal to each other. Hence

$$\||(6.32)\rangle\|^2 \le O\left(\frac{1}{2^n}\right) \cdot \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \left|a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\right|^2 = O\left(\frac{1}{2^n}\right)\cdot\left\|\Pi_{\not\perp}\,|\phi^{\mathsf{good}}_{2i-1}\rangle\right\|^2 \le O\left(\frac{1}{2^n}\right) \tag{6.37}$$

holds.

Upper bounding the norm of $|(6.33)\rangle$.
We have

$$\begin{aligned}
\||(6.33)\rangle\|^2 &= \left\| \sum_{\substack{u,v,y,z,\alpha,\gamma,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \frac{1}{2^n} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h} \,|u,v\rangle\,|y\rangle\,|z\rangle \otimes |D_f\cup(u,\gamma), D_g\star D_h\rangle\otimes|\gamma\rangle \right\|^2 \\
&= \sum_{\substack{u,v,y,z,\gamma,D_f;\\ D_f(u)=\perp}} \frac{1}{2^{2n}} \left\| \sum_{\substack{\alpha,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\,|D_g\star D_h\rangle \right\|^2 \\
&= \sum_{\substack{u,v,y,z,\gamma,D_f;\\ D_f(u)=\perp}} \frac{1}{2^{2n}} \sum_{D'_h} \left\| \sum_{\substack{\alpha,D_g,D_h;\\ D_g\star D_h=D'_h\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h}\,|D'_h\rangle \right\|^2 \\
&= \sum_{\substack{u,v,y,z,\gamma,D_f;\\ D_f(u)=\perp}} \frac{1}{2^{2n}} \sum_{D'_h} \left| \sum_{\substack{\alpha,D_g,D_h;\\ D_g\star D_h=D'_h\\ (D_f\cup(u,\alpha),D'_h)\text{: good}}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h} \right|^2 .
\end{aligned} \tag{6.38}$$

For each fixed tuple (u,α,D_f,D'_h), there exist at most only one pair (D_g,D_h) such that $D_g\star D_h = D'_h$ and $(D_f\cup(u,\alpha),D'_h)$ becomes good. Let us denote this pair by $\left(D_g[u,\alpha,D_f,D'_h], D_h[u,\alpha,D_f,D'_h]\right)$ (when such a pair exists). In addition, for each fixed tuple (u,D_f,D'_h), the number of α such that $(D_f\cup(u,\alpha),D'_h)$ becomes good is at most $|D'_h|\le O(i)$. Therefore, for summands of (6.38) we have

$$\begin{aligned}
&\sum_{D'_h} \left| \sum_{\substack{\alpha,D_g,D_h;\\ D_g\star D_h=D'_h\\ (D_f\cup(u,\alpha),D'_h)\text{: good}}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h} \right|^2 \\
&= \sum_{D'_h} \left| \sum_{\substack{\alpha;\\ (D_f\cup(u,\alpha),D'_h)\text{: good}}} a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_g[u,\alpha,D_f,D'_h]D_h[u,\alpha,D_f,D'_h]} \right|^2 \\
&\le \sum_{D'_h} O(i)\cdot \sum_{\substack{\alpha;\\ (D_f\cup(u,\alpha),D'_h)\text{: good}}} \left| a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_g[u,\alpha,D_f,D'_h]D_h[u,\alpha,D_f,D'_h]} \right|^2 \\
&= O(i)\cdot \sum_{D'_h} \sum_{\substack{\alpha,D_g,D_h;\\ D_g\star D_h=D'_h\\ (D_f\cup(u,\alpha),D'_h)\text{: good}}} \left| a^{(2i-1)}_{uvyzD_f\cup(u,\alpha)D_gD_h} \right|^2
\end{aligned}$$

$$= O(i) \cdot \sum_{\substack{\alpha, D_g, D_h; \\ (D_f \cup (u,\alpha), D_g \star D_h)\text{: good}}} \left| a^{(2i-1)}_{uvyzD_f \cup (u,\alpha) D_g D_h} \right|^2, \tag{6.39}$$

where we used convexity of quadratic functions for the inequality. From (6.38) and (6.39),

$$\begin{aligned}
\| |(6.33)\rangle \|^2 &\le O(i) \cdot \sum_{\substack{u,v,y,z,\gamma, D_f; \\ D_f(u)=\perp}} \frac{1}{2^{2n}} \sum_{\substack{\alpha, D_g, D_h; \\ (D_f \cup (u,\alpha), D_g \star D_h)\text{: good}}} \left| a^{(2i-1)}_{uvyzD_f \cup (u,\alpha) D_g D_h} \right|^2 \\
&= O\left(\frac{i}{2^n}\right) \cdot \sum_{\substack{u,v,y,z,\alpha, D_f, D_g, D_h; \\ D_f(u)=\perp \\ (D_f \cup (u,\alpha), D_g \star D_h)\text{: good}}} \left| a^{(2i-1)}_{uvyzD_f \cup (u,\alpha) D_g D_h} \right|^2 \cdot \left(\sum_\gamma \frac{1}{2^n} \right) \\
&= O\left(\frac{i}{2^n}\right) \cdot \left\| \Pi_\perp \left| \phi^{\mathsf{good}}_{2i-1} \right\rangle \right\|^2 \cdot 1 \le O\left(\frac{i}{2^n}\right)
\end{aligned} \tag{6.40}$$

follows.

Upper bounding the norm of $|(6.34)\rangle$.
On the term (6.34), we have that

$$\begin{aligned}
\| |(6.34)\rangle \|^2 &= \frac{1}{2^{2n}} \left\| \sum_{\substack{u,v,y,z,\alpha, D_f, D_g, D_h; \\ (D_f \cup (u,\alpha), D_g, D_h)\text{: good} \\ D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_f \cup (u,\alpha) D_g D_h} |u,v\rangle |y\rangle |z\rangle \right. \\
&\qquad \left. \otimes \left(2 \sum_\gamma \frac{1}{\sqrt{2^n}} |D_f \cup (u,\gamma)\rangle - |D_f\rangle \right) |D_g \star D_h\rangle \otimes |\widehat{0^n}\rangle \right\|^2 \\
&\le O\left(\frac{1}{2^{2n}}\right) \left\| \sum_{\substack{u,v,y,z,\alpha, D_f, D_g, D_h; \\ (D_f \cup (u,\alpha), D_g, D_h)\text{: good} \\ D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_f \cup (u,\alpha) D_g D_h} |u,v\rangle |y\rangle |z\rangle \right. \\
&\qquad \left. \otimes |D_f\rangle \otimes |D_g \star D_h\rangle \otimes |\widehat{0^n}\rangle \right\|^2 \\
&= O\left(\frac{1}{2^{2n}}\right) \sum_{\substack{u,v,y,z, D_f, D_g, D_h; \\ D_f(u)=\perp}} \left| \sum_{\substack{\alpha; \\ (D_f \cup (u,\alpha), D_g, D_h)\text{: good}}} a^{(2i-1)}_{uvyzD_f \cup (u,\alpha) D_g D_h} \right|^2 \\
&\le O\left(\frac{1}{2^{2n}}\right) \sum_{\substack{u,v,y,z, D_f, D_g, D_h; \\ D_f(u)=\perp}} \left(2^n \sum_{\substack{\alpha; \\ (D_f \cup (u,\alpha), D_g, D_h)\text{: good}}} \left| a^{(2i-1)}_{uvyzD_f \cup (u,\alpha) D_g D_h} \right|^2 \right) \\
&= O\left(\frac{1}{2^n}\right) \sum_{\substack{u,v,y,z,\alpha, D_f, D_g, D_h; \\ (D_f \cup (u,\alpha), D_g, D_h)\text{: good} \\ D_f(u)=\perp}} \left| a^{(2i-1)}_{uvyzD_f \cup (u,\alpha) D_g D_h} \right|^2 \\
&= O\left(\frac{1}{2^n}\right) \cdot \left\| \Pi_\perp \left| \phi^{\mathsf{good}}_{2i-1} \right\rangle \right\|^2 \le O\left(\frac{1}{2^n}\right)
\end{aligned} \tag{6.41}$$

holds, where we used convexity of quadratic functions for the second inequality.

Upper bounding the norm of $\Pi_{\mathsf{pre\text{-}bad}} |(6.35)\rangle$.
When (D_f, D_g, D_h) is good and $D_f(u) = \perp$, the number of α such that $(D_f \cup (u,\alpha), D_g \star D_h)$ becomes pre-bad is at

most $|D_f| + |D_h| \leq O(i)$. Therefore,

$$\begin{aligned}
\left\|\Pi_{\text{pre-bad}} |(6.35)\rangle\right\|^2 &= \left\| \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp\\ (D_f\cup(u,\alpha),D_g,D_h)\text{:pre-bad}}} \frac{1}{\sqrt{2^n}} a^{(2i-1)}_{uvyzD_fD_gD_h} |u,v\rangle |y\rangle |z\rangle \right. \\
&\qquad \left. \otimes |D_f \cup (u,\alpha), D_g \star D_h\rangle \otimes |\alpha\rangle \right\|^2 \\
&= \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \left|a^{(2i-1)}_{uvyzD_fD_gD_h}\right|^2 \sum_{\substack{\alpha;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{:pre-bad}}} \frac{1}{2^n} \\
&\leq O\left(\frac{i}{2^n}\right) \cdot \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \left|a^{(2i-1)}_{uvyzD_fD_gD_h}\right|^2 \\
&= O\left(\frac{i}{2^n}\right) \cdot \left\|\Pi_\perp |\phi^{\text{good}}_{2i-1}\rangle\right\|^2 \leq O\left(\frac{i}{2^n}\right)
\end{aligned} \tag{6.42}$$

holds.

Upper bounding the norm of $|(6.36)\rangle$.
For the term (6.36), since the summands are orthogonal to each other we have

$$\begin{aligned}
\||(6.36)\rangle\|^2 &= \left\| \frac{1}{\sqrt{2^n}} \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp}} a^{(2i-1)}_{uvyzD_fD_gD_h} |u,v\rangle |y\rangle |z\rangle \right. \\
&\qquad \left. \otimes \left(|D_f\rangle - \sum_\gamma \frac{1}{\sqrt{2^n}} |D_f \cup (u,\gamma)\rangle \right) |D_g \star D_h\rangle \otimes |\widehat{0^n}\rangle \right\|^2 \\
&\leq O\left(\frac{1}{2^n}\right) \cdot \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \left|a^{(2i-1)}_{uvyzD_fD_gD_h}\right|^2 \\
&= O\left(\frac{1}{2^n}\right) \cdot \left\|\Pi_\perp |\phi^{\text{good}}_{2i-1}\rangle\right\|^2 \leq O\left(\frac{1}{2^n}\right)
\end{aligned} \tag{6.43}$$

holds.

Upper bounding the norm of $|\phi^{\text{bad},1}_{2i-1}\rangle$.
Since we always obtain a valid database when we measure $\mathsf{RstOE}_f |\phi_{2i-1}\rangle$, we have $\mathsf{RstOE}_f |\phi_{2i-1}\rangle = \Pi_{\text{valid}}\mathsf{RstOE}_f |\phi_{2i-1}\rangle$. Thus, from (6.37), (6.40), (6.41), (6.42), and (6.43).

$$\begin{aligned}
\left\||\phi^{\text{bad},1}_{2i-1}\rangle\right\| &= \left\|\mathsf{RstOE}_f |\phi_{2i-1}\rangle - |\phi^{\text{good},1}_{2i-1}\rangle\right\| \\
&= \left\|\Pi_{\text{valid}}\mathsf{RstOE}_f |\phi_{2i-1}\rangle - |\phi^{\text{good},1}_{2i-1}\rangle\right\| \\
&\leq \left\||\phi^{\text{bad}}_{2i-1}\rangle\right\| + \left\|\Pi_{\text{valid}}\mathsf{RstOE}_f |\phi^{\text{good}}_{2i-1}\rangle - |\phi^{\text{good},1}_{2i-1}\rangle\right\| \\
&\leq \left\||\phi^{\text{bad}}_{2i-1}\rangle\right\| + \||(6.32)\rangle\| + \||(6.33)\rangle\| + \||(6.34)\rangle\| + \left\|\Pi_{\text{pre-bad}} |(6.35)\rangle\right\| + \||(6.36)\rangle\| \\
&\leq \left\||\phi^{\text{bad}}_{2i-1}\rangle\right\| + O\left(\sqrt{\frac{i}{2^n}}\right)
\end{aligned} \tag{6.44}$$

follows. Hence the sixth property of the lemma for $|\phi^{\text{bad},1}_{2i-1}\rangle$ holds. The sixth property of the lemma for $|\psi^{\text{bad},1}_{2i-1}\rangle$ can be shown in the same way. □

Next we prove the following lemma, which shows that the behavior of RstOE_g on a pre-good database for F_2 is the same as that of RstOE_h on the corresponding pre-good database for F_1^h.

Lemma 19. *Let (D_f, D_g, D_h) and (D'_f, D'_g, D'_h) be pre-good databases for F_2. Then, for each $u, u', \zeta, \zeta', y, y' \in \{0,1\}^n$ and $v, v' \in \{0,1\}^m$,*

$$\begin{aligned}&\langle u', v', \zeta', y'| \langle D'_f, D'_g, D'_h| \,\mathsf{RstOE}_g\, |u, v, \zeta, y\rangle |D_f, D_g, D_h\rangle \\ &\quad = \langle u', v', \zeta', y'| \langle D'_f, D'_g \star D'_h| \,\mathsf{RstOE}_h\, |u, v, \zeta, y\rangle |D_f, D_g \star D_h\rangle \end{aligned} \tag{6.45}$$

holds, where RstOE_g acts on $|u, v, \zeta, y\rangle$ and $|D_g\rangle$, and RstOE_h acts on $|v, \zeta, y\rangle$ and $|D_g \star D_h\rangle$. ($|u, v, \zeta\rangle$ corresponds to an input to g, and $|v, \zeta\rangle$ corresponds to an input to h. The answers to the queries are written (added) to $|y\rangle$ register.)

Proof. Since RstOE_g and RstOE_h do not change the registers $|u\rangle$, $|v\rangle$, $|\zeta\rangle$, and $|D_f\rangle$, both sides of (6.45) are 0 when $(u, v, \zeta, D_f) \neq (u', v', \zeta', D'_f)$. Below we show the equation when $(u, v, \zeta, D_f) = (u', v', \zeta', D'_f)$.

RstOE_g does not act on the $|D_h\rangle$ register. In addition, RstOE_g does not affect the register that corresponds to the element $((\tilde{u}, \tilde{v}, \tilde{\zeta}), \tilde{w})$ in D_g when $(\tilde{u}, \tilde{v}, \tilde{\zeta}) \neq (u, v, \zeta)$. Therefore, it suffices to show the equation when (i) $D_h = \emptyset$ and $D_g = \{((u, v, \zeta), w)\}$ (D_g has only a single entry), or (ii) $D_h = \emptyset$ and $D_g = \emptyset$.

In the case (i), $D_g \star D_h = \{((v, \zeta), w)\}$ holds, and the equation (6.45) follows from the first property in Proposition 3. In the case (ii), $D_g \star D_h = \emptyset$ holds, and the equation (6.45) follows from the second property in Proposition 3. □

Next we prove the following lemma, which shows how the quantum states $\mathsf{RstOE}_f |\phi^{\mathsf{good}}_{2i-1}\rangle$ and $\mathsf{RstOE}_f |\psi^{\mathsf{good}}_{2i-1}\rangle$ change when RstOE^h and RstOE_g act on them.

Lemma 20 (Actions of RstOE_h in $O_{F_1^h}$ and RstOE_g in O_{F_2})**.** *Suppose that there exist vectors $|\psi^{\mathsf{good}}_{2i-1}\rangle$, $|\psi^{\mathsf{bad}}_{2i-1}\rangle$, $|\phi^{\mathsf{good}}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad}}_{2i-1}\rangle$ that satisfy the properties of Proposition 21. Then there exist $|\psi^{\mathsf{good},2}_{2i-1}\rangle$, $|\psi^{\mathsf{bad},2}_{2i-1}\rangle$, $|\phi^{\mathsf{good},2}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad},2}_{2i-1}\rangle$ that satisfy the following properties.*

1. $\mathsf{RstOE}_g\mathsf{RstOE}_f |\psi_{2i-1}\rangle = |\psi^{\mathsf{good},2}_{2i-1}\rangle + |\psi^{\mathsf{bad},2}_{2i-1}\rangle$ *and* $\mathsf{RstOE}_h\mathsf{RstOE}_f |\phi_{2i-1}\rangle = |\phi^{\mathsf{good},2}_{2i-1}\rangle + |\phi^{\mathsf{bad},2}_{2i-1}\rangle$ *hold.*
2. $|\phi^{\mathsf{good},2}_{2i-1}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V^{(1)}_{\mathsf{pre\text{-}good}} \otimes \mathcal{H}_{\mathrm{aux}}$ *and* $|\psi^{\mathsf{good},2}_{2i-1}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V^{(2)}_{\mathsf{pre\text{-}good}} \otimes \mathcal{H}_{\mathrm{aux}}$.
3. $|\phi^{\mathsf{good},2}_{2i-1}\rangle = \left[|\psi^{\mathsf{good},2}_{2i-1}\rangle\right]_1$.
4. *There exists complex number $a^{(2i-1),2}_{uvyzD_fD_gD_h}$ that satisfies the following properties (a) and (b).*
   (a) *It holds that*
   $$|\psi^{\mathsf{good},2}_{2i-1}\rangle = \sum_{\substack{u,v,y,z,D_f,D_g,D_h \\ (D_f,D_g,D_h):\, pre\text{-}good \\ D_f(u)\neq\perp}} a^{(2i-1),2}_{uvyzD_fD_gD_h} |u, v\rangle |y\rangle |z\rangle \otimes |D_f, D_g, D_h\rangle \otimes |D_f(u)\rangle,$$
   where (u, v), y, and z corresponds $\mathcal{A}$'s register to send queries, the register to receive answers from oracles, and the register for offline computations, respectively.
   (b) $a^{(2i-1),2}_{uvyzD_fD_gD_h} = a^{(2i-1),2}_{uvyzD'_fD'_gD'_h}$ *holds if (D_f, D_g, D_h) and (D'_f, D'_g, D'_h) are equivalent,*
5. *For a pre-good database (D_f, D_g, D_h) with non-zero coefficient in $|\psi^{\mathsf{good},2}_{2i-1}\rangle$, $|D_g| \leq i$, $|D_f| \leq 2(i-1)+1$, and $|D_h| \leq i-1$ hold.*
6. $\| |\psi^{\mathsf{bad},2}_{2i-1}\rangle \| \leq \| |\psi^{\mathsf{bad}}_{2i-1}\rangle \| + O\left(\sqrt{i/2^n}\right)$ *and* $\| |\phi^{\mathsf{bad},2}_{2i-1}\rangle \| \leq \| |\phi^{\mathsf{bad}}_{2i-1}\rangle \| + O\left(\sqrt{i/2^n}\right)$ *hold.*

Proof. By Lemma 18, there exist vectors $|\psi^{\mathsf{good},1}_{2i-1}\rangle$, $|\psi^{\mathsf{bad},1}_{2i-1}\rangle$, $|\phi^{\mathsf{good},1}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad},1}_{2i-1}\rangle$ that satisfy the six properties in Lemma 18.

Define $|\psi^{\mathsf{good},2}_{2i-1}\rangle$, $|\psi^{\mathsf{bad},2}_{2i-1}\rangle$, $|\phi^{\mathsf{good},2}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad},2}_{2i-1}\rangle$ by

$$\begin{aligned}|\psi^{\mathsf{good},2}_{2i-1}\rangle &:= \Pi_{\mathsf{valid}}\mathsf{RstOE}_g |\psi^{\mathsf{good},1}_{2i-1}\rangle, \\ |\psi^{\mathsf{bad},2}_{2i-1}\rangle &:= \mathsf{RstOE}_g\mathsf{RstOE}_f |\psi_{2i-1}\rangle - |\psi^{\mathsf{good},2}_{2i-1}\rangle, \\ |\phi^{\mathsf{good},2}_{2i-1}\rangle &:= \Pi_{\mathsf{valid}}\mathsf{RstOE}_h |\phi^{\mathsf{good},1}_{2i-1}\rangle, \\ |\phi^{\mathsf{bad},2}_{2i-1}\rangle &:= \mathsf{RstOE}_h\mathsf{RstOE}_f |\phi_{2i-1}\rangle - |\phi^{\mathsf{good},1}_{2i-1}\rangle.\end{aligned}$$

Remark 22. *The intuition behind the definition of $|\psi_{2i-1}^{\mathsf{good},2}\rangle$ is as follows. First, by definition of pre-good databases, all pre-good databases in $|\psi_{2i-1}^{\mathsf{good},1}\rangle$ remain pre-good (as long as it does not become invalid) after the action of RstOE_g due to the following reasoning: If a database in $|\psi_{2i-1}^{\mathsf{good},1}\rangle$ is pre-good and bad before the query, then the current query to RstOE_g is fresh and the database becomes good after the query. If a database in $|\psi_{2i-1}^{\mathsf{good},1}\rangle$ is good before the query, then the current query to RstOE_g has been recorded in D_g. The record may be overwritten (resp., removed) after the query, but the resulting database remains good (resp., changes to pre-good) by definition of good (resp., pre-good) databases. In particular, databases do not change to pre-bad. Thus we define $|\psi_{2i-1}^{\mathsf{good},2}\rangle$ as above. $|\psi_{2i-1}^{\mathsf{bad},2}\rangle$ is defined so that property 1 of the lemma will hold. The intuition behind the definition of $|\phi_{2i-1}^{\mathsf{good},2}\rangle$ and $|\phi_{2i-1}^{\mathsf{good},2}\rangle$ is the same.*

Then, property 1, 4-(a), and 5 of the lemma follows by the definition of $|\psi_{2i-1}^{\mathsf{good},2}\rangle$, $|\psi_{2i-1}^{\mathsf{bad},2}\rangle$, $|\phi_{2i-1}^{\mathsf{good},2}\rangle$, and $|\phi_{2i-1}^{\mathsf{bad},2}\rangle$.

As explained in the above remark, all pre-good database remain pre-good (as long as it does not become invalid) after the action of RstOE_h in $O_{F_1^h}$ (and RstOE_g in O_{F_2}). Hence property 2 of Lemma 20 follows from property 2 of Lemma 18.

Recall that property 3 of Lemma 18 guarantees that the coefficient of each basis vector in $|\phi_{2i-1}^{\mathsf{good},1}\rangle$ is equal to that of the corresponding basis vector in $|\psi_{2i-1}^{\mathsf{good},1}\rangle$. Lemma 19 assures that the same thing holds for $|\phi_{2i-1}^{\mathsf{good},1}\rangle$ and $|\psi_{2i-1}^{\mathsf{good},2}\rangle$. Hence property 3 of the Lemma 20 also holds.

From property 6 in Lemma 18 it follows that

$$\begin{aligned}
\left\||\psi_{2i-1}^{\mathsf{bad},2}\rangle\right\| &= \left\|\mathsf{RstOE}_g\mathsf{RstOE}_f\,|\psi_{2i-1}\rangle - |\psi_{2i-1}^{\mathsf{good},2}\rangle\right\| \\
&= \left\|\Pi_{\mathsf{valid}}\mathsf{RstOE}_g\mathsf{RstOE}_f\,|\psi_{2i-1}\rangle - |\psi_{2i-1}^{\mathsf{good},2}\rangle\right\| \\
&= \left\|\Pi_{\mathsf{valid}}\mathsf{RstOE}_g\left(|\psi_{2i-1}^{\mathsf{good},1}\rangle + |\psi_{2i-1}^{\mathsf{bad},1}\rangle\right) - \Pi_{\mathsf{valid}}\mathsf{RstOE}_g\,|\psi_{2i-1}^{\mathsf{good},1}\rangle\right\| \\
&\leq \left\||\psi_{2i-1}^{\mathsf{bad},1}\rangle\right\| \leq \left\||\psi_{2i-1}^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i}{2^n}}\right)
\end{aligned}$$

holds,[12] and similarly $\left\||\phi_{2i-1}^{\mathsf{bad},2}\rangle\right\| \leq \left\||\phi_{2i-1}^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{i/2^n}\right)$ also holds. Hence property 6 of Lemma 20 also holds.

In what follows, we show that property 4-(b) of Lemma 20 holds. Suppose that (D_f, D_g, D_h) and $(\tilde{D}_f, \tilde{D}_g, \tilde{D}_h)$ are equivalent pre-good databases for F_2 such that $|D_g| \leq i$, $|D_f| \leq 2(i-1)+1$, and $|D_h| \leq i-1$ hold, and there exists u such that $D_f(u) \neq \perp$ and $\tilde{D}_f(u) \neq \perp$. Below we show $a_{uvyzD_fD_gD_h}^{(2i-1),2} = a_{uvyz\tilde{D}_f\tilde{D}_g\tilde{D}_h}^{(2i-1),2}$ for arbitrary v, y, and z.

If both of (D_f, D_g, D_h) and $(\tilde{D}_f, \tilde{D}_g, \tilde{D}_h)$ are good, then by definition of good databases and definition of equivalent databases, there exists an integer $s \geq 0$ and $u_i \in \{0,1\}^n$, $X_i, Y_i \in \{0,1\}^n$, $v_i^{(j)} \in \{0,1\}^m$, $w_i^{(j)} \in \{0,1\}^n$ for $i = 1, \ldots, s$ and $j = 1, \ldots, t_i$ (t_i is a positive integer for each i) such that

1. $u_i \neq u_{i'}$, $X_i \neq X_{i'}$, $Y_i \neq Y_{i'}$ for $i \neq i'$,
2. $v_i^{(j)} \neq v_i^{(j')}$ for each i and $j \neq j'$,

and

$$D_f = \{(u_i, X_i)\}_{1\leq i\leq s},\ D_g = \left\{\left(\left(u_i, v_i^{(j)}, X_i\right), w_i^{(j)}\right)\right\}_{1\leq i\leq s, 1\leq j\leq t_i}, \tag{6.46}$$

$$\tilde{D}_f = \{(u_i, Y_i)\}_{1\leq i\leq s},\ \tilde{D}_g = \left\{\left(\left(u_i, v_i^{(j)}, Y_i\right), w_i^{(j)}\right)\right\}_{1\leq i\leq s, 1\leq j\leq t_i} \tag{6.47}$$

hold.

If both of (D_f, D_g, D_h) and $(\tilde{D}_f, \tilde{D}_g, \tilde{D}_h)$ are pre-good and bad, there exist additional elements $u_0, X_0, Y_0 \in \{0,1\}^n$ such that $u_0 \neq u_i$, $X_0 \neq X_i$, $Y_0 \neq Y_i$ for $i \geq 1$, and

$$D_f = \{(u_i, X_i)\}_{0\leq i\leq s},\ D_g = \left\{\left(\left(u_i, v_i^{(j)}, X_i\right), w_i^{(j)}\right)\right\}_{1\leq i\leq s, 1\leq j\leq t_i}, \tag{6.48}$$

$$\tilde{D}_f = \{(u_i, Y_i)\}_{0\leq i\leq s},\ \tilde{D}_g = \left\{\left(\left(u_i, v_i^{(j)}, Y_i\right), w_i^{(j)}\right)\right\}_{1\leq i\leq s, 1\leq j\leq t_i} \tag{6.49}$$

hold (note that (D_f, D_g, D_h) and $(\tilde{D}_f, \tilde{D}_g, \tilde{D}_h)$ are not equivalent if one of them is good and the other is bad).

Regardless whether (D_f, D_g, D_h) is good or (D_f, D_g, D_h) is pre-good and bad, there exists a unique i such that $u = u_i$ holds. In addition, there exist a non-negative integer s' and $\zeta_1, \ldots, \zeta_{s'} \in \{0,1\}^n$, $\eta_1, \ldots, \eta_{s'} \in \{0,1\}^m$, $\xi_1, \ldots, \xi_{s'} \in \{0,1\}^n$ such that

[12] For the second equality, we used the fact that we always obtain a valid database when we measure the state $\mathsf{RstOE}_g\mathsf{RstOE}_f\,|\psi_{2i-1}\rangle$, which implies that $\mathsf{RstOE}_g\mathsf{RstOE}_f\,|\psi_{2i-1}\rangle = \Pi_{\mathsf{valid}}\mathsf{RstOE}_g\mathsf{RstOE}_f\,|\psi_{2i-1}\rangle$ holds.

1. $(\eta_i, \zeta_i) \neq (\eta_{i'}, \zeta_{i'})$ for $i \neq i'$,
2. $\zeta_i \neq X_\alpha$ and $\zeta_i \neq Y_\beta$ hold for arbitrary $i \in \{1, \ldots, s'\}$ and $\alpha, \beta \in \{1, \ldots, s\}$,

and

$$D_h = \tilde{D}_h = \{((\eta_i, \zeta_i), \xi_i)\}_{1 \leq i \leq s'} \tag{6.50}$$

holds.

Let π be a permutation on $\{0,1\}^n$ such that $\pi(X_i) = Y_i$ for each X_i and $\pi(\zeta_i) = \zeta_i$ for each ζ_i. For arbitrary D'_g such that (D_f, D'_g, D_h) is pre-good, define a database (D''_f, D''_g, D''_h) by

1. $D''_h = D_h$,
2. $D''_f = \tilde{D}_f$, and
3. $((u'', v'', \zeta''), w'') \in D''_g$ if and only if $((u'', v'', \pi^{-1}(\zeta'')), w'') \in D''_g$.

Then (D''_f, D''_g, D''_h) is a pre-good database that is equivalent to (D_f, D'_g, D_h) Let us denote this database (D''_f, D''_g, D''_h) by $\pi[D_f, D'_g, D_h]$.

Since (a) of the fourth property in Lemma 18 holds, by the definition of $|\psi^{\mathsf{good},2}_{2i-1}\rangle$,

$$\begin{aligned}
a^{(2i-1),2}_{uvyzD_fD_gD_h} &= \left(\langle u, v, y, z| \otimes \langle D_f, D_g, D_h| \otimes \langle D_f(u)|\right) |\psi^{\mathsf{good},2}_{2i-1}\rangle \\
&= \sum_{\substack{y', D'_g; \\ (D_f, D'_g, D_h)\text{: pre-good}}} \langle u, v, y, z| \otimes \langle D_f, D_g, D_h| \otimes \langle D_f(u)| \, \mathsf{RstOE}_g \, |u, v, y', z\rangle \otimes |D_f, D'_g, D_h\rangle \otimes |D_f(u)\rangle \\
&\qquad \cdot \left(\langle u, v, y', z| \otimes \langle D_f, D'_g, D_h| \otimes \langle D_f(u)|\right) |\psi^{\mathsf{good},1}_{2i-1}\rangle \\
&= \sum_{\substack{y', D'_g; \\ (D_f, D'_g, D_h)\text{: pre-good}}} c\left[y', D_f, D'_g, D_h \to y, D_f, D_g, D_h\right] \cdot a^{(2i-1),1}_{uvy'zD_fD'_gD_h}
\end{aligned}$$

follows, where we put

$$c\left[y', D_f, D'_g, D_h \to y, D_f, D_g, D_h\right] := \langle u, v, y, z| \otimes \langle D_f, D_g, D_h| \otimes \langle D_f(u)| \, \mathsf{RstOE}_g \, |u, v, y', z\rangle \otimes |D_f, D'_g, D_h\rangle \otimes |D_f(u)\rangle .$$

Now, for arbitrary y' and D'_g such that (D_f, D'_g, D_h) is pre-good,

$$a^{(2i-1),1}_{uvy'zD_fD'_gD_h} = a^{(2i-1),1}_{uvy'z\pi[D_fD'_gD_h]} \tag{6.51}$$

holds by the fourth property in Lemma 18, and

$$c\left[y', D_f, D'_g, D_h \to y, D_f, D_g, D_h\right] = c\left[y', \pi[D_f, D'_g, D_h] \to y, \pi[D_f, D_g, D_h]\right] \tag{6.52}$$

follows from the first property of Proposition 3. In addition, the followings hold:

I. $\pi[D_f, D_g, D_h] = (\tilde{D}_f, \tilde{D}_g, \tilde{D}_h)$ holds.

II. $\pi[\cdot]$ is a bijection between the set of pre-good databases of the form (D_f, D'_g, D_h) (for some D'_g) and the set of pre-good databases of the form $(\tilde{D}_f, D''_g, \tilde{D}_h)$ (for some D''_g).

Therefore we have

$$\begin{aligned}
a^{(2i-1),2}_{uvyzD_fD_gD_h} &= \sum_{\substack{y', D'_g; \\ (D_f, D'_g, D_h)\text{: pre-good}}} c\left[y', D_f, D'_g, D_h \to y, D_f, D_g, D_h\right] \cdot a^{(2i-1),1}_{uvy'zD_fD'_gD_h} \\
&\overset{\text{((6.51) and (6.52))}}{=} \sum_{\substack{y', D'_g; \\ (D_f, D'_g, D_h)\text{: pre-good}}} c\left[y', \pi[D_f, D'_g, D_h] \to y, \pi[D_f, D_g, D_h]\right] \cdot a^{(2i-1),1}_{uvy'z\pi[D_fD'_gD_h]} \\
&\overset{\text{(from I)}}{=} \sum_{\substack{y', D'_g; \\ (D_f, D'_g, D_h)\text{: pre-good}}} c\left[y', \pi[D_f, D'_g, D_h] \to y, \tilde{D}_f, \tilde{D}_g, \tilde{D}_h\right] \cdot a^{(2i-1),1}_{uvy'z\pi[D_fD'_gD_h]} \\
&\overset{\text{(from II)}}{=} \sum_{\substack{y', D''_g; \\ (\tilde{D}_f, D''_g, \tilde{D}_h)\text{: pre-good}}} c\left[y', \tilde{D}_f, D''_g, \tilde{D}_h \to y, \tilde{D}_f, \tilde{D}_g, \tilde{D}_h\right] \cdot a^{(2i-1),1}_{uvy'z\tilde{D}_fD''_g\tilde{D}_h} \\
&= a^{(2i-1),2}_{uvyz\tilde{D}_f\tilde{D}_g\tilde{D}_h},
\end{aligned} \tag{6.53}$$

which shows that property 4-(b) of Lemma 20 also holds. □

Next we prove the following lemma, which shows how the quantum states $\mathsf{RstOE}_h \cdot \mathsf{RstOE}_f\,|\phi^{\mathsf{good}}_{2i-1}\rangle$ and $\mathsf{RstOE}_g \cdot \mathsf{RstOE}_f\,|\psi^{\mathsf{good}}_{2i-1}\rangle$ change when RstOE^*_f acts on them.

Lemma 21 (Action of RstOE^*_f)**.** *Suppose that there exist vectors $|\psi^{\mathsf{good}}_{2i-1}\rangle$, $|\psi^{\mathsf{bad}}_{2i-1}\rangle$, $|\phi^{\mathsf{good}}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad}}_{2i-1}\rangle$ that satisfy the sixth properties of Proposition 21. Then there exist vectors $|\psi^{\mathsf{good},3}_{2i-1}\rangle$, $|\psi^{\mathsf{bad},3}_{2i-1}\rangle$, $|\phi^{\mathsf{good},3}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad},3}_{2i-1}\rangle$ that satisfy the following properties:*

1. $\mathsf{RstOE}^*_f\mathsf{RstOE}_g\mathsf{RstOE}_f\,|\psi_{2i-1}\rangle = |\psi^{\mathsf{good},3}_{2i-1}\rangle + |\psi^{\mathsf{bad},3}_{2i-1}\rangle$ *holds, and* $\mathsf{RstOE}^*_f\mathsf{RstOE}_h \cdot \mathsf{RstOE}_f\,|\phi_{2i-1}\rangle = |\phi^{\mathsf{good},3}_{2i-1}\rangle + |\phi^{\mathsf{bad},3}_{2i-1}\rangle$ *holds.*
2. $|\phi^{\mathsf{good},3}_{2i-1}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V^{(1)}_{\mathsf{good}}$ *and* $|\psi^{\mathsf{good},3}_{2i-1}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V^{(2)}_{\mathsf{good}}$.
3. $|\phi^{\mathsf{good},3}_{2i-1}\rangle = \left[|\psi^{\mathsf{good},3}_{2i-1}\rangle\right]_1$.
4. *There exists complex number $a^{(2i-1),3}_{uvyzD_fD_gD_h}$ such that the following properties (a) and (b) hold:*
   (a) *It holds that*
   $$|\psi^{\mathsf{good},3}_{2i-1}\rangle = \sum_{\substack{u,v,y,z,D_f,D_g,D_h:\\(D_f,D_g,D_h):good}} a^{(2i-1),3}_{uvyzD_fD_gD_h}\,|u,v\rangle\,|y\rangle\,|z\rangle \otimes |D_f, D_g, D_h\rangle, \tag{6.54}$$
   where (u, v), y, and z correspond to $\mathcal{A}$'s register to send queries, register to receive answers from oracles, and register for offline computations, respectively.
   (b) *If (D_f, D_g, D_h) and (D'_f, D'_g, D'_h) are equivalent good databases, then $a^{(2i-1),3}_{uvyzD_fD_gD_h} = a^{(2i-1),3}_{uvyzD'_fD'_gD'_h}$ holds.*
5. *For a good database (D_f, D_g, D_h) with non-zero coefficient in $|\psi^{\mathsf{good},3}_{2i-1}\rangle$, $|D_g| \le i$, $|D_f| \le 2i$, and $|D_h| \le i-1$ hold.*
6. $\| |\phi^{\mathsf{bad},3}_{2i-1}\rangle \| \le \| |\phi^{\mathsf{bad}}_{2i-1}\rangle \| + O\left(\sqrt{i/2^n}\right)$ *and* $\| |\psi^{\mathsf{bad},3}_{2i-1}\rangle \| \le \| |\psi^{\mathsf{bad}}_{2i-1}\rangle \| + O\left(\sqrt{i/2^n}\right)$ *hold.*

Proof. By Lemma 20, there exist vectors $|\phi^{\mathsf{good},2}_{2i-1}\rangle$, $|\phi^{\mathsf{bad},2}_{2i-1}\rangle$, $|\psi^{\mathsf{good},2}_{2i-1}\rangle$, and $|\psi^{\mathsf{bad},2}_{2i-1}\rangle$ that satisfy the six properties in Lemma 20.

For each tuple $(u, v, y, z, D_f, D_g, D_h)$ such that

1. $|D_g| \le i$, $|D_f| \le 2i$, and $|D_h| \le i-1$,
2. (D_f, D_g, D_h) is good, and
3. $D_f(u) = \perp$,

let α be an n-bit string such that $(D_f \cup (u, \alpha), D_g, D_h)$ is pre-good, and define

$$a^{(2i-1),3}_{uvyzD_fD_gD_h} := \sqrt{2^n}\,a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}. \tag{6.55}$$

Due to property 4-(b) of Lemma 20, the definition (6.55) is independent from the choice of α.

In addition, for each tuple $(u, v, y, z, D_f, D_g, D_h)$ such that

1. $|D_g| \le i$, $|D_f| \le 2i$, and $|D_h| \le i-1$ hold,
2. (D_f, D_g, D_h) is good,
3. $D_f(u) \ne \perp$,

define

$$a^{(2i-1),3}_{uvyzD_fD_gD_h} := a^{(2i-1),2}_{uvyzD_fD_gD_h}. \tag{6.56}$$

When the conditions $|D_g| \le i$, $|D_f| \le 2i$, and $|D_h| \le i-1$ are not satisfied, let

$$a^{(2i-1),3}_{uvyzD_fD_gD_h} := 0. \tag{6.57}$$

Define $|\psi^{\mathsf{good},3}_{2i-1}\rangle$ by the equation (6.54), where the coefficients $a^{(2i-1),3}_{uvyzD_fD_gD_h}$ are those defined in (6.55), (6.56), and (6.57). In addition, define $|\phi^{\mathsf{good},3}_{2i-1}\rangle$ by $|\phi^{\mathsf{good},3}_{2i-1}\rangle := \left[|\psi^{\mathsf{good},3}_{2i-1}\rangle\right]_1$. Define $|\psi^{\mathsf{bad},3}_{2i-1}\rangle$ and $|\phi^{\mathsf{bad},3}_{2i-1}\rangle$ by $|\psi^{\mathsf{bad},3}_{2i-1}\rangle := \mathsf{RstOE}^*_f\mathsf{RstOE}_g\mathsf{RstOE}_f|\psi_{2i-1}\rangle - |\psi^{\mathsf{good},3}_{2i-1}\rangle$ and $|\phi^{\mathsf{bad},3}_{2i-1}\rangle := \mathsf{RstOE}^*_f\mathsf{RstOE}_h\mathsf{RstOE}_f|\phi_{2i-1}\rangle - |\phi^{\mathsf{good},3}_{2i-1}\rangle$.

Remark 23. *The intuition behind the definition of $|\psi^{\mathsf{good},3}_{2i-1}\rangle$ is as follows. Roughly speaking, we defined $|\psi^{\mathsf{good},3}_{2i-1}\rangle$ in such a way that $\Pi_{\text{pre-good}}\mathsf{RstOE}_f|\psi^{\mathsf{good},3}_{2i-1}\rangle$ will be close to $|\psi^{\mathsf{good},2}_{2i-1}\rangle$. Suppose we have $|\psi^{\mathsf{good},3}_{2i-1}\rangle$ that satisfies* (6.54) *and let RstOE_f act on it (rather than we have $|\psi^{\mathsf{good},2}_{2i-1}\rangle$ and let RstOE^*_f act on it). Then, since this RstOE_f writes outputs into an auxiliary register, the behavior of RstOE_f is close to the classical lazy sampling. Intuitively, the followings will hold if $\Pi_{\text{pre-good}}\mathsf{RstOE}_f|\psi^{\mathsf{good},3}_{2i-1}\rangle = |\psi^{\mathsf{good},2}_{2i-1}\rangle$.*

1. *Databases $|D_f, D_g, D_h\rangle$ with $D_f(u) \neq \perp$ are not changed by RstOE_f, and* (6.55) *holds.*
2. *Databases $|D_f, D_g, D_h\rangle$ with $D_f(u) = \perp$ are changed to $\sum_\alpha \frac{1}{\sqrt{2^n}}|D_f \cup (u,\alpha), D_g, D_h\rangle$ by RstOE_f, and* (6.56) *holds.*

This is the reason that we defined $a^{(2i-1),3}_{uvyzD_fD_gD_h}$ and $|\psi^{\mathsf{good},3}_{2i-1}\rangle$ like above. We provided definitions based on $|\psi^{\mathsf{good},3}_{2i-1}\rangle$ rather than $|\psi^{\mathsf{good},2}_{2i-1}\rangle$, unlike previous lemmas, because it makes the proof for property 4-(b) simple (or just trivial). We defined $|\psi^{\mathsf{bad},3}_{2i-1}\rangle$, $|\phi^{\mathsf{good},3}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad},3}_{2i-1}\rangle$ in such a way that property 1-5 of the lemma will be satisfied.

Then, property 1, 2, 3, 4-(a), and 5 of Lemma 21 immediately follow from the definitions of $|\psi^{\mathsf{good},3}_{2i-1}\rangle$, $|\psi^{\mathsf{good},3}_{2i-1}\rangle$, $|\phi^{\mathsf{bad},3}_{2i-1}\rangle$, and $|\phi^{\mathsf{bad},3}_{2i-1}\rangle$. In addition, property 4-(b) of Lemma 21 follows from the definition of the coefficients $a^{(2i-1),3}_{uvyzD_fD_gD_h}$ and property 4-(b) of Lemma 20. Below we show that property 6 of Lemma 21 holds.

Remark 24. *Later, we will show that $\left\||\phi^{\mathsf{bad},3}_{2i-1}\rangle\right\|$ is upper bounded by $\left\||\phi^{\mathsf{bad},2}_{2i-1}\rangle\right\| + \left\||\phi^{\mathsf{good},3}_{2i-1}\rangle - \Pi_{\mathsf{reg}}\mathsf{RstOE}^*_f|\phi^{\mathsf{good},2}_{2i-1}\rangle\right\|$. In what follows, our main goal is to show that $\left\||\phi^{\mathsf{good},3}_{2i-1}\rangle - \Pi_{\mathsf{reg}}\mathsf{RstOE}^*_f|\phi^{\mathsf{good},2}_{2i-1}\rangle\right\|$ is in $O(\sqrt{i/2^n})$.*

By applying the first property of Proposition 3, and by definition of regular states[13], we have

$$\begin{aligned}
\Pi_{\mathsf{reg}}\mathsf{RstOE}^*_f\Pi_{\mathsf{good}}|\phi^{\mathsf{good},2}_{2i-1}\rangle &= \Pi_{\mathsf{reg}}\mathsf{RstOE}_f \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h):\text{good}\\ D_f(u)=\perp}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}|u,v\rangle|y\rangle|z\rangle \\
&\qquad\qquad \otimes|D_f\cup(u,\alpha), D_g\star D_h\rangle\otimes|\alpha\rangle \\
&= \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h):\text{ good}\\ D_f(u)=\perp}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}|u,v\rangle|y\rangle|z\rangle \\
&\qquad\qquad \otimes|D_f\cup(u,\alpha), D_g\star D_h\rangle \qquad (6.58)\\
&\quad + \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h):\text{ good}\\ D_f(u)=\perp}} \frac{1}{\sqrt{2^n}}a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}|u,v\rangle|y\rangle|z\rangle \qquad (6.59)\\
&\qquad\qquad \otimes\left(|D_f\rangle - \sum_\gamma\frac{1}{\sqrt{2^n}}|D_f\cup(u,\gamma)\rangle\right)|D_g\star D_h\rangle \\
&\quad - \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h):\text{ good}\\ D_f(u)=\perp}} \frac{1}{2^n}a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}|u,v\rangle|y\rangle|z\rangle \qquad (6.60)\\
&\qquad\qquad \otimes|D_f\cup(u,\alpha), D_g\star D_h\rangle \\
&\quad + \frac{1}{2^{3n/2}}\sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h):\text{ good}\\ D_f(u)=\perp}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}|u,v\rangle|y\rangle|z\rangle \\
&\qquad\qquad \otimes\left(2\sum_\gamma\frac{1}{\sqrt{2^n}}|D_f\cup(u,\gamma)\rangle - |D_f\rangle\right)|D_g\star D_h\rangle, \qquad (6.61)
\end{aligned}$$

where the terms (6.58)-(6.61) correspond to (3.12)-(3.15), respectively.

[13]Recall that a state is regular if and only if it does not contain invalid databases and the auxiliary register is set to be 0. In particular, the projection Π_{reg} nullifies the terms with invalid databases and those of which auxiliary register is non-zero.

On the term (6.58).

Let $\Pi_{\not\perp}$ be the orthogonal projection onto the space spanned by the vectors $|u, v\rangle |y\rangle |z\rangle |D_f, D_g, D_h\rangle$ such that $D_f(u) \neq \perp$. Then

$$|(6.58)\rangle = \Pi_{\not\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle \tag{6.62}$$

holds.

Upper bounding the norm of the terms (6.59) and (6.61).

First we have

$$\begin{aligned}
&\left\| \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \frac{1}{\sqrt{2^n}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} |u, v\rangle |y\rangle |z\rangle |D_f, D_g \star D_h\rangle \right\|^2 \\
&= \left\| \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h,D'_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\ D_f(u)=\perp\\ D_g\star D_h=D'_h}} \frac{1}{\sqrt{2^n}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} |u, v\rangle |y\rangle |z\rangle |D_f, D'_h\rangle \right\|^2 \\
&= \sum_{\substack{u,v,y,z,D_f;\\ D_f(u)=\perp}} \frac{1}{2^n} \sum_{D'_h} \left| \sum_{\substack{\alpha,D_g,D_h;\\ D_g\star D_h=D'_h\\ (D_f\cup(u,\alpha),D'_h)\text{: good}}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} \right|^2 .
\end{aligned} \tag{6.63}$$

For each database (D_f, D'_h) such that $D_f(u) = \perp$ for F_1^h, the number of α such that $(D_f \cup (u, \alpha), D'_h)$ becomes good is at most $|D'_h| \leq O(i)$. Hence we can show

$$\sum_{D'_h} \left| \sum_{\substack{\alpha,D_g,D_h;\\ D_g\star D_h=D'_h\\ (D_f\cup(u,\alpha),D'_h)\text{: good}}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} \right|^2 \leq O(i) \cdot \sum_{\substack{\alpha,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}}} \left| a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} \right|^2 \tag{6.64}$$

in the same way as we showed (6.39). From (6.63) and (6.64), it follows that

$$\begin{aligned}
&\left\| \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \frac{1}{\sqrt{2^n}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} |u, v\rangle |y\rangle |z\rangle |D_f, D_g \star D_h\rangle \right\|^2 \\
&\leq \sum_{\substack{u,v,y,z,D_f;\\ D_f(u)=\perp}} O\left(\frac{i}{2^n}\right) \cdot \sum_{\substack{\alpha,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}}} \left| a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} \right|^2 \\
&= O\left(\frac{i}{2^n}\right) \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \left| a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} \right|^2 \\
&\leq O\left(\frac{i}{2^n}\right) \cdot \left\| |\phi_{2i-1}^{\mathsf{good},2}\rangle \right\|^2 \leq O\left(\frac{i}{2^n}\right)
\end{aligned} \tag{6.65}$$

holds. We can show

$$\left\| \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\ D_f(u)=\bot}} \frac{1}{\sqrt{2^n}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} |u,v\rangle |y\rangle |z\rangle \otimes \left(\sum_\gamma \frac{1}{\sqrt{2^n}} |D_f \cup (u,\gamma)\rangle \right) |D_g \star D_h\rangle \right\|^2 \leq O\left(\frac{i}{2^n}\right) \cdot \left\| |\phi^{\mathsf{good},2}_{2i-1}\rangle \right\|^2 \leq O\left(\frac{i}{2^n}\right) \tag{6.66}$$

in the same way. Now,

$$\| |(6.59)\rangle \| \leq O\left(\sqrt{\frac{i}{2^n}}\right) \text{ and } \| |(6.61)\rangle \| \leq O\left(\sqrt{\frac{i}{2^n}}\right) \tag{6.67}$$

follow from (6.65) and (6.66).

Upper bounding the norm of the term (6.60).
We have that

$$\| |(6.60)\rangle \|^2 = \frac{1}{2^{2n}} \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: good}\\ D_f(u)=\bot}} \left| a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h} \right|^2 \leq \frac{1}{2^{2n}} \left\| |\phi^{\mathsf{good},2}_{2i-1}\rangle \right\|^2 \leq O\left(\frac{1}{2^{2n}}\right) \tag{6.68}$$

holds since all summands are orthogonal to each other.

Now, from (6.58) - (6.61), (6.62), (6.67), and (6.68),

$$\left\| \Pi_{\not\perp} |\phi^{\mathsf{good},3}_{2i-1}\rangle - \Pi_{\mathsf{reg}} \mathsf{RstOE}^*_f \Pi_{\mathsf{good}} |\phi^{\mathsf{good},2}_{2i-1}\rangle \right\| \leq O\left(\sqrt{\frac{i}{2^n}}\right) \tag{6.69}$$

follows.

Remark 25. *So far we have shown* $\left\| \Pi_{\not\perp} |\phi^{\mathsf{good},3}_{2i-1}\rangle - \Pi_{\mathsf{reg}} \mathsf{RstOE}^*_f \Pi_{\mathsf{good}} |\phi^{\mathsf{good},2}_{2i-1}\rangle \right\|$ *is small. Next we will prove* $\| \Pi_\bot |\phi^{\mathsf{good},3}_{2i-1}\rangle - \Pi_{\mathsf{reg}} \mathsf{RstOE}^*_f \Pi_{\mathsf{bad}} |\phi^{\mathsf{good},2}_{2i-1}\rangle \|$ *is small, which will lead to showing that* $\left\| |\phi^{\mathsf{good},3}_{2i-1}\rangle - \Pi_{\mathsf{reg}} \mathsf{RstOE}^*_f |\phi^{\mathsf{good},2}_{2i-1}\rangle \right\|$ *is small.*

Next, let $\Pi_\bot$ be the orthogonal projection onto the space spanned by the vectors $|u,v\rangle |y\rangle |z\rangle |D_f, D_g \star D_h\rangle$ such that $D_f(u) = \bot$. Then, by applying the second property in Proposition 3, we have

$$\mathsf{RstOE}_f \Pi_\bot |\phi^{\mathsf{good},3}_{2i-1}\rangle = \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\bot}} \frac{1}{\sqrt{2^n}} a^{(2i-1),3}_{uvyzD_fD_gD_h} |u,v\rangle |y\rangle |z\rangle \otimes |D_f \cup (u,\alpha), D_g \star D_h\rangle \otimes |\alpha\rangle \tag{6.70}$$

$$+ \frac{1}{\sqrt{2^n}} \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\bot}} a^{(2i-1),3}_{uvyzD_fD_gD_h} |u,v\rangle |y\rangle |z\rangle \otimes \left(|D_f\rangle - \sum_\gamma \frac{1}{\sqrt{2^n}} |D_f \cup (u,\gamma)\rangle \right) |D_g \star D_h\rangle \otimes |\widehat{0^n}\rangle, \tag{6.71}$$

where the terms (6.70) and (6.71) correspond to (3.16) and (3.17), respectively.

On the term $\Pi_{\mathsf{pre\text{-}good}} |(6.70)\rangle$.
By the equation (6.55),

$$\Pi_{\mathsf{pre\text{-}good}} |(6.70)\rangle = \Pi_{\mathsf{bad}} |\phi^{\mathsf{good},2}_{2i-1}\rangle \tag{6.72}$$

holds.[14]

[14] Note that here we are focusing on *pre-good and bad* databases. See also Remark 19.

Upper bounding the norms of the terms $\Pi_{\text{pre-bad}}\,|(6.70)\rangle$ and $|(6.71)\rangle$.

For a good database (D_f, D_g, D_h) for F_2, let $\mathsf{NumPreGood}(D_f, D_g, D_h)$ be the number of α such that $(D_f \cup (u,\alpha), D_g, D_h)$ becomes pre-good. Then we have $\left|\mathsf{NumPreGood}(D_f, D_g, D_h)\right| \geq 2^n - |D_f| - |D_h| \geq 2^n - 2i$, and

$$\begin{aligned}\left|a^{(2i-1),3}_{uvyzD_fD_gD_h}\right| &= \left|\frac{\sqrt{2^n}}{\mathsf{NumPreGood}(D_f, D_g, D_h)} \sum_{\substack{\alpha;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: pre-good}}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}\right| \\ &\leq \left|\frac{\sqrt{2^n}}{2^n-2i} \sum_{\substack{\alpha;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: pre-good}}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}\right| \end{aligned} \tag{6.73}$$

holds. Thus we have that

$$\begin{aligned}\left\|\Pi_\perp\,|\phi^{\mathsf{good},3}_{2i-1}\rangle\right\|^2 &= \left\|\sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp}} a^{(2i-1),3}_{uvyzD_fD_gD_h}\,|u,v\rangle\,|y\rangle\,|z\rangle\otimes|D_f, D_g\star D_h\rangle\right\|^2 \\ &= \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \left|a^{(2i-1),3}_{uvyzD_fD_gD_h}\right|^2 \\ &\overset{(6.73)}{\leq} \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \left|\frac{\sqrt{2^n}}{2^n-2i} \sum_{\substack{\alpha;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: pre-good}}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}\right|^2 \\ &= \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \left(\frac{\sqrt{2^n}}{2^n-2i}\right)^2 \left|\sum_{\substack{\alpha;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: pre-good}}} a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}\right|^2 \\ &\overset{\text{convexity}}{\leq} \sum_{\substack{u,v,y,z,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp}} \left(\frac{\sqrt{2^n}}{2^n-2i}\right)^2 \cdot 2^n \sum_{\substack{\alpha;\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: pre-good}}} \left|a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}\right|^2 \\ &= O(1)\cdot \sum_{\substack{u,v,y,z,\alpha,D_f,D_g,D_h;\\ (D_f,D_g,D_h)\text{: good}\\ D_f(u)=\perp\\ (D_f\cup(u,\alpha),D_g,D_h)\text{: pre-good}}} \left|a^{(2i-1),2}_{uvyzD_f\cup(u,\alpha)D_gD_h}\right|^2 \\ &\leq O(1)\cdot\left\|\Pi_{\mathsf{bad}}\,|\phi^{\mathsf{good},2}_{2i-1}\rangle\right\|^2 \end{aligned} \tag{6.74}$$

holds, where "convexity" denotes convexity of square functions. [15] Therefore

$$\left\|\Pi_\perp\,|\phi^{\mathsf{good},3}_{2i-1}\rangle\right\| \leq \left\|\Pi_{\mathsf{bad}}\,|\phi^{\mathsf{good},2}_{2i-1}\rangle\right\|\cdot O(1) \leq O(1) \tag{6.75}$$

holds.

Since (6.75) holds, we can show

$$\left\|\Pi_{\text{pre-bad}}\,|(6.70)\rangle\right\| \leq O\left(\sqrt{\frac{i}{2^n}}\right)\cdot\left\|\Pi_\perp\,|\phi^{\mathsf{good},3}_{2i-1}\rangle\right\| \leq O\left(\sqrt{\frac{i}{2^n}}\right) \tag{6.76}$$

[15] Note that Π_{bad} do not cancel pre-good *and bad* databases.

and

$$\||(6.71)\rangle\| \leq O\left(\sqrt{\frac{i}{2^n}}\right) \cdot \left\|\Pi_{\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle\right\| \leq O\left(\sqrt{\frac{i}{2^n}}\right) \tag{6.77}$$

in the same way as we showed (6.42) and (6.43) in the proof of Lemma 18, respectively.

Now it follows that

$$\begin{aligned}
\left\|\mathsf{RstOE}_f \Pi_{\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle - \Pi_{\mathsf{bad}} |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| &= \left\|(|(6.70)\rangle + |(6.71)\rangle) - \Pi_{\mathsf{bad}} |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| \\
&= \left\|\Pi_{\mathsf{pre\text{-}good}} |(6.70)\rangle + \Pi_{\mathsf{pre\text{-}bad}} |(6.70)\rangle + |(6.71)\rangle - \Pi_{\mathsf{bad}} |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| \\
&\overset{(6.72)}{=} \left\|\Pi_{\mathsf{pre\text{-}bad}} |(6.70)\rangle + |(6.71)\rangle\right\| \\
&\overset{(6.76) \text{ and } (6.77)}{\leq} O\left(\sqrt{\frac{i}{2^n}}\right)
\end{aligned} \tag{6.78}$$

holds.

Since $\Pi_{\mathsf{reg}}\Pi_{\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle = \Pi_{\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle$ holds by definition of $|\phi_{2i-1}^{\mathsf{good},3}\rangle$,

$$\begin{aligned}
\left\|\Pi_{\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle - \Pi_{\mathsf{reg}}\mathsf{RstOE}_f^* \Pi_{\mathsf{bad}} |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| &= \left\|\Pi_{\mathsf{reg}} \left(\Pi_{\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle - \mathsf{RstOE}_f^* \Pi_{\mathsf{bad}} |\phi_{2i-1}^{\mathsf{good},2}\rangle\right)\right\| \\
&\leq \left\|\Pi_{\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle - \mathsf{RstOE}_f^* \Pi_{\mathsf{bad}} |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| \\
&\overset{(6.78)}{\leq} O\left(\sqrt{\frac{i}{2^n}}\right)
\end{aligned} \tag{6.79}$$

holds.

From (6.69) and (6.79), it follows that

$$\begin{aligned}
\left\||\phi_{2i-1}^{\mathsf{good},3}\rangle - \Pi_{\mathsf{reg}}\mathsf{RstOE}_f^* |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| &\leq \left\|\Pi_{\not\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle - \Pi_{\mathsf{reg}}\mathsf{RstOE}_f^* \Pi_{\mathsf{good}} |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| \\
&\quad + \left\|\Pi_{\perp} |\phi_{2i-1}^{\mathsf{good},3}\rangle - \Pi_{\mathsf{reg}}\mathsf{RstOE}_f^* \Pi_{\mathsf{bad}} |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| \\
&\leq O\left(\sqrt{\frac{i}{2^n}}\right)
\end{aligned} \tag{6.80}$$

holds.

Since we obtain a regular database whenever we measure the state $\mathsf{RstOE}_f^*\mathsf{RstOE}_h \cdot \mathsf{RstOE}_f |\phi_{2i-1}\rangle$,

$$\Pi_{\mathsf{reg}}\mathsf{RstOE}_f^*\mathsf{RstOE}_h\mathsf{RstOE}_f |\phi_{2i-1}\rangle = \mathsf{RstOE}_f^*\mathsf{RstOE}_h\mathsf{RstOE}_f |\phi_{2i-1}\rangle \tag{6.81}$$

holds. Therefore, from property 1 and 6 in Lemma 20, (6.80), and (6.81),

$$\begin{aligned}
\left\||\phi_{2i-1}^{\mathsf{bad},3}\rangle\right\| &= \left\|\mathsf{RstOE}_f^*\mathsf{RstOE}_h\mathsf{RstOE}_f |\phi_{2i-1}\rangle - |\phi_{2i-1}^{\mathsf{good},3}\rangle\right\| \\
&\overset{(6.81)}{=} \left\|\Pi_{\mathsf{reg}}\mathsf{RstOE}_f^*\mathsf{RstOE}_h\mathsf{RstOE}_f |\phi_{2i-1}\rangle - |\phi_{2i-1}^{\mathsf{good},3}\rangle\right\| \\
&\overset{\text{property 1}}{=} \left\|\Pi_{\mathsf{reg}}\mathsf{RstOE}_f^* \left(|\phi_{2i-1}^{\mathsf{good},2}\rangle + |\phi_{2i-1}^{\mathsf{bad},2}\rangle\right) - |\phi_{2i-1}^{\mathsf{good},3}\rangle\right\| \\
&\leq \left\||\phi_{2i-1}^{\mathsf{good},3}\rangle - \Pi_{\mathsf{reg}}\mathsf{RstOE}_f^* |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| + \left\||\phi_{2i-1}^{\mathsf{bad},2}\rangle\right\| \\
&\overset{\text{property 6}}{\leq} \left\||\phi_{2i-1}^{\mathsf{good},3}\rangle - \Pi_{\mathsf{reg}}\mathsf{RstOE}_f^* |\phi_{2i-1}^{\mathsf{good},2}\rangle\right\| + \left\||\phi_{2i-1}^{\mathsf{bad}}\rangle\right\| + O\left(\sqrt{\frac{i}{2^n}}\right) \\
&\overset{(6.80)}{\leq} O\left(\sqrt{\frac{i}{2^n}}\right) + \left\||\phi_{2i-1}^{\mathsf{bad}}\rangle\right\|
\end{aligned} \tag{6.82}$$

follows, which implies that property 6 of Lemma 21 for $|\phi_{2i-1}^{\mathsf{bad},3}\rangle$ holds. We can show property 6 of the lemma for $|\psi_{2i-1}^{\mathsf{bad},3}\rangle$ in the same way. □

Proof of Proposition 21. We show the claim by induction on j. The claim for $j = 1$ obviously holds by setting $|\phi_1^{\mathsf{good}}\rangle = |\phi_1\rangle$, $|\psi_1^{\mathsf{good}}\rangle = |\psi_1\rangle$, $|\phi_1^{\mathsf{bad}}\rangle = 0$, and $|\psi_1^{\mathsf{bad}}\rangle = 0$.

From $(2i-1)$ to $2i$. Here we show that the claim holds for $j = 2i$ if the claim holds for $j = 1, \ldots, 2i-1$. By Lemma 21, there exist vectors $|\psi_{2i-1}^{\mathsf{good},3}\rangle$, $|\psi_{2i-1}^{\mathsf{bad},3}\rangle$, $|\phi_{2i-1}^{\mathsf{good},3}\rangle$, and $|\phi_{2i-1}^{\mathsf{bad},3}\rangle$ that satisfy the six properties in Lemma 21.

Let U_{2i-1} denote the unitary operator that corresponds to the offline computation by $\mathcal{A}$ between the $(2i-1)$-th query (the i-th query to F_1^h or F_2) and the $2i$-th query (the i-th query to h), and define

$$|\psi_{2i}^{\mathsf{good}}\rangle := U_{2i-1}\,|\psi_{2i-1}^{\mathsf{good},3}\rangle, \quad |\psi_{2i}^{\mathsf{bad}}\rangle = U_{2i-1}\,|\psi_{2i-1}^{\mathsf{bad},3}\rangle,$$
$$|\phi_{2i}^{\mathsf{good}}\rangle := U_{2i-1}\,|\phi_{2i-1}^{\mathsf{good},3}\rangle, \quad |\phi_{2i}^{\mathsf{bad}}\rangle = U_{2i-1}\,|\phi_{2i-1}^{\mathsf{bad},3}\rangle\,.$$

Then, the six properties in Proposition 21 for $j = 2i$ immediately follow from the six properties in Lemma 21. Hence the claim holds for $j = 2i$.

From $2i$ to $2i+1$. Here we show that the claim holds for $j = 2i+1$ if the claim holds for $j = 1, \ldots, 2i$. Let Π_{hit} be the orthogonal projection onto the space that is spanned by the vectors $|v,\zeta\rangle\,|y\rangle\,|z\rangle \otimes |D_f, D_g, D_h\rangle$ (or, $|v,\zeta\rangle\,|y\rangle\,|z\rangle \otimes |D_f, D_h\rangle$) such that $(u,\zeta) \in D_f$ for some u[16]. In addition, let $\Pi_{\neg\mathsf{hit}} := I - \Pi_{\mathsf{hit}}$.

Let U_{2i} denote the unitary operator that corresponds to the offline computation by $\mathcal{A}$ between the $2i$-th query (the i-th query to h) and the $(2i+1)$-st query (the $(i+1)$-st query to F_1^h or F_2). We define $|\psi_{2i}^{\mathsf{good}}\rangle$, $|\psi_{2i}^{\mathsf{bad}}\rangle$, $|\phi_{2i}^{\mathsf{good}}\rangle$, and $|\phi_{2i}^{\mathsf{bad}}\rangle$ by $|\psi_{2i+1}^{\mathsf{good}}\rangle := U_{2i}\Pi_{\mathsf{valid}}\mathsf{RstOE}_h\Pi_{\neg\mathsf{hit}}\,|\psi_{2i}^{\mathsf{good}}\rangle$, $|\psi_{2i+1}^{\mathsf{bad}}\rangle := |\psi_{2i+1}\rangle - |\psi_{2i+1}^{\mathsf{good}}\rangle$, $|\phi_{2i+1}^{\mathsf{good}}\rangle := U_{2i}\Pi_{\mathsf{valid}}\mathsf{RstOE}_h\Pi_{\neg\mathsf{hit}}\,|\phi_{2i}^{\mathsf{good}}\rangle$, $|\phi_{2i+1}^{\mathsf{bad}}\rangle := |\phi_{2i+1}\rangle - |\phi_{2i+1}^{\mathsf{good}}\rangle$.

Then property 1 of Proposition 21 for $j = 2i+1$ holds by definition of $|\psi_{2i}^{\mathsf{good}}\rangle$, $|\psi_{2i}^{\mathsf{bad}}\rangle$, $|\phi_{2i}^{\mathsf{good}}\rangle$, and $|\phi_{2i}^{\mathsf{bad}}\rangle$. Property 2, 3, 4, 5 for $j = 2i+1$ can be shown by checking how the coefficients of basis vectors in $\Pi_{\neg\mathsf{hit}}\,|\psi_{2i}^{\mathsf{good}}\rangle$ and $\Pi_{\neg\mathsf{hit}}\,|\phi_{2i}^{\mathsf{good}}\rangle$ change when RstOE_h act on them (by applying Proposition 3 on RstOE_h). [17]

Below we show that property 6 holds for $j = 2i+1$.

For a good database (D_f, D_g, D_h) for F_2, let $\mathsf{Equiv}(D_f, D_g, D_h)$ be the set of good databases that are equivalent to (D_f, D_g, D_h). Let R be a complete system of representatives of the equivalence relation on good databases for F_2 (i.e., R is a set of good databases for F_2 such that the set of all good databases for F_2 is decomposed into the disjoint union $\coprod_{(\tilde{D}_f,\tilde{D}_g,\tilde{D}_h)\in\mathsf{R}} \mathsf{Equiv}(\tilde{D}_f, \tilde{D}_g, \tilde{D}_h)$). In addition, for a good database (D_f, D_g, D_h) for F_2 and ζ, let $\mathsf{EquivHit}_\zeta(D_f, D_g, D_h)$ be the set of good databases (D'_f, D'_g, D'_h) such that (D'_f, D'_g, D'_h) is equivalent to (D_f, D_g, D_h) and $(u,\zeta) \in D'_f$ for some u. Then the following claim holds.

Claim 6. *For each ζ and each good database $(D_f, D_g, D_h) \in \mathsf{R}$ such that $a^{(2i)}_{v\zeta y z D_f D_g D_h} \neq 0$ for some v, ζ, y, z,*

$$\frac{\left|\mathsf{EquivHit}_\zeta(D_f, D_g, D_h)\right|}{\left|\mathsf{Equiv}(D_f, D_g, D_h)\right|} \leq O\left(\frac{i}{2^n}\right)$$

holds. [18]

Proof. Let

$$S := \{\zeta' \in \{0,1\}^n | \exists v, w \text{ s.t. } ((v,\zeta'), w) \in D_h\}\,,$$

and

$$\Pi_S := \{\pi : \{0,1\}^n \to \{0,1\}^n | \pi \text{ is a permutation and } \pi(\zeta') = \zeta' \text{ for all } \zeta' \in S\}\,.$$

Then, a good database (D'_f, D'_h, D'_h) is equivalent to (D_f, D_g, D_h) if and only if there exists $\pi \in \Pi_S$ such that

1. $D_h = D'_h$,
2. $(u,\zeta') \in D_f$ if and only if $(u, \pi(\zeta')) \in D'_f$, and
3. $((u, v, \zeta'), w) \in D_g$ if and only if $((u, v, \pi(\zeta')), w) \in D'_g$ holds.

[16] This projection corresponds to the event hit in Section 6.2.

[17] Intuitively, the behavior of RstOE_h on $\Pi_{\neg\mathsf{hit}}\,|\psi_{2i}^{\mathsf{good}}\rangle$ is the same as that of RstOE_h on $\Pi_{\neg\mathsf{hit}}\,|\phi_{2i}^{\mathsf{good}}\rangle$.

[18] In (6.21) we used the symbol $a^{(2i)}_{uvyzD_fD_gD_h}$ for ease of notations, but here we use $a^{(2i)}_{v\zeta yzD_fD_gD_h}$ ("uv" is replaced with "$v\zeta$") because we use the symbol $v||\zeta$ to denote an input to h.

Therefore we have

$$\frac{\left|\mathsf{EquivHit}_\zeta(D_f, D_g, D_h)\right|}{\left|\mathsf{Equiv}(D_f, D_g, D_h)\right|} = \Pr_{\pi \xleftarrow{\$} \Pi_S}\left[\text{There exists } (u, \zeta') \in D_f \text{ such that } \pi(\zeta') = \zeta\right].$$

The probability on the right hand side is upper bounded as

$$\begin{aligned}\Pr_{\pi \xleftarrow{\$} \Pi_S}\left[\text{There exists } (u, \zeta') \in D_f \text{ such that } \pi(\zeta') = \zeta\right] &\le \sum_{(u,\zeta') \in D_f} \Pr_{\pi \xleftarrow{\$} \Pi_S}\left[\pi(\zeta') = \zeta\right] \\ &= \sum_{(u,\zeta') \in D_f} \frac{|\{\pi \in \Pi_S | \pi(\zeta') = \zeta\}|}{|\Pi_S|} \\ &= \sum_{(u,\zeta') \in D_f} \frac{(2^n - |S| - 1)!}{(2^n - |S|)!} = \frac{|D_f|}{2^n - |D_h|} \quad \le \quad O\left(\frac{i}{2^n}\right).\end{aligned}$$

Hence the claim follows. □

Now we have

$$\begin{aligned}\left\|\Pi_{\mathsf{hit}} |\psi_{2i}^{\mathsf{good}}\rangle\right\|^2 &= \left\| \sum_{\substack{v,\zeta,y,z,D_f,D_g,D_h; \\ (D_f,D_g,D_h)\text{: good} \\ \exists u \text{ s.t. } (u,\zeta)\in D_f}} a^{(2i)}_{v\zeta yz D_f D_g D_h} |v,\zeta\rangle |y\rangle |z\rangle \otimes |D_f, D_g, D_h\rangle \right\|^2 \\ &= \sum_{\substack{v,\zeta,y,z,D_f,D_g,D_h; \\ (D_f,D_g,D_h)\text{: good} \\ \exists u \text{ s.t. } (u,\zeta)\in D_f}} \left| a^{(2i)}_{v\zeta yz D_f D_g D_h} \right|^2 \\ &= \sum_{(\tilde{D}_f,\tilde{D}_g,\tilde{D}_h)\in \mathsf{R}} \sum_{\substack{v,\zeta,y,z,D_f,D_g,D_h; \\ (D_f,D_g,D_h)\in \mathsf{Equiv}(\tilde{D}_f,\tilde{D}_g,\tilde{D}_h) \\ \exists u \text{ s.t. } (u,\zeta)\in D_f}} \left| a^{(2i)}_{v\zeta yz D_f D_g D_h} \right|^2 \\ &\overset{\substack{\text{property 4} \\ \text{for } j = 2i}}{=} \sum_{(\tilde{D}_f,\tilde{D}_g,\tilde{D}_h)\in \mathsf{R}} \sum_{\substack{v,\zeta,y,z,D_f,D_g,D_h; \\ (D_f,D_g,D_h)\in \mathsf{Equiv}(\tilde{D}_f,\tilde{D}_g,\tilde{D}_h) \\ \exists u \text{ s.t. } (u,\zeta)\in D_f}} \left| a^{(2i)}_{v\zeta yz \tilde{D}_f \tilde{D}_g \tilde{D}_h} \right|^2 \\ &= \sum_{(\tilde{D}_f,\tilde{D}_g,\tilde{D}_h)\in \mathsf{R}} \sum_{v,\zeta,y,z} \left|\mathsf{EquivHit}_\zeta(\tilde{D}_f, \tilde{D}_g, \tilde{D}_h)\right| \left| a^{(2i)}_{v\zeta yz \tilde{D}_f \tilde{D}_g \tilde{D}_h} \right|^2 \\ &\overset{\text{(Claim)}}{\le} O\left(\frac{i}{2^n}\right) \cdot \sum_{(\tilde{D}_f,\tilde{D}_g,\tilde{D}_h)\in \mathsf{R}} \sum_{v,\zeta,y,z} \left|\mathsf{Equiv}(\tilde{D}_f, \tilde{D}_g, \tilde{D}_h)\right| \left| a^{(2i)}_{v\zeta yz \tilde{D}_f \tilde{D}_g \tilde{D}_h} \right|^2 \\ &\overset{\substack{\text{property 4} \\ \text{for } j = 2i}}{=} O\left(\frac{i}{2^n}\right) \cdot \sum_{(\tilde{D}_f,\tilde{D}_g,\tilde{D}_h)\in \mathsf{R}} \sum_{\substack{v,\zeta,y,z,D_f,D_g,D_h; \\ (D_f,D_g,D_h)\in \mathsf{Equiv}(\tilde{D}_f,\tilde{D}_g,\tilde{D}_h)}} \left| a^{(2i)}_{v\zeta yz D_f D_g D_h} \right|^2 \\ &= O\left(\frac{i}{2^n}\right) \cdot \sum_{\substack{v,\zeta,y,z,D_f,D_g,D_h; \\ (D_f,D_g,D_h)\text{: good}}} \left| a^{(2i)}_{v\zeta yz D_f D_g D_h} \right|^2 \\ &= O\left(\frac{i}{2^n}\right) \cdot \left\||\psi_{2i}^{\mathsf{good}}\rangle\right\|^2 \le O\left(\frac{i}{2^n}\right). \end{aligned} \tag{6.83}$$

Therefore we have

$$\begin{aligned}
\left\| |\psi^{\mathsf{bad}}_{2i+1}\rangle \right\| &= \left\| |\psi_{2i+1}\rangle - |\psi^{\mathsf{good}}_{2i+1}\rangle \right\| \\
&= \left\| U_{2i}\mathsf{RstOE}_h\,|\psi_{2i}\rangle - U_{2i}\Pi_{\mathsf{valid}}\mathsf{RstOE}_h\Pi_{\neg\mathsf{hit}}\,|\psi^{\mathsf{good}}_{2i}\rangle \right\| \\
&= \left\| \Pi_{\mathsf{valid}}\mathsf{RstOE}_h\,|\psi_{2i}\rangle - \Pi_{\mathsf{valid}}\mathsf{RstOE}_h\Pi_{\neg\mathsf{hit}}\,|\psi^{\mathsf{good}}_{2i}\rangle \right\| \\
&\leq \left\| |\psi_{2i}\rangle - \Pi_{\neg\mathsf{hit}}\,|\psi^{\mathsf{good}}_{2i}\rangle \right\| = \left\| |\psi^{\mathsf{good}}_{2i}\rangle + |\psi^{\mathsf{bad}}_{2i}\rangle - \Pi_{\neg\mathsf{hit}}\,|\psi^{\mathsf{good}}_{2i}\rangle \right\| \\
&\leq \left\| |\psi^{\mathsf{bad}}_{2i}\rangle \right\| + \left\| \Pi_{\mathsf{hit}}\,|\psi^{\mathsf{good}}_{2i}\rangle \right\| \leq \left\| |\psi^{\mathsf{bad}}_{2i}\rangle \right\| + O\left(\sqrt{\frac{i}{2^n}}\right),
\end{aligned}$$

where we used the fact that we always obtain a valid database when we measure the state $\mathsf{RstOE}_h\,|\psi_{2i}\rangle$, for the third equality. Hence the sixth property for $|\psi^{\mathsf{bad}}_{2i+1}\rangle$ holds. We can show that the sixth property for $|\phi^{\mathsf{bad}}_{2i+1}\rangle$ holds in the same way. □

6.5 Quantum Security Proofs for HMAC and NMAC

The goal of this section is to show the following proposition, which is the formal version of Theorem 3.

Proposition 22. *Let $h : \{0,1\}^{m+n} \to \{0,1\}^n$ be a quantum random oracle. Suppose that the padding function $\mathsf{pad} : \{0,1\}^* \to (\{0,1\}^m)^+$ for the Merkle-Damgård construction satisfies that: (i) pad is injective, (ii) there exists a function $\mathsf{p} : \mathbb{Z}_{\geq 0} \to \{0,1\}^*$ such that $\mathsf{pad}(M) = M||\mathsf{p}(|M|)$ [19]. Let $\mathcal{A}$ be a quantum adversary that runs relative to two quantum oracles O^h and h, where O^h may depend on h [20]. Suppose that the lengths of messages that $\mathcal{A}$ queries to O^h after the padding are at most $m \cdot \ell$ when O^h is HMAC^h_K or $\mathsf{NMAC}^h_{K_1,K_2}$. In addition, suppose that $\mathcal{A}$ makes at most Q queries to O^h and q_h queries to h. Then $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{HMAC}^h_K}(\mathcal{A}) \leq O\left(\sqrt{\frac{(q_h+Q)^3\ell^5}{2^n}} + \frac{q_h+Q\ell}{2^{k/2}}\right)$ and $\mathbf{Adv}^{\mathrm{qPRF}}_{\mathsf{NMAC}^h_{K_1,K_2}}(\mathcal{A}) \leq O\left(\sqrt{\frac{(q_h+Q)^3\ell^5}{2^n}}\right)$ hold.*

Recall that HMAC^h_K (resp., $\mathsf{NMAC}^h_{K_1,K_2}$) is the composition of the functions $\mathsf{MD}^h(IV, K_{in}||\cdot)$ and $\mathsf{MD}^h(IV, K_{out}||\cdot)$ (resp., $\mathsf{MD}^h(K_1,\cdot)$ and $\mathsf{MD}^h(K_2,\cdot)$). Let us call the first and second functions the *inner function* and the *outer function*, respectively. In addition, let $\mathsf{MD}'^h : \{0,1\}^n \times (\{0,1\}^m)^+ \to \{0,1\}^n$ be the function that is defined in the same way as MD^h but without padding. Then, to prove Proposition 22, it suffices to prove the claim in the case that the inner function of HMAC^h_K (resp., $\mathsf{NMAC}^h_{K_1,K_2}$) is replaced with $\mathsf{MD}'^h(IV, K_{in}||\cdot)$ (resp., $\mathsf{MD}'^h(K_1,\cdot)$) and the lengths of messages queried by $\mathcal{A}$ is always a multiple m and at most $\ell \cdot m$, since this change does not decrease adversaries' ability to distinguish.

Thus, in what follows, we prove Proposition 22 in the case where HMAC^h_K and $\mathsf{NMAC}^h_{K_1,K_2}$ are modified as above. We show it by introducing $(2\ell+2)$ games $G_{0,H}, G_{0,N}, G_i$ $(1 \leq i \leq \ell)$, G'_i $(1 \leq i \leq \ell)$.

Game $G_{0,H}$. This is the game that the adversary is given oracle access to the quantum oracle of HMAC^h_K, in addition to h.

Game $G_{0,N}$. This is the game that the adversary is given oracle access to the quantum oracle of $\mathsf{NMAC}^h_{K_1,K_2}$, in addition to h.

Game G_i for $1 \leq i \leq \ell$. In the game G_i, the adversary is given quantum oracle access to the function H^h_i (in addition to h) that is defined as follows. Let $M := M[1]||\cdots||M[j]$ ($M[t] \in \{0,1\}^m$ for each t) be an input message for H^h_i.

1. If $j < i$, $H^h_i(M) := g_j(M)$ for a random function $g_j : \{0,1\}^{mj} \to \{0,1\}^n$.
2. If $j = i$, $H^h_i(M) := f_{out}(f_i(M))$ for a random function $f_i : \{0,1\}^{mi} \to \{0,1\}^n$ and $f_{out} : \{0,1\}^n \to \{0,1\}^n$.
3. If $j > i$, first $S_i := f_i(M[1]||\cdots||M[i])$ is computed, and then $S_t := h(M[t]||S_{t-1})$ is iteratively computed for $i < t \leq j$, and finally $H^h_i(M)$ is set as $H^h_i(M) := f_{out}(S_j)$.

See also Fig. 6.4.

Game G'_i for $1 \leq i \leq \ell$. In the game G'_i, the adversary is given quantum oracle access to the function H'^h_i (in addition to h) that is defined as follows. Let $M := M[1]||\cdots||M[j]$ ($M[t] \in \{0,1\}^m$ for each t) be an input message for H'^h_i.

[19] These conditions are satisfied for usual concrete hash functions such as SHA-2. Recall that $(\{0,1\}^m)^+$ is the set of bit strings of length positive multiple of m bits.

[20] O^h will be HMAC^h_K, $\mathsf{NMAC}^h_{K_1,K_2}$, or a random function.

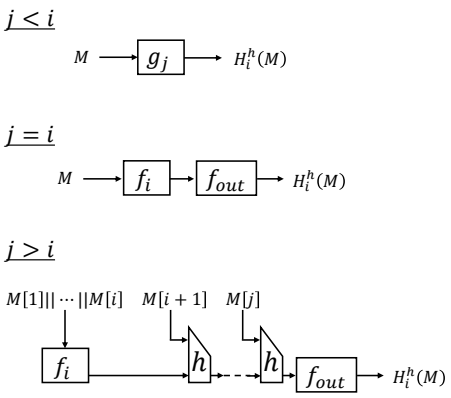


Figure 6.4: $H_i^h(M)$ in game G_i.

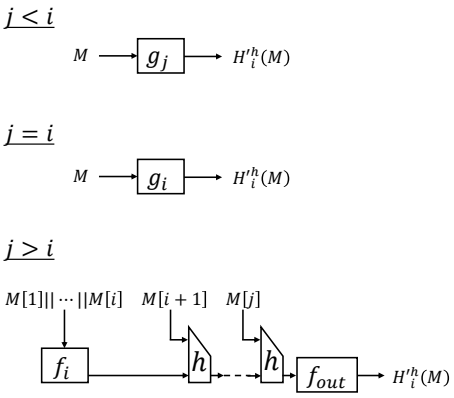


Figure 6.5: $H_i'^h(M)$ in game G_i'.

1. If $j \leq i$, $H_i'^h(M) := g_j(M)$ for a random function $g_j : \{0,1\}^{mj} \to \{0,1\}^n$.
2. If $j > i$, first $S_i := f_i(M[1]||\cdots||M[i])$ is computed, and then $S_t := h(M[t]||S_{t-1})$ is iteratively computed for $i < t \leq j$, and finally $H_i'^h(M)$ is set as $H_i'^h(M) := f_{out}(S_j)$. Here, $f_i : \{0,1\}^{mi} \to \{0,1\}^n$ and $f_{out} : \{0,1\}^n \to \{0,1\}^n$ are random functions.

See also Fig. 6.5. Since the lengths of messages queried by $\mathcal{A}$ is at most $m \cdot \ell$, G'_ℓ becomes the ideal game that $\mathcal{A}$ runs relative to a random function and h.

For the distinguishing advantage between $G_{0,N}$ and G_1, the following lemma holds.

Lemma 22 ($G_{0,N}$ and G_1)**.** $\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{NMAC}^h_{K_1,K_2},h),(H_1^h,h)}(\mathcal{A})$ *is in* $O\left(\sqrt{(q_h + Q\ell)^3/2^n}\right)$.

Proof. Recall that each message for NMAC is first processed with $\mathsf{MD}'^h(K_1,\cdot)$[21] and second with $\mathsf{MD}^h(K_2,\cdot)$. In addition, the length of messages processed with $\mathsf{MD}^h(K_2,\cdot)$ is fixed to be n. Let $\overline{\mathsf{MD}}^h(K_2,\cdot) : \{0,1\}^n \to \{0,1\}^n$ be the function that is the same as $\mathsf{MD}^h(K_2,\cdot)$ but the domain is restricted to $\{0,1\}^n$. Recall that we call $\mathsf{MD}'^h(K_1,\cdot)$ and $\overline{\mathsf{MD}}^h(K_2,\cdot)$ the inner function and the outer function, respectively. Then, the difference between $\mathsf{NMAC}^h_{K_1,K_2}$ and the function H_1^h in G_1 are: (i) The first application of h in the inner function in $\mathsf{NMAC}^h_{K_1,K_2}$ (i.e., the function $h(\cdot||K_1)$) is replaced with a random function f_1 in H_1^h. (ii) The outer function in $\mathsf{NMAC}^h_{K_1,K_2}$ is replaced with a random function f_{out} in H_1^h.

Let $\tilde{H}_1^h$ be the function that is the same as H_1^h except that the random function f_1 is replaced with $h(\cdot||K_1)$ ($K_1 \in \{0,1\}^n$ is chosen uniformly at random). Then, for a quantum adversary $\mathcal{A}$ to distinguish $(\mathsf{NMAC}^h_{K_1,K_2},h)$ from $(\tilde{H}_1^h,h)$ that makes at most Q quantum queries to $\mathsf{NMAC}^h_{K_1,K_2}$ or $\tilde{H}_1^h$ and at most q_h quantum queries to h, we can construct another adversary $\mathcal{B}$ to distinguish $(\overline{\mathsf{MD}}^h(K_2,\cdot),h)$ from (f_{out},h) that makes at most $O(Q)$ queries to $\overline{\mathsf{MD}}^h(K_2,\cdot)$ or f_{out} and at most $O(q_h + Q\ell)$ quantum queries to h as follows.

$\mathcal{B}$ is given quantum oracle access to O^h ($O^h = \overline{\mathsf{MD}}^h(K_2,\cdot)$ or $O^h = f_{out}$) and h. First, $\mathcal{B}$ chooses $K_1 \in \{0,1\}^n$ uniformly at random, and runs $\mathcal{A}$. When $\mathcal{A}$ makes a query to the second oracle (which is supposed to be h), $\mathcal{B}$ responds by querying to h. When $\mathcal{A}$ queries a message M to the first oracle (which is supposed to be $\mathsf{NMAC}^h_{K_1,K_2}$ or $\tilde{H}_1^h$), $\mathcal{B}$ computes the value $T := O^h(\mathsf{MD}'^h(K_1,M))$ by making queries to O^h and h, and responds to $\mathcal{A}$ with T. Finally $\mathcal{B}$ returns $\mathcal{A}$'s output as its own output.

Then $\mathcal{B}$ makes at most $O(Q)$ queries to O^h and at most $O(q_h + Q\ell)$ queries to h. In addition, $\mathcal{B}$ completely simulates $\mathsf{NMAC}^h_{K_1,K_2}$ or $\tilde{H}_1$ depending on $O^h = \overline{\mathsf{MD}}^h(K_2,\cdot)$ or $O^h = f_{out}$. Thus

$$\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{NMAC}^h_{K_1,K_2},h),(\tilde{H}_1^h,h)}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{dist}}_{(\overline{\mathsf{MD}}^h(K_2,\cdot),h),(f_{out},h)}(\mathcal{B}) = \mathbf{Adv}^{\mathrm{qPRF}}_{\overline{\mathsf{MD}}^h(K_2,\cdot)}(\mathcal{B}) \tag{6.84}$$

holds.

[21] Remember that the definition of $\mathsf{NMAC}^h_{K_1,K_2}$ is slightly modified during the proof of Proposition 22.

Below we consider two cases depending on whether $|\mathsf{pad}(M)| = m$ for $M \in \{0,1\}^n$.

Proof for the case that $|\mathsf{pad}(M)| = m$ for $M \in \{0,1\}^n$.

In this case, $\overline{\mathsf{MD}}^h(K_2, M) = h(\mathsf{pad}(M)||K_2)$ holds for all $M \in \{0,1\}^n$. Thus, from Lemma 13,

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\overline{\mathsf{MD}}^h(K_2,\cdot)}(\mathcal{B}) = \mathbf{Adv}^{\mathrm{qPRF}}_{h(\mathsf{pad}(\cdot)||K_2)}(\mathcal{B}) \leq O\left(\frac{q_h + Q\ell}{2^{n/2}}\right) \tag{6.85}$$

follows. From (6.84) and (6.85),

$$\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{NMAC}^h_{K_1,K_2},h),(\tilde{H}^h_1,h)}(\mathcal{A}) \leq O\left(\frac{q_h + Q\ell}{2^{n/2}}\right) \tag{6.86}$$

holds.

In the same way as we showed (6.86), we can show that

$$\mathbf{Adv}^{\mathrm{dist}}_{(\tilde{H}^h_1,h),(H^h_1,h)}(\mathcal{A}) \leq O\left(\frac{q_h + Q\ell}{2^{n/2}}\right) \tag{6.87}$$

holds (that is, we can replace $h(\cdot||K_1)$ in the inner function of $\tilde{H}^h_1$ with the random function f_1). Hence

$$\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{NMAC}^h_{K_1,K_2},h),(H^h_1,h)}(\mathcal{A}) \leq O\left(\frac{q_h + Q\ell}{2^{n/2}}\right) \tag{6.88}$$

follows from (6.86) and (6.87).

Proof for the case that $|\mathsf{pad}(M)| = m \cdot j$ $(j > 1)$ for $M \in \{0,1\}^n$.

We show the claim for the case that $|\mathsf{pad}(M)| = 2m$ for $M \in \{0,1\}^n$. Other cases can be shown in the same way.

Let $\hat{f}_{out} : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}^n$ be the function defined by $\hat{f}_{out}(u,v) := h(v||\rho(u))$, where $\rho : \{0,1\}^m \to \{0,1\}^n$ is a random function. Let $f_{big} : \{0,1\}^m \times \{0,1\}^m \to \{0,1\}^n$ be another random function.

Now,

$$\mathbf{Adv}^{\mathrm{dist}}_{(\overline{\mathsf{MD}}^h(K_2,\cdot),h),(\hat{f}_{out}\circ\mathsf{pad},h)}(\mathcal{B}) \leq O\left(\frac{q_h + Q\ell}{2^{n/2}}\right) \tag{6.89}$$

follows from Lemma 13[22], and

$$\mathbf{Adv}^{\mathrm{dist}}_{(\hat{f}_{out}\circ\mathsf{pad},h),(f_{big}\circ\mathsf{pad},h)}(\mathcal{B}) \leq O\left(\sqrt{\frac{(q_h + Q\ell)^3}{2^n}}\right) \tag{6.90}$$

follows from Proposition 20. In addition,

$$\mathbf{Adv}^{\mathrm{dist}}_{(\hat{f}_{out}\circ\mathsf{pad},h),(f_{big}\circ\mathsf{pad},h)}(\mathcal{B}) = \mathbf{Adv}^{\mathrm{dist}}_{(\hat{f}_{out}\circ\mathsf{pad},h),(f_{out},h)}(\mathcal{B}) \tag{6.91}$$

holds since $\mathsf{pad} : M \mapsto \mathsf{pad}(M)$ is injective for $M \in \{0,1\}^n$ and f_{big} is a random function. From (6.89), (6.90), and (6.91),

$$\mathbf{Adv}^{\mathrm{qPRF}}_{\overline{\mathsf{MD}}^h(K_2,\cdot)}(\mathcal{B}) = \mathbf{Adv}^{\mathrm{dist}}_{(\overline{\mathsf{MD}}^h(K_2,\cdot),h),(f_{out},h)}(\mathcal{B}) \leq O\left(\sqrt{\frac{(q_h + Q\ell)^3}{2^n}}\right) \tag{6.92}$$

follows.

Since (6.87) also holds when $|\mathsf{pad}(M)| > m$ for $M \in \{0,1\}^n$,

$$\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{NMAC}^h_{K_1,K_2},h),(H^h_1,h)}(\mathcal{A}) \leq O\left(\sqrt{\frac{(q_h + Q\ell)^3}{2^n}}\right) \tag{6.93}$$

follows from (6.84), (6.87), and (6.92). □

For the distinguishing advantage between $G_{0,H}$ and G_1, the following lemma holds.

[22]The difference between $\overline{\mathsf{MD}}^h(K_2, \cdot)$ and $\hat{f}_{out} \circ \mathsf{pad}$ is that $h(\cdot||K_2)$ in the former is replaced with ρ in the latter.

Lemma 23 ($G_{0,H}$ and G_1)**.** $\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{HMAC}^h_K,h),(H^h_1,h)}(\mathcal{A})$ *is in* $O(\sqrt{(q_h+Q\ell)^3/2^n}+(q_h+Q\ell)/2^{k/2})$.

Proof. Let $\widehat{\mathsf{NMAC}}^h_{K_1,K_2}$ be the function that is defined in the same way as $\mathsf{NMAC}^h_{K_1,K_2}$ but the outer function $\mathsf{MD}^h(K_2,\cdot)$ is replaced with the function $\mathsf{MD}''^h(K_2,\cdot)$, where $\mathsf{MD}''^h:\{0,1\}^n\times\{0,1\}^*\to\{0,1\}^n$ is defined in the same way as MD^h but the padding function is replaced from pad to pad'', which is defined by $\mathsf{pad}''(M)=M||\mathsf{p}(|M|+m)$. Then we have

$$\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{HMAC}^h_K,h),(H^h_1,h)}(\mathcal{A})\le\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{HMAC}^h_K,h),(\widehat{\mathsf{NMAC}}^h_{K_1,K_2},h)}(\mathcal{A})+\mathbf{Adv}^{\mathrm{dist}}_{(\widehat{\mathsf{NMAC}}^h_{K_1,K_2},h),(H^h_1,h)}(\mathcal{A}),\tag{6.94}$$

and we can show

$$\mathbf{Adv}^{\mathrm{dist}}_{(\widehat{\mathsf{NMAC}}^h_{K_1,K_2},h),(F^h_1,h)}(\mathcal{A})\le\begin{cases}O\left(\sqrt{\frac{q_h+Q\ell}{2^{n/2}}}\right) & \text{if } |\mathsf{p}(m+n)|=2m,\\ O\left(\sqrt{\frac{(q_h+Q\ell)^3}{2^n}}\right) & \text{if } |\mathsf{p}(n+m)|=m\cdot j\ (j>2),\end{cases}\tag{6.95}$$

in the same way as we proved Lemma 22.

Upper bounding the term $\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{HMAC}^h_K,h),(\widehat{\mathsf{NMAC}}^h_{K_1,K_2},h)}(\mathcal{A})$.

Let $\rho^h:\{0,1\}^k\to\{0,1\}^{2n}$ be the function defined by

$$\rho^h(K):=h((K||0^{m-k}\oplus\mathsf{ipad})||IV)||h((K||0^{m-k}\oplus\mathsf{opad})||IV).\tag{6.96}$$

For a quantum adversary $\mathcal{A}$ to distinguish (HMAC^h_K,h) from $(\widehat{\mathsf{NMAC}}^h_{K_1,K_2},h)$ that makes at most Q quantum queries to HMAC^h_K or $\widehat{\mathsf{NMAC}}^h_{K_1,K_2}$ and at most q_h quantum queries to h, we construct another adversary $\mathcal{B}$ to distinguish the bit string $\rho^h(K)$ (K is chosen uniformly at random) from a truly random $2n$-bit string by making $O(q_h+Q\ell)$ quantum queries to h, as follows.

$\mathcal{B}$ is given quantum oracle access to h, and given a bit string $X\in\{0,1\}^{2n}$, which is $\rho^h(K)$ ($K\leftarrow^{\$}\{0,1\}^k$) or chosen uniformly at random. Let X_1 and X_2 be the most significant n-bit and the least significant n-bit of X, respectively. First, $\mathcal{B}$ runs $\mathcal{A}$. When $\mathcal{A}$ makes a query to the second oracle (which is supposed to be h), $\mathcal{B}$ responds by querying to the oracle of h. When $\mathcal{A}$ queries a message M to the first oracle (which is supposed to be HMAC^h_K or $\widehat{\mathsf{NMAC}}^h_{K_1,K_2}$), $\mathcal{B}$ computes the value $T:=\widehat{\mathsf{NMAC}}^h_{X_1,X_2}(M)$ by making queries to h, and responds to $\mathcal{A}$ with T. Finally $\mathcal{B}$ returns $\mathcal{A}$'s output as its own output.

Then, $\mathcal{B}$ perfectly simulates HMAC^h_K or $\widehat{\mathsf{NMAC}}^h_{K_1,K_2}$ depending on whether X is $\rho^h(K)$ ($K\leftarrow^{\$}\{0,1\}^k$) or chosen uniformly at random, which implies that $\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{HMAC}^h_K,h),(\widehat{\mathsf{NMAC}}^h_{K_1,K_2},h)}(\mathcal{A})=\mathbf{Adv}^{\mathrm{qPRG}}_{\rho^h}(\mathcal{B})$. In addition, $\mathcal{B}$ makes at most $O(q_h+Q\ell)$ quantum queries to h. Thus, from Lemma 14,

$$\mathbf{Adv}^{\mathrm{dist}}_{(\mathsf{HMAC}^h_K,h),(\widehat{\mathsf{NMAC}}^h_{K_1,K_2},h)}(\mathcal{A})=\mathbf{Adv}^{\mathrm{qPRG}}_{\rho^h}(\mathcal{B})\le O\left(\frac{q_h+Q\ell}{2^{k/2}}\right)\tag{6.97}$$

follows.

The claim of Lemma 23 follows from (6.94), (6.95), and (6.97). □

For the distinguishing advantage between G_i and G'_i for $1\le i\le\ell$, the following lemma holds.

Lemma 24 (G_i and G'_i)**.** $\mathbf{Adv}^{\mathrm{dist}}_{(H^h_i,h),(H'^h_i,h)}(\mathcal{A})$ *is in* $O(\sqrt{q^3\ell^3/2^n})$*, where* $q=\max\{Q,q_h\}$.

Here we provide a rough proof overview. Details of the proof is provided later in Section 6.5.1.

Proof Overview. First, let us slightly modify the definition of H'^h_i. For a message $M=M[1]||\cdots||M[i]$ of length $m\cdot i$, the value $H'^h_i(M)$ was defined as $H'^h(M):=g_i(M)$ for a random function g_i, but here we re-define $H'^h_i(M):=f'_{out}(M,f_i(M))$, where $f'_{out}:\{0,1\}^{mi}\times\{0,1\}^n\to\{0,1\}^n$ is another random function. This modification does not change the distribution of H'^h_i since f'_{out} is random.

Our proof strategy for Lemma 24 is similar to that for Proposition 20, and we use RstOE to show the indistinguishability. In fact proving Lemma 24 is easier than proving Proposition 20 because the following difference exists between Proposition 20 and Lemma 24.

1. In the proof of Proposition 20, a function to which adversaries can *directly* query in one construction (i.e., h in F_1^h) is replaced with another function to which adversaries can query *only indirectly* in the other construction (i.e., g in F_2).

2. On the other hand, in Lemma 24, a function to which adversaries can query *only indirectly* in one construction (i.e., f_{out} in H_i^h of G_i) is replaced with another function to which adversaries can query *only indirectly* in the other construction (i.e., f'_{out} in $H_i'^h$ of G'_i).

In the proof of Proposition 20, we had to assure that the probability that an adversary directly queries to h a value that is recorded in a database is very small (i.e., the probability of the bad event hit in Section 6.2 is very small). This is the reason that we introduced the notion of equivalent databases. On the other hand, in Lemma 24, adversaries can query to both of f_{out} and f'_{out} only indirectly (adversaries do not have full control on inputs to f_{out} and f'_{out}). In particular, we can define bad events in Lemma 24 in such a way that whether they happen or not do not depend on the values of $\mathcal{A}$'s queries, and their probability can be bounded by using the randomness of outputs of random functions (like coll in Section 6.2). Therefore we do not have to introduce the notion of equivalent databases in Lemma 24. Hence it easier to prove Lemma 24 than to prove Proposition 20.

For the distinguishing advantage between G'_i and G_{i+1} for $1 \leq i < \ell$, the following lemma holds.

Lemma 25 (G'_i and G_{i+1})**.** $\mathbf{Adv}^{\mathrm{dist}}_{(H_i'^h,h),(H_{i+1}^h,h)}(\mathcal{A})$ *is in* $O\left(\sqrt{(q_h + Q\ell)^3/2^n}\right)$.

Proof. Let $f_{i+1}'^h : \{0,1\}^{m(i+1)} \to \{0,1\}^n$ be the function defined by $f_{i+1}'^h(M[1]||\cdots||M[i+1]) := h(M[i+1]||f_i(M[1]||\cdots||M[i]))$.

For an adversary $\mathcal{A}$ to distinguish $(H_i'^h, h)$ from (H_{i+1}^h, h) that makes at most Q quantum queries to $H_i'^h$ or H_{i+1}^h and at most q_h quantum queries to h, we construct another adversary $\mathcal{B}$ to distinguish $(f_{i+1}'^h, h)$ and (f_{i+1}, h) by making $O(Q)$ quantum queries to $f_{i+1}'^h$ or f_{i+1} and $O(q_h + Q\ell)$ quantum queries to h, as follows.

$\mathcal{B}$ is given a quantum oracle access to O^h, which is $f_{i+1}'^h$ or f_{i+1}, in addition to a quantum oracle access to h. First, $\mathcal{B}$ chooses functions $\tilde{g}_j : \{0,1\}^{jm} \to \{0,1\}^n$ for $j = 1, \ldots, i$ and $f_{out} : \{0,1\}^n \to \{0,1\}^n$ uniformly at random, and runs $\mathcal{A}$. When $\mathcal{A}$ makes a query to the second oracle (which is supposed to be h), $\mathcal{B}$ responds by querying to h. When $\mathcal{A}$ queries $M = M[1]||\cdots||M[j]$ to the first oracle (which is supposed to be $H_i'^h$ or H_{i+1}^h), $\mathcal{B}$ responds to $\mathcal{A}$ as follows:

1. If $j \leq i$, $\mathcal{B}$ computes $T = \tilde{g}_j(M)$ by itself, and responds to $\mathcal{A}$ with T.

2. If $j > i$, $\mathcal{B}$ computes $S_{i+1} := O^h(M)$, $S_u := h(M[u]||S_{u-1})$ for $u = i+2, \ldots, j$, and $T := f_{out}(S_j)$, by making queries to O^h and h. Then $\mathcal{B}$ responds to $\mathcal{A}$ with T.

Finally, $\mathcal{B}$ returns $\mathcal{A}$'s output as its own output.

Then $\mathcal{B}$ perfectly simulates $H_i'^h$ or H_{i+1}^h depending on whether $O^h = f_{i+1}'^h$ or $O^h = f_{i+1}$, which implies that $\mathbf{Adv}^{\mathrm{dist}}_{(H_i'^h,h),(H_{i+1}^h,h)}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{dist}}_{(f_{i+1}'^h,h),(f_{i+1},h)}(\mathcal{B})$. In addition, $\mathcal{B}$ makes at most $O(Q)$ quantum queries to $f_{i+1}'^h$ or f_{i+1} and $O(q_h + Q\ell)$ quantum queries to h. Therefore

$$\mathbf{Adv}^{\mathrm{dist}}_{(H_i'^h,h),(H_{i+1}^h,h)}(\mathcal{A}) = \mathbf{Adv}^{\mathrm{dist}}_{(f_{i+1}'^h,h),(f_{i+1},h)}(\mathcal{B}) \leq O\left(\sqrt{\frac{(q_h + Q\ell)^3}{2^n}}\right) \tag{6.98}$$

follows from Proposition 20. □

Proof of Proposition 22. The claim of the proposition immediately follows from Lemma 22, Lemma 23, Lemma 24, and Lemma 25. □

6.5.1 Proof of Lemma 24

As mentioned in the proof overview below Lemma 24, in this proof we modify the definition of $H_i'^h$ a little bit. Let $M = M[1]||\cdots||M[i]$ be a message of length $m \cdot i$. On this input, the value $H_i'^h(M)$ was defined as $H'^h(M) := g_i(M)$ for a random function g_i, but here we re-define it as

$$H_i'^h(M) := f'_{out}(M, f_i(M)), \tag{6.99}$$

where $f'_{out} : \{0,1\}^{mi} \times \{0,1\}^n \to \{0,1\}^n$ is another random function. Since f'_{out} is random, this modification does not change the distribution of the function $H_i'^h$. This subsection gives a proof only for the case $i = 1$. The proof for $i > 1$ can be done in the same way.

As in Section 2.4.2, we assume that $\mathcal{A}$ makes queries to H_1^h and h (or, $H_1^{h'}$ and h) in a sequential order. In particular, we assume that $\mathcal{A}$'s $(2i-1)$-th query is made to H_1^h (or $H_1^{h'}$) and $2i$-th query is made to h for $1 \leq i \leq q$. (For instance, $\mathcal{A}$ first queries to H_1^h (or $H_1^{h'}$) and second queries to h.) We call queries to H_1^h and $H_1^{h'}$ *online queries*, and queries to h *offline queries* since computations of h is done offline on adversaries' (quantum) computers in practical settings.

Recall that, when a message M is queried to an oracle, we implicitly assume that the length of the message $|M|$ is encoded with M like $|(|M|, M)\rangle$ (see also Remark 6). Since H_1^h and $H_1^{'h}$ take messages of different length as inputs, we carefully describe how we implement them. We assume that the unitary operators to process queries to H_1^h and $H_1^{h'}$ are implemented as follows.

Quantum Oracle of H_1^h.

1. Take $|M\rangle|y\rangle$ as an input, where $y \in \{0,1\}^n$ and $M \in \{0,1\}^{mj}$ for some $1 \leq j \leq \ell$. For ease of notations, let us define $M[t] := 0^m$ for $j+1 \leq t \leq \ell$.
2. Query $M[1]$ to f_1 and obtain
$$|M\rangle|y\rangle \otimes |S_1\rangle, \tag{6.100}$$
where $S_1 := f_1(M[1])$.
3. For $t = 2, \ldots, \ell$, iteratively compute $S_t := h(M[t]||S_{t-1})$ by querying $M[t]||S_{t-1}$ to h, to obtain
$$|M\rangle|y\rangle \otimes |S_1\rangle \cdots |S_\ell\rangle. \tag{6.101}$$
4. Copy S_j into an additional register to obtain
$$|M\rangle|y\rangle \otimes |S_1\rangle \cdots |S_\ell\rangle \otimes |S_j\rangle. \tag{6.102}$$
5. Query S_j (in the rightmost register) to f_{out} and add the result to y to obtain
$$|M\rangle|y \oplus H_1^h(M)\rangle \otimes |S_1\rangle \cdots |S_\ell\rangle \otimes |S_j\rangle. \tag{6.103}$$
6. Uncompute Steps 2 - 4 to obtain $|M\rangle|y \oplus H_1^h(M)\rangle$.

Remark 26. *Some readers may wonder why we compute not only $S_1, \ldots, S_j$ but also $S_{j+1}, \ldots, S_\ell$, and copy S_j into an auxiliary register. Those operations may seem redundant, but we perform them so that the implementation will be independent of the length of the message. (Among Steps 1-5, only Step 4 depends on the message lengths $|M|$.)*

Quantum Oracle of $H_1^{'h}$.

1. Take $|M\rangle|y\rangle$ as an input, where $y \in \{0,1\}^n$ and $M \in \{0,1\}^{mj}$ for some $1 \leq j \leq \ell$. For ease of notations, let us define $M[t] := 0^m$ for $j+1 \leq t \leq \ell$.
2. Query $M[1]$ to f_1 and obtain
$$|M\rangle|y\rangle \otimes |S_1\rangle, \tag{6.104}$$
where $S_1 := f_1(M[1])$.
3. For $t = 2, \ldots, \ell$, iteratively compute $S_t := h(M[t]||S_{t-1})$ by querying $M[t]||S_{t-1}$ to h, to obtain
$$|M\rangle|y\rangle \otimes |S_1\rangle \cdots |S_\ell\rangle. \tag{6.105}$$
4. Copy S_j into an additional register to obtain
$$|M\rangle|y\rangle \otimes |S_1\rangle \cdots |S_\ell\rangle \otimes |S_j\rangle. \tag{6.106}$$
5. If $j = 1$, query $(M[1], S_1)$ to f'_{out} and add the result to y to obtain
$$|M\rangle|y \oplus H_1^{'h}(M)\rangle \otimes |S_1\rangle \cdots |S_\ell\rangle \otimes |S_j\rangle. \tag{6.107}$$

6. If $j > 1$, query S_j (in the rightmost register) to f_{out} and add the result to y to obtain

$$|M\rangle\,|y \oplus H_1^{'h}(M)\rangle \otimes |S_1\rangle \cdots |S_\ell\rangle \otimes |S_j\rangle\,. \tag{6.108}$$

7. Uncompute Steps 2 - 4 to obtain $|M\rangle\,|y \oplus H_1^{'h}(M)\rangle$.

We show the hardness of distinguishing H_1^h and $H_1^{'h}$ by using the recording standard oracle with errors (RstOE). We assume that the quantum oracles of f_1, h, f_{out}, and f'_{out} are implemented by using RstOE (quantum queries are processed with RstOE). Let RstOE_{f_1}, RstOE_h, $\mathsf{RstOE}_{f_{out}}$, and $\mathsf{RstOE}_{f'_{out}}$ be the recording standard oracle with errors for f_1, h, f_{out}, and f'_{out}, respectively. We use the symbols D_{f_1}, D_h, $D_{f_{out}}$, and $D_{f'_{out}}$ to denote databases for f_1, h, f_{out}, and f'_{out}, respectively.

Let $O_{H_1^h}$ be the unitary operator to process queries to H_1^h implemented as above. Then, $O_{H_1^h}$ can be decomposed as

$$O_{H_1^h} = \mathsf{RstOE}^*_{f_1} \cdot \underbrace{\mathsf{RstOE}^*_h \cdots \mathsf{RstOE}^*_h}_{\ell-1 \text{ times}} \cdot \mathsf{CP} \cdot O_{out} \cdot \mathsf{CP} \cdot \underbrace{\mathsf{RstOE}_h \cdots \mathsf{RstOE}_h}_{\ell-1 \text{ times}} \cdot \mathsf{RstOE}_{f_1}, \tag{6.109}$$

where $O_{out} = \mathsf{RstOE}_{f_{out}}$ and CP denotes the unitary operator to perform the copy operation in Step 4.

Similarly, let $O_{H_1^{'h}}$ be the unitary operator to process queries to $H_1^{'h}$ implemented as above. In addition, let Π_1 be the orthogonal projection onto the space spanned by the vectors of messages $|M\rangle$ such that $|M| = 1$. Then, $O_{H_1^{'h}}$ can be decomposed as

$$O_{H_1^{'h}} = \mathsf{RstOE}^*_{f_1} \cdot \underbrace{\mathsf{RstOE}^*_h \cdots \mathsf{RstOE}^*_h}_{\ell-1 \text{ times}} \cdot \mathsf{CP} \cdot O'_{out} \cdot \mathsf{CP} \cdot \underbrace{\mathsf{RstOE}_h \cdots \mathsf{RstOE}_h}_{\ell-1 \text{ times}} \cdot \mathsf{RstOE}_{f_1}, \tag{6.110}$$

where $O'_{out} := \Pi_1 \otimes \mathsf{RstOE}_{f'_{out}} + (I - \Pi_1) \otimes \mathsf{RstOE}_{f_{out}}$.

6.5.1.1 Good and Bad Databases

Based on the description above, we introduce the notion of good and bad databases for H_1^h and $H_1^{'h}$.[23]

We say that a (tuple of) valid database $(D_{f_1}, D_h, D_{f_{out}})$ for H_1^h is *good* if and only if it satisfies the following properties.

1. For (u, ζ) and (u', ζ') in D_{f_1} such that $u \neq u'$, $\zeta \neq \zeta'$ holds (there is no collision for f_1).
2. For $((v, \zeta), w)$ and $((v', \zeta'), w')$ in D_h such that $(v, \zeta) \neq (v', \zeta')$, $w \neq w'$ holds (there is no collision for h).
3. For all $(u, \zeta) \in D_{f_1}$ and $((v, \zeta'), w) \in D_h$, $\zeta \neq w$ holds (there is no collision between outputs of f_1 and h).
4. For each $(\alpha, \beta) \in D_{f_{out}}$, there exists $(u, \alpha) \in D_{f_1}$ for some u, or there exists $((v, \zeta), \alpha) \in D_h$ for some v and ζ.

We say that $(D_{f_1}, D_h, D_{f_{out}})$ is *bad* if it is not good.

Similarly, we say that a (tuple of) valid database $(D_{f_1}, D_h, D_{f_{out}}, D_{f'_{out}})$ for $H_1^{'h}$ is *good* if and only if it satisfies the following properties.

1. For (u, ζ) and (u', ζ') in D_{f_1} such that $u \neq u'$, $\zeta \neq \zeta'$ holds (there is no collision for f_1).
2. For $((v, \zeta), w)$ and $((v', \zeta'), w')$ in D_h such that $(v, \zeta) \neq (v', \zeta')$, $w \neq w'$ holds (there is no collision for h).
3. For all $(u, \zeta) \in D_{f_1}$ and $((v, \zeta'), w) \in D_h$, $\zeta \neq w$ holds (there is no collision between outputs of f_1 and h).
4. For each $(\alpha, \beta) \in D_{f_{out}}$, there exists $((v, \zeta), \alpha) \in D_h$ for some v and ζ.
5. For each $((u, \alpha), \beta) \in D_{f'_{out}}$, $(u, \alpha) \in D_{f_1}$ holds.

We say that $(D_{f_1}, D_h, D_{f_{out}}, D_{f'_{out}})$ is *bad* if it is not good.

Intuition Behind Good and Bad Databases. Intuitively, a database $(D_{f_1}, D_h, D_{f_{out}})$ for H_1^h is defined to be good if and only if D_{f_1} does not contain collisions (the first condition on H_1^h), D_h does not contain collisions (the second condition on H_1^h), and there is no collision of output values between D_{f_1} and D_h (the third condition on H_1^h). The fourth condition on H_1^h is included so that a weird situation such as "α has been queried to f_{out}, but both of f_1 and h have not returned the value α as output" will not happen for good databases. Good databases for $H_1^{'h}$ are defined in the same way. Intuitively, a good database changes to bad if and only if an output value of f_1 or h is randomly sampled at a query, and collide with a previous output of f_1 or h.

[23] We use the symbols $u, \zeta, w, \alpha, \beta, u', \zeta', w', \alpha', \beta'$ to denote n-bit strings, and use the symbols v, v' to denote m-bit strings.

6.5.1.2 One-to-One Correspondence for Good Databases

For a good database $(D_{f_\emptyset}, D_h, D_{f_{out}}, D_{f'_{out}})$ for $H_1^{'h}$, let $\tilde{D}_{f_{out}}$ be the valid database for f_{out} such that $(\alpha, \beta) \in \tilde{D}_{f_{out}}$ if and only if $(\alpha, \beta) \in D_{f_{out}}$ or $((u, \alpha), \beta) \in D_{f'_{out}}$ for some u. Then $(D_{f_\emptyset}, D_h, \tilde{D}_{f_{out}})$ becomes a good database for H_1^h. Let us denote $(D_{f_\emptyset}, D_h, \tilde{D}_{f_{out}})$ by $[(D_{f_\emptyset}, D_h, D_{f_{out}}, D_{f'_{out}})]_{\mathsf{uni}}$ (uni is an abbreviation of "unify"). Then, it is easy to check that the map $[\cdot]_{\mathsf{uni}} : (D_{f_\emptyset}, D_h, D_{f_{out}}, D_{f'_{out}}) \mapsto [(D_{f_\emptyset}, D_h, D_{f_{out}}, D_{f'_{out}})]_{\mathsf{uni}}$ is a bijection between the set of good databases for $H_1^{'h}$ and the set of good databases for H_1^h. Let $[\cdot]_{\mathsf{sep}}$ (sep is an abbreviation of "separate") denote the inverse map of $[\cdot]_{\mathsf{uni}}$, i.e., the map from the set of good databases for H_1^h to that for $H_1^{'h}$ defined by $[[(D_{f_\emptyset}, D_h, D_{f_{out}}, D_{f'_{out}})]_{\mathsf{uni}}]_{\mathsf{sep}} = (D_{f_\emptyset}, D_h, D_{f_{out}}, D_{f'_{out}})$.

The bijections extend to (partially defined) isometries between the state spaces. Let $\mathcal{H}_{\mathcal{A}}$ be the state space of the adversary, and $\mathcal{H}_{DB}$ (resp., $\mathcal{H}'_{DB}$) be the state space of the databases for H_1^h (resp., $H_1^{'h}$). In addition, let $V_{\mathsf{good}} \subset \mathcal{H}_{DB}$ (resp., $V'_{\mathsf{good}} \subset \mathcal{H}'_{DB}$) be the subspace spanned by good databases. Then, the linear map from $\mathcal{H}_{\mathcal{A}} \otimes V_{\mathsf{good}}$ to $\mathcal{H}_{\mathcal{A}} \otimes V'_{\mathsf{good}}$ that maps $|\eta\rangle \otimes |D_{f_\emptyset}, D_h, D_{f_{out}}\rangle$ to $|\eta\rangle \otimes |[D_{f_\emptyset}, D_h, D_{f_{out}}]_{\mathsf{sep}}\rangle$ for $|\eta\rangle \in \mathcal{H}_{\mathcal{A}}$ and a good database $(D_{f_\emptyset}, D_h, D_{f_{out}})$ for H_1^h becomes an isometry. We denote this isometry and its inverse also by $[\cdot]_{\mathsf{sep}}$ and $[\cdot]_{\mathsf{uni}}$, respectively.

6.5.1.3 Notations for State Vectors

Recall that, when an adversary $\mathcal{A}$ is given oracle accesses to H_1^h (or $H_1^{'h}$) and h, we assume that the $(2i-1)$-th query is made to H_1^h (or $H_1^{'h}$) and the $2i$-th query is made to h for $1 \le i \le q$. Let $|\phi_{2i-1}\rangle$ be the whole quantum state just before $\mathcal{A}$'s i-th query to H_1^h when $\mathcal{A}$ runs relative to H_1^h and h. In addition, let $|\phi_{2i}\rangle$ be the whole quantum state just before $\mathcal{A}$'s i-th query to h when $\mathcal{A}$ runs relative to H_1^h and h. Define $|\psi_{2i-1}\rangle$ and $|\psi_{2i}\rangle$ similarly when $\mathcal{A}$ runs relative to $H_1^{'h}$ and h. For ease of notation, let $|\phi_{2q+1}\rangle$ and $|\psi_{2q+1}\rangle$ be the quantum states just before the final measurement when $\mathcal{A}$ runs relative to (H_1^h, h) and $(H_1^{'h}, h)$, respectively.

We can show that Lemma 24 follows from the proposition below in the same way as we showed Proposition 20 follows from Proposition 21.

Proposition 23. *For each $j = 1, \ldots, 2q+1$, there exist vectors $|\phi_j^{\mathsf{good}}\rangle$, $|\phi_j^{\mathsf{bad}}\rangle$, $|\psi_j^{\mathsf{good}}\rangle$, and $|\psi_j^{\mathsf{bad}}\rangle$ that satisfy the following properties:*

1. *$|\phi_j\rangle = |\phi_j^{\mathsf{good}}\rangle + |\phi_j^{\mathsf{bad}}\rangle$ and $|\psi_j\rangle = |\psi_j^{\mathsf{good}}\rangle + |\psi_j^{\mathsf{bad}}\rangle$ hold.*
2. *$|\phi_j^{\mathsf{good}}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V_{\mathsf{good}}$ and $|\psi_j^{\mathsf{good}}\rangle \in \mathcal{H}_{\mathcal{A}} \otimes V'_{\mathsf{good}}$.*
3. *$|\phi_{2i-1}^{\mathsf{good}}\rangle = \left[|\psi_{2i-1}^{\mathsf{good}}\rangle\right]_{\mathsf{uni}}$*
4. *For a good database $(D_{f_\emptyset}, D_h, D_{f_{out}}, D_{f'_{out}})$ with non-zero coefficient in $|\psi_{2i-1}^{\mathsf{good}}\rangle$ (resp., in $|\psi_{2i}^{\mathsf{good}}\rangle$), $|D_{f_\emptyset}| \le 2(i-1)$, $|D_h| \le (2\ell+1)(i-1)$, $|D_{f_{out}}| \le i-1$, and $|D_{f'_{out}}| \le i-1$ hold (resp., $|D_{f_\emptyset}| \le 2i$, $|D_h| \le (2\ell+1)(i-1)+2\ell$, $|D_{f_{out}}| \le i$, and $|D_{f'_{out}}| \le i$ hold).*
5. *$\| |\phi_j^{\mathsf{bad}}\rangle \| \le \| |\phi_{j-1}^{\mathsf{bad}}\rangle \| + O\left(\ell\sqrt{j\ell/2^n}\right)$ and $\| |\psi_j^{\mathsf{bad}}\rangle \| \le \| |\psi_{j-1}^{\mathsf{bad}}\rangle \| + O\left(\ell\sqrt{j\ell/2^n}\right)$ hold (we regard that $\| |\phi_0^{\mathsf{bad}}\rangle \| = \| |\phi_0^{\mathsf{bad}}\rangle \| = 0$).*

Intuition behind the claim of this proposition is almost the same for that of Proposition 21 (see explanations below Proposition 21), except that Proposition 23 does not contain a claim on equivalent databases (such as property 4 of Proposition 21).

As we mentioned above, in Proposition 23, a good database changes to bad only when a randomly chosen output of a random function happens to collide with an existing element in databases, like coll in Section 6.2. In particular, there does not exist a bad event that corresponds to hit in Section 6.2. This is the reason that Proposition 23 does not contain a claim on equivalent databases (recall that equivalent databases are introduced to deal with bad events like hit).

Proposition 23 can be shown in a similar way as we showed Proposition 21 by decomposing $O_{H_1^h}$ and $O_{H_1^{'h}}$ as in (6.109) and (6.110), respectively, and checking how the quantum states change when $\mathsf{RstOE}_{f_\emptyset}$, RstOE_h, $\mathsf{RstOE}_{f_{out}}$, $\mathsf{RstOE}_{f'_{out}}$, RstOE_h^*, and $\mathsf{RstOE}_{f_\emptyset}^*$ act in a sequential order. In fact the proof of Proposition 23 is even simpler than the proof of Proposition 21: Proposition 23 can be proven only with the proof techniques used in Chapter 4 and Chapter 5 because it does not contain claims on equivalent databases.

Hence, in what follows, we omit writing the details and explain only the differences between the proofs of Proposition 23 and Proposition 21. The main differences are summarized as follows.

D1. Proposition 23 does not contain a claim on equivalent databases (such as property 4 of Proposition 21).

D2. The oracles $O_{H_1^h}$ and $O_{H_1'^h}$ in Proposition 23 take inputs of various lengths while the length of inputs to the oracles in Proposition 21 are fixed.

D3. The oracles $O_{H_1^h}$ and $O_{H_1'^h}$ in Proposition 23 invoke random functions many (about 2ℓ) times whereas the oracles in Proposition 21 do at most only 3 times.

As mentioned before, the difference D1 just simplify some parts of the proof. To translate the proof of Proposition 21 into a proof of Proposition 23, what we have to do about the differences D1 is just to ignore the arguments on property 4 of Proposition 21.

The second difference D2 may look like it make the proof of Proposition 23 complex, but actually it does not. Each message M is encoded with its length $|M|$ like $|(|M|, M)\rangle$, and the vector $|(|M|, M)\rangle$ is orthogonal to the vector of another message $|(|M'|, M')\rangle$ if $|M'| \neq |M|$. In addition, the oracles do not affect the message register. Thus, to show the five properties of Proposition 23, it suffices to prove such properties hold when the lengths of all the messages are fixed and equal. When $|M| \geq 2m$ (i.e., M consists of two or more blocks), apparently the behaviors of the oracles $O_{H_1^h}$ and $O_{H_1'^h}$ on M are the same as long as databases are good because $H_1^h(M) = H_1'^h(M)$. When $|M| = m$ (i.e., M consists of a single block), we can also prove that the behaviors of $O_{H_1^h}$ and $O_{H_1'^h}$ are the same as long as databases are good in a way similar to the proof of Proposition 21. Hence properties 1-4 of Proposition 23 can be shown. The proof for property 5 of Proposition 23 is similar to that for property 6 of Proposition 21, except that the upper bounds of $\| |\phi_j^{\mathsf{bad}}\rangle \|$ and $\| |\psi_j^{\mathsf{bad}}\rangle \|$ are slightly different. This difference is attributed to D3, which we explain below.

The difference D3 increases the number of total queries made to h to $O(\ell q)$, and the number of elements in the database of h at the i-th query to $O_{H_1^h}$ (resp., $O_{H_1'^h}$) or at the i-th offline query to h becomes $O(\ell \cdot i)$. Hence, roughly speaking, the norm of the "bad" vector increases by $O(\sqrt{\ell i/2^n})$ (but not $O(\sqrt{i/2^n})$) at each query to h during the i-th query to $O_{H_1^h}$ (resp., $O_{H_1'^h}$) or the i-th offline query to h. In addition, h and f_1 are invoked $O(\ell)$ times in total at each query to $O_{H_1^h}$ (resp., $O_{H_1'^h}$). Hence the upper bound of $\| |\phi_j^{\mathsf{bad}}\rangle \|$ in property 5 of Proposition 23 is $\| |\phi_{j-1}^{\mathsf{bad}}\rangle \| + O\left(\ell\sqrt{j\ell/2^n}\right)$ but not $\| |\phi_{j-1}^{\mathsf{bad}}\rangle \| + O\left(\sqrt{j/2^n}\right)$ (resp., the upper bound of $\| |\psi_j^{\mathsf{bad}}\rangle \|$ is $\| |\psi_{j-1}^{\mathsf{bad}}\rangle \| + O\left(\ell\sqrt{j\ell/2^n}\right)$ but not $\| |\psi_{j-1}^{\mathsf{bad}}\rangle \| + O\left(\sqrt{j/2^n}\right)$), unlike property 6 of Proposition 21.

Chapter 7

Indifferentiability of the SKINNY-HASH Internal Functions

This chapter provides a formal proof that the SKINNY-HASH internal function (the SHI function) is indifferentiable from the random oracle. The SHI function is a function of fixed input-output length based on a tweakable block cipher, which is used in a function-based sponge hash called SKINNY-HASH [BJK+20]. The designers of the SKINNY-HASH claim that the SHI function is indifferentiable from a random oracle, but they do not provide formal security proofs. We prove that the SHI function is indeed provably secure as claimed by the designers by showing a formal security proof. See also Section 1.6 for a more detailed overview.

The result of this chapter is practical rather than theoretical: It shows we can achieve an efficient and highly secure construction to build functions of fixed input-output length from tweakable block ciphers in practical use cases. Unlike previous chapters, this chapter provides only a *classical* security proof due to technical limitations. Nevertheless, we still think that the result has some implications in post-quantum cryptography. Though we do not have any post-quantum security proof of the SHI function, it is unlikely to be broken by quantum attacks. Hence we will be able to build post-quantum secure hash functions based on the SHI function. The SHI function is an important example of an internal function for function-based sponge hash because there does not exist many other instances. Thus it will also play an important role when we understand post-quantum security of function-based sponge hash functions. Moreover, when post-quantum security of the SHI function will be proved, the proof will be based on our classical proof. Therefore our result will help future studies on post-quantum security of hash functions. See also Section 1.7 for the relationship of the results in this chapter with those in other chapters.

Let E denote an n-bit ideal cipher with ℓn-bit keys, where ℓ is a small constant. Recall that the SHI function F^E is defined as

$$F^E(x) := E_x(c_1)||\cdots||E_x(c_\ell), \tag{7.1}$$

where $c_1, \ldots, c_\ell$ are fixed distinct n-bit constants.

The goal of this chapter is to prove the following theorem, which shows that the SHI function is indifferentiable from a random oracle up to $O(2^n)$ queries. Together with the composition theorem, this theorem assures that the security of the sponge construction does not decrease when its internal function is instantiated with the SHI function up to $O(2^n)$ queries.

Theorem 12. *There exists a simulator $\mathcal{S}$ that satisfies the following conditions.*

1. *$\mathcal{S}$ makes at most* 1 *query to* RO *and returns an output in time $O(1)$ at each invocation of $\mathcal{S}$.*
2. *For an arbitrary adversary $\mathcal{A}$ that makes at most $Q_{\mathcal{A}}$ queries to H^E and makes $q_{\mathcal{A}}$ queries to E and E^{-1} in total,*

$$\mathbf{Adv}^{\mathrm{indiff}}_{(F^E,(E,E^{-1})),\mathsf{RO},\mathcal{S}}(\mathcal{A}) \leq \frac{\ell^2(q_{\mathcal{A}} + \ell Q_{\mathcal{A}})}{2^n}$$

holds.

Intuition of the Proof for Theorem 12. Intuitively, we construct a simulator $\mathcal{S}$ as follows[1].

[1]Our intuition for the simulator is based on "Rationale of F_{256} and F_{384}" in the original specification [BJK+20]. Note that the original explanation in [BJK+20] is very rough (only two paragraphs) and it is not trivial how to derive a formal security proof from that.

When an adversary $\mathcal{A}$ queries a value (K, X) to E that $\mathcal{A}$ has already queried before, $\mathcal{S}$ just returns the previous result stored in a list L_K.

When $\mathcal{A}$ queries a fresh value (K, X) to E such that $\mathcal{A}$ has never queried (K, Z) for any Z to E nor E^{-1}, $\mathcal{S}$ first queries K to the random oracle $\mathsf{RO} : \{0,1\}^{n\ell} \to \{0,1\}^{n\ell}$, and simulates the values $E_K(c_1), \ldots, E_K(c_\ell)$ as $E_K(c_1)||\cdots||E_K(c_\ell) := \mathsf{RO}(K)$. $\mathcal{S}$ stores the pairs $(c_1, E_K(c_1)), \ldots, (c_\ell, E_K(c_\ell))$ into L_K. If $X = c_i$ for some i, then $\mathcal{S}$ returns the value $E_K(c_i)$ to $\mathcal{A}$. If $X \neq c_i$ for all i, then $\mathcal{S}$ picks a value Y from $\{0,1\}^n \setminus \{E_K(c_1), \ldots, E_K(c_\ell)\}$ uniformly at random, simulates the value $E_K(X)$ as $E_K(X) := Y$, stores the pair (X, Y) into the list L_K, and returns Y to $\mathcal{A}$.

When $\mathcal{A}$ queries a value (K, X) to E such that $\mathcal{A}$ has already queried (K, Z) for some Z to E or E^{-1} before but $(X, Y) \notin L_K$ for any Y, $\mathcal{S}$ chooses Y from $\{0,1\}^{n\ell}$ randomly in such a way that $Y \neq Y'$ holds for every pair $(X', Y') \in L_K$, stores the pair (X, Y) into the list L_K, and returns Y to $\mathcal{A}$.

Queries to E^{-1} are simulated in the same way.

The above simulation fails only when $\mathcal{S}$ queries K to the random oracle RO, and $\mathsf{RO}(K) = Y_1||\cdots||Y_\ell$ ($Y_i \in \{0,1\}^n$ for each i) happens to satisfy $Y_i = Y_j$ for some $i \neq j$. Roughly speaking, the probability of this event can be upper bounded by $O(1/2^n)$ for each K, and thus the failure probability of $\mathcal{S}$ is always negligibly small if the number of queries made by $\mathcal{A}$ is smaller than 2^n. Note that such an event never holds in the real world since, if we divide $F^E(K) \in \{0,1\}^{n\ell}$ into n-bit blocks as $F^E(K) = Y_1||\cdots||Y_\ell$, then $Y_i = E_K(c_i)$ never matches $Y_j = E_K(c_j)$ for $i \neq j$, for arbitrary K.

Our contribution in this chapter is to provide a formal proof that the above intuition is correct.

Proof of Theorem 4. We show the theorem with the code-based game-playing proof technique [BR06], by introducing 6 games $G_1, \ldots, G_6$.

Game G_1. G_1 is the *real* game, where the adversary $\mathcal{A}$ runs relative to the oracles F^E, E, and E^{-1}. We assume that the oracle of the ideal cipher E is implemented by using lazy sampling. See Fig. 7.1 for details.

Games G_2 and G_3. G_2 is identical to G_1 except that, when a value (K, X) (resp., (K, Y)) is queried to E (resp., E^{-1}) such that (K, Z) has not been queried to E nor E^{-1} for any Z, the values $E_K(c_1), \ldots, E_K(c_\ell)$ are sampled before answering to the query. In addition, the sampling of $E_K(c_1), \ldots, E_K(c_\ell)$ are performed as follows:

1. Choose $Y_1, \ldots, Y_\ell \in \{0,1\}^n$ independently and uniformly at random.
2. If $Y_i = Y_j$ holds for some $i \neq j$, set flag to be bad, and re-sample $Y_1, \ldots, Y_\ell$ in such a way that $Y_i \neq Y_j$ holds for all $i \neq j$.
3. Set $E_K(c_i) := Y_i$ for $i = 1, \ldots, \ell$.

The procedure F^E is not changed from G_1. G_3 is identical to G_2 except that the re-sampling of $Y_1, \ldots, Y_\ell$ is not performed even if flag is set to be bad. See Fig. 7.2 for details.

Games G_4 and G_5. In the game G_4, compared to G_3, a random oracle RO is introduced, and the sampling of $Y_1, \ldots, Y_\ell$ in E and E^{-1} when L_K is empty is replaced with the query of K to the random oracle RO. F^E is not changed in G_4. The game G_5 is identical to G_4 except that F^E is modified in such a way that $F^E(T) := \mathsf{RO}(T)$. See Fig. 7.3 for details.

Game G_6. G_6 is the ideal game. In G_6, $\mathcal{A}$ runs relative to RO and $\mathcal{S}^{\mathsf{RO}}$ instead of F^E and (E, E^{-1}), where $\mathcal{S}$ is a simulator defined as in Fig. 7.4. Given an input $(b, K, Z) \in \{0,1\} \times \{0,1\}^{n\ell} \times \{0,1\}^n$, $\mathcal{S}$ simulates $E(K, Z)$ if $b = 0$ and $E^{-1}(K, Z)$ if $b = 1$. The behavior of $\mathcal{S}$ is the same as that of E and E^{-1} in the games G_4 and G_5.

Below we give an upper bound of the indifferentiability advantage $\mathbf{Adv}^{\mathrm{indiff}}_{(F^E,(E,E^{-1})),\mathsf{RO},\mathcal{S}}(\mathcal{A})$. First, by definition of the games,

$$\left|\Pr\left[1 \leftarrow G_i^{\mathcal{A}}\right] - \Pr\left[1 \leftarrow G_{i+1}^{\mathcal{A}}\right]\right| = 0 \tag{7.2}$$

holds for $i = 1, 3, 4, 5$.

On the difference between G_2 and G_3, let $\mathsf{SetBad}(i)$ denote the event that flag is set to be bad at the i-th query to E

Game $G_1^{\mathcal{A}}$
$x \leftarrow \mathcal{A}^{F^E,(E,E^{-1})}$
return x

Procedure $E(K, X)$
if there exists Y such that $(X, Y) \in L_K$
  return Y
else
  $Y \xleftarrow{\$} \{0,1\}^n \setminus L_{K,\text{out}}$
  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{X\}$
  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y\}$
  $L_K \leftarrow L_K \cup \{(X, Y)\}$
  return Y

Procedure $E^{-1}(K, Y)$
if there exists X such that $(X, Y) \in L_K$
  return X
else
  $X \xleftarrow{\$} \{0,1\}^n \setminus L_{K,\text{in}}$
  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{X\}$
  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y\}$
  $L_K \leftarrow L_K \cup \{(X, Y)\}$
  return X

Procedure $F^E(T)$
$S \leftarrow E(T, c_1)||\ldots||E(T, c_\ell)$
return S

Figure 7.1: The real game G_1. The lists L_K, $L_{K,\text{in}}$, and $L_{K,\text{out}}$ (for $K \in \{0,1\}^{n\ell}$) are set to be empty at the beginning of the game.

or E^{-1} (note that $1 \le i \le q_{\mathcal{A}} + \ell \cdot Q_{\mathcal{A}}$ holds since one invocation of F^E makes ℓ queries to E). Then, for each i,

$$\begin{aligned}
\Pr[\mathsf{SetBad}(i)] &= \Pr_{Y_1,\ldots,Y_\ell \xleftarrow{\$} \{0,1\}^n}\left[Y_j = Y_k \text{ for some } 1 \le j < k \le \ell\right] \\
&\le \sum_{1 \le j < k \le \ell} \Pr_{Y_j, Y_k \xleftarrow{\$} \{0,1\}^n}\left[Y_j = Y_k\right] \\
&= \sum_{1 \le j < k \le \ell} \sum_{W \in \{0,1\}^n} \Pr_{Y_j, Y_k \xleftarrow{\$} \{0,1\}^n}\left[Y_j = W \wedge Y_k = W\right] \\
&= \sum_{1 \le j < k \le \ell} \sum_{W \in \{0,1\}^n} \frac{1}{2^{2n}} \le \frac{\ell^2}{2^n}
\end{aligned}$$

holds. Therefore

$$\left|\Pr\left[1 \leftarrow G_2^{\mathcal{A}}\right] - \Pr\left[1 \leftarrow G_3^{\mathcal{A}}\right]\right| \le \Pr[\mathsf{flag} \leftarrow \mathsf{bad} \text{ in } G_2] \le \sum_{1 \le i \le q_{\mathcal{A}} + \ell Q_{\mathcal{A}}} \Pr[\mathsf{SetBad}(i)] \le \frac{\ell^2 (q_{\mathcal{A}} + \ell Q_{\mathcal{A}})}{2^n} \tag{7.3}$$

holds.

From (7.2) and (7.3),

$$\mathbf{Adv}^{\text{indiff}}_{(F^E,(E,E^{-1})),\mathsf{RO},\mathcal{S}}(\mathcal{A}) = \left|\Pr\left[1 \leftarrow G_1^{\mathcal{A}}\right] - \Pr\left[1 \leftarrow G_6^{\mathcal{A}}\right]\right| \le \sum_{1 \le i \le 5} \left|\Pr\left[1 \leftarrow G_i^{\mathcal{A}}\right] - \Pr\left[1 \leftarrow G_{i+1}^{\mathcal{A}}\right]\right| \le \frac{\ell^2 (q_{\mathcal{A}} + \ell Q_{\mathcal{A}})}{2^n}$$

Procedure $E(K, X)$
if L_K is empty
    $Y_1, \ldots, Y_\ell \xleftarrow{\$} \{0,1\}^n$
    if $Y_i = Y_j$ for some $i \neq j$
        flag $\leftarrow$ bad
    for $i = 1, \ldots, \ell$ **do:**
        $Y_i \xleftarrow{\$} \{0,1\}^n \setminus \{Y_1, \ldots, Y_{i-1}\}$
    $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{c_1, \ldots, c_\ell\}$
    $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y_1, \ldots, Y_\ell\}$
    $L_K \leftarrow L_K \cup \{(c_1, Y_1), \ldots, (c_\ell, Y_\ell)\}$
if there exists Y such that $(X, Y) \in L_K$
    return Y
else
    $Y \xleftarrow{\$} \{0,1\}^n \setminus L_{K,\text{out}}$
    $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{X\}$
    $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y\}$
    $L_K \leftarrow L_K \cup \{(X, Y)\}$
    return Y

Procedure $E^{-1}(K, Y)$
if L_K is empty
    $Y_1, \ldots, Y_\ell \xleftarrow{\$} \{0,1\}^n$
    if $Y_i = Y_j$ for some $i \neq j$
        flag $\leftarrow$ bad
    for $i = 1, \ldots, \ell$ **do:**
        $Y_i \xleftarrow{\$} \{0,1\}^n \setminus \{Y_1, \ldots, Y_{i-1}\}$
    $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{c_1, \ldots, c_\ell\}$
    $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y_1, \ldots, Y_\ell\}$
    $L_K \leftarrow L_K \cup \{(c_1, Y_1), \ldots, (c_\ell, Y_\ell)\}$
if there exists X such that $(X, Y) \in L_K$
    return X
else
    $X \xleftarrow{\$} \{0,1\}^n \setminus L_{K,\text{in}}$
    $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{X\}$
    $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y\}$
    $L_K \leftarrow L_K \cup \{(X, Y)\}$
    return X

Figure 7.2: The modified versions of $E(K, X)$ and $E^{-1}(K, Y)$ in the games G_2 and G_3. The steps surrounded by a square is performed in G_3 but not performed in G_2.

Procedure $\mathsf{RO}(T)$
if there exists W s.t. $(T, W) \in L_{\mathsf{RO}}$
  return W
else
  $W \xleftarrow{\$} \{0,1\}^{n\ell}$
  $L_{\mathsf{RO}} \leftarrow L_{\mathsf{RO}} \cup \{(T, W)\}$
  return W

Procedure $E(K, X)$
if L_K is empty
  $Y_1||\cdots||Y_\ell \leftarrow \mathsf{RO}(K)$ (here, $Y_i \in \{0,1\}^n$ for each i)
  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{c_1, \ldots, c_\ell\}$
  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y_1, \ldots, Y_\ell\}$
  $L_K \leftarrow L_K \cup \{(c_1, Y_1), \ldots, (c_\ell, Y_\ell)\}$
if there exists Y such that $(X, Y) \in L_K$
  return Y
else
  $Y \xleftarrow{\$} \{0,1\}^n \setminus L_{K,\text{out}}$
  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{X\}$
  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y\}$
  $L_K \leftarrow L_K \cup \{(X, Y)\}$
  return Y

Procedure $E^{-1}(K, Y)$
if L_K is empty
  $Y_1||\cdots||Y_\ell \leftarrow \mathsf{RO}(K)$ (here, $Y_i \in \{0,1\}^n$ for each i)
  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{c_1, \ldots, c_\ell\}$
  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y_1, \ldots, Y_\ell\}$
  $L_K \leftarrow L_K \cup \{(c_1, Y_1), \ldots, (c_\ell, Y_\ell)\}$
if there exists X such that $(X, Y) \in L_K$
  return X
else
  $X \xleftarrow{\$} \{0,1\}^n \setminus L_{K,\text{in}}$
  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{X\}$
  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y\}$
  $L_K \leftarrow L_K \cup \{(X, Y)\}$
  return X

Procedure $F^E(T)$
$S \leftarrow E(T, c_1)||\ldots||E(T, c_\ell)$
$\boxed{S \leftarrow \mathsf{RO}(T)}$
return S

Figure 7.3: The procedure RO and the modified versions of $E(K, X)$, $E^{-1}(K, Y)$, and F^E in the games G_4 and G_5. The list L_{RO} is set to be empty at the beginning of the game. The step surrounded by a square is included in G_5 but not included in G_4.

Game $G_6^{\mathcal{A}}$

$x \leftarrow \mathcal{A}^{\mathsf{RO},\mathcal{S}^{\mathsf{RO}}}$

return x

Procedure $\mathcal{S}(0, K, Z)$

if L_K is empty

  $Y_1 || \cdots || Y_\ell \leftarrow \mathsf{RO}(K)$ (here, $Y_i \in \{0,1\}^n$ for each i)

  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{c_1, \ldots, c_\ell\}$

  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y_1, \ldots, Y_\ell\}$

  $L_K \leftarrow L_K \cup \{(c_1, Y_1), \ldots, (c_\ell, Y_\ell)\}$

if there exists Y such that $(X, Y) \in L_K$

  return Y

else

  $Y \xleftarrow{\$} \{0,1\}^n \setminus L_{K,\text{out}}$

  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{X\}$

  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y\}$

  $L_K \leftarrow L_K \cup \{(X, Y)\}$

  return Y

Procedure $\mathcal{S}(1, K, Y)$

if L_K is empty

  $Y_1 || \cdots || Y_\ell \leftarrow \mathsf{RO}(K)$ (here, $Y_i \in \{0,1\}^n$ for each i)

  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{c_1, \ldots, c_\ell\}$

  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y_1, \ldots, Y_\ell\}$

  $L_K \leftarrow L_K \cup \{(c_1, Y_1), \ldots, (c_\ell, Y_\ell)\}$

if there exists X such that $(X, Y) \in L_K$

  return X

else

  $X \xleftarrow{\$} \{0,1\}^n \setminus L_{K,\text{in}}$

  $L_{K,\text{in}} \leftarrow L_{K,\text{in}} \cup \{X\}$

  $L_{K,\text{out}} \leftarrow L_{K,\text{out}} \cup \{Y\}$

  $L_K \leftarrow L_K \cup \{(X, Y)\}$

  return X

Figure 7.4: The ideal game G_6 and the simulator $\mathcal{S}$. The procedure RO is the same as that of G_4 and G_5. The procedures $\mathcal{S}(0, K, X)$ and $\mathcal{S}(1, K, X)$ are described separately so that the notations will be compatible with those in G_4 and G_5. $\mathcal{S}(0, \cdot, \cdot)$ simulates $E(\cdot, \cdot)$ and $\mathcal{S}(1, \cdot, \cdot)$ simulates $E^{-1}(\cdot, \cdot)$.

follows.

By definition of the simulator $\mathcal{S}$ (Fig. 7.4), at each invocation of $\mathcal{S}$, it makes at most one query to RO and returns an output in time $O(1)$. Therefore the claim of the theorem holds. □

Chapter 8

Conclusions

In this paper we studied post-quantum security of symmetric-key schemes from the perspective of both theory and practice. First, in Chapter 3 we overviewed the compressed oracle technique and provided an alternative formalization, which we heavily used to prove quantum security in other chapters.

On the theoretical side, this paper provided answers to two theoretically important, unresolved problems. One is whether the r-round Luby-Rackoff construction is a secure qPRP for some $r \geq 4$. The Luby-Rackoff construction is the most important scheme to convert PRFs to PRPs. Thus the problem of whether the r-round Luby-Rackoff construction is a secure qPRP for some r is theoretically significant. However, the problem has been unresolved since Kuwakado and Morii showed the 3-round quantum distinguisher [KM10]. In Chapter 4 we solved the problem affirmatively by proving that the 4-round Luby-Rackoff construction is a qPRP. We also showed that its tight quantum security bound is $\Theta(2^{n/6})$, where n is the input and output length of the Luby-Rackoff construction.

The other theoretical problem that we solved is whether we can make a quantum-secure tweakable block cipher from a quantum-secure block cipher. Since Kaplan et al. showed the efficient quantum attack on the LRW construction [KLLN16a], the problem has been unresolved. This problem is of theoretical interest because TBCs play important roles to build efficient symmetric-key schemes such as MACs and authenticated encryption schemes in the classical setting. In Chapter 5 we solved the problem by showing the new construction LRWQ is secure. Together with the results of Chapter 4, we can deduce that a quantum-secure TBC exists if a qPRF exists.

On the practical side, we showed the tight security bound of HMAC and NMAC in the quantum random oracle model. HMAC and NMAC are the most basic and important construction to convert Merkle-Damgård hash functions into PRFs. There already exists a previous work on quantum security of HMAC and NMAC [SY17] in the standard model, but it guarantees the security only up to $O(2^{n/5})$ or $O(2^{n/8})$ quantum queries in the QROM. In Chapter 6 we proved that $O(2^{n/3})$ is the tight quantum security bound of HMAC and NMAC in the QROM (for short messages). The gap between $O(2^{n/3})$ and $O(2^{n/5})$ (or $O(2^{n/8})$) is significant in practical use cases. This result shows that we can achieve a highly quantum-secure PRF and MAC from a hash function (or, a compression function of fixed input-output length) by using HMAC and NMAC.

As another practical result, we also provided a formal proof that the SKINNY-HASH internal function (the SHI function) is indifferentiable from a random oracle in Chapter 7. The SHI function is a function of fixed input-output length based on a tweakable block cipher, which is used in a function-based sponge hash called SKINNY-HASH [BJK+20]. The designers of the SKINNY-HASH claim that the SHI function is indifferentiable from a random oracle, but they do not provide formal security proofs. We proved that the SHI function is indeed provably secure as claimed by the designers, by showing a formal security proof. The result on the SHI function shows we can achieve an efficient and highly secure construction to build functions of fixed input-output length from tweakable block ciphers in practical use cases. Unlike other results, only a *classical* security proof is provided for the SHI function due to technical limitations. Nevertheless, we still think that the result has some implications in post-quantum cryptography. Though we do not have any post-quantum security proof of the SHI function, it is unlikely to be broken by quantum attacks. Hence we will be able to build post-quantum secure hash functions based on the SHI function. The SHI function is an important example of an internal function for function-based sponge hash because there does not exist many other instances. Thus it will also play an important role when we understand post-quantum security of function-based sponge hash functions. Moreover, when post-quantum security of the SHI function will be proved, the proof will be based on our classical proof. Therefore our result will help future studies on post-quantum security of hash functions.

Future Works

On the Luby-Rackoff construction, we showed security only against qCPAs but it is still unknown whether the r-round Luby-Rackoff construction becomes secure against qCCAs. Hence it is an interesting future work to prove the security against qCCAs for some $r \geq 5$. On quantum-secure TBCs, an interesting future work is to investigate how we can build a mode of operations to build TBCs that are secure against qCCAs, because our construction can be broken by a (classical) CCA. On HMAC and NMAC, our bound is tight for short messages but it does not seem tight for exponentially long messages. Thus it is worth investigating whether we can improve the security bound for long messages. On the SHI function, an important future work is definitely to prove indifferentiability in the quantum setting.

There is a common technical issue to tackle with the problems raised above, except for the one on HMAC and NMAC. The issue is how to treat the quantum oracles of ideally random permutations and ciphers that allow queries to *inverse oracles*. In the quantum setting, this paper focused on the situation where the quantum oracle of a permutation P or a cipher E allows adversaries to make queries to P and E but *not to* P^{-1} *nor* E^{-1}. The biggest reason of this is that, when the inverse oracles are available to adversaries, the compressed oracle technique cannot be applied[1] and proving quantum security becomes extremely difficult. To solve the above problems (except for HMAC and NMAC) in future works, new proof techniques will be required.

There still exist lots of important and interesting problems on post-quantum security in symmetric-key cryptography. It is important to keep studying them to contribute to the development of secure and efficient information and communications technology in the post-quantum era.

[1] At the time of writing this paper (July 2021), to the best of author's knowledge, there is no published work that successfully extend the compressed oracle technique to random permutations (and ideal ciphers) that allows inverse queries in such a way that it can be widely applied to prove quantum security of various cryptographic schemes (though, some preprint papers argue about such extensions [Cza21, Ros21]).

Bibliography

[AIK+00] Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, and Toshio Tokita. Camellia: A 128-bit block cipher suitable for multiple platforms - design and analysis. In Douglas R. Stinson and Stafford E. Tavares, editors, *Selected Areas in Cryptography, 7th Annual International Workshop, SAC 2000, Waterloo, Ontario, Canada, August 14-15, 2000, Proceedings*, volume 2012 of *Lecture Notes in Computer Science*, pages 39–56. Springer, 2000.

[Amb04] Andris Ambainis. Quantum walk algorithm for element distinctness. In *45th Symposium on Foundations of Computer Science (FOCS 2004), 17-19 October 2004, Rome, Italy, Proceedings*, pages 22–31. IEEE Computer Society, 2004.

[Amb07] Andris Ambainis. Quantum walk algorithm for element distinctness. *SIAM J. Comput.*, 37(1):210–239, 2007.

[AMRS20] Gorjan Alagic, Christian Majenz, Alexander Russell, and Fang Song. Quantum-access-secure message authentication via blind-unforgeability. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part III*, volume 12107 of *Lecture Notes in Computer Science*, pages 788–817. Springer, 2020.

[ANS17] ANSI. Retail Financial Services Symmetric Key Management Part 1: Using Symmetric Techniques. ANSI X9.24-1-2017, 2017.

[AR17] Gorjan Alagic and Alexander Russell. Quantum-secure symmetric-key cryptography based on hidden shifts. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *Advances in Cryptology - EUROCRYPT 2017 - 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Paris, France, April 30 - May 4, 2017, Proceedings, Part III*, volume 10212 of *Lecture Notes in Computer Science*, pages 65–93, 2017.

[ATTU16] Mayuresh Vivekanand Anand, Ehsan Ebrahimi Targhi, Gelo Noel Tabia, and Dominique Unruh. Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation. In Tsuyoshi Takagi, editor, *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, volume 9606 of *Lecture Notes in Computer Science*, pages 44–63. Springer, 2016.

[BCK96] Mihir Bellare, Ran Canetti, and Hugo Krawczyk. Keying hash functions for message authentication. In Neal Koblitz, editor, *Advances in Cryptology - CRYPTO '96, 16th Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 1996, Proceedings*, volume 1109 of *Lecture Notes in Computer Science*, pages 1–15. Springer, 1996.

[BDF+11] Dan Boneh, Özgür Dagdelen, Marc Fischlin, Anja Lehmann, Christian Schaffner, and Mark Zhandry. Random oracles in a quantum world. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011 - 17th International Conference on the Theory and Application of Cryptology and Information Security, Seoul, South Korea, December 4-8, 2011. Proceedings*, volume 7073 of *Lecture Notes in Computer Science*, pages 41–69. Springer, 2011.

[BDPA08] Guido Bertoni, Joan Daemen, Michaël Peeters, and Gilles Van Assche. On the indifferentiability of the sponge construction. In Nigel P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 181–197. Springer, 2008.

[BGIM19] Zhenzhen Bao, Jian Guo, Tetsu Iwata, and Kazuhiko Minematsu. ZOCB and ZOTR: tweakable blockcipher modes for authenticated encryption with full absorption. *IACR Trans. Symmetric Cryptol.*, 2019(2):1–54, 2019.

[BHT97] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. *SIGACT News*, 28(2):14–19, 1997.

[BHT98] Gilles Brassard, Peter Høyer, and Alain Tapp. Quantum cryptanalysis of hash and claw-free functions. In Claudio L. Lucchesi and Arnaldo V. Moura, editors, *LATIN '98: Theoretical Informatics, Third Latin American Symposium, Campinas, Brazil, April, 20-24, 1998, Proceedings*, volume 1380 of *Lecture Notes in Computer Science*, pages 163–169. Springer, 1998.

[BJK+16] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. The SKINNY family of block ciphers and its low-latency variant MANTIS. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 123–153. Springer, 2016.

[BJK+20] Christof Beierle, Jérémy Jean, Stefan Kölbl, Gregor Leander, Amir Moradi, Thomas Peyrin, Yu Sasaki, Pascal Sasdrich, and Siang Meng Sim. SKINNY-AEAD and SKINNY-Hash. *IACR Trans. Symmetric Cryptol.*, 2020(S1):88–131, 2020.

[BKR94] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of cipher block chaining. In Yvo Desmedt, editor, *Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings*, volume 839 of *Lecture Notes in Computer Science*, pages 341–358. Springer, 1994.

[BKR00] Mihir Bellare, Joe Kilian, and Phillip Rogaway. The security of the cipher block chaining message authentication code. *J. Comput. Syst. Sci.*, 61(3):362–399, 2000.

[BN18] Xavier Bonnetain and María Naya-Plasencia. Hidden shift quantum cryptanalysis and implications. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 560–592. Springer, 2018.

[BNS19] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. Quantum security analysis of AES. *IACR Trans. Symmetric Cryptol.*, 2019(2):55–93, 2019.

[BR00] John Black and Phillip Rogaway. CBC MACs for arbitrary-length messages: The three-key constructions. In Mihir Bellare, editor, *Advances in Cryptology - CRYPTO 2000, 20th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 2000, Proceedings*, volume 1880 of *Lecture Notes in Computer Science*, pages 197–215. Springer, 2000.

[BR02] John Black and Phillip Rogaway. A block-cipher mode of operation for parallelizable message authentication. In Lars R. Knudsen, editor, *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Cryptographic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings*, volume 2332 of *Lecture Notes in Computer Science*, pages 384–397. Springer, 2002.

[BR05] John Black and Phillip Rogaway. CBC macs for arbitrary-length messages: The three-key constructions. *J. Cryptol.*, 18(2):111–131, 2005.

[BR06] Mihir Bellare and Phillip Rogaway. The security of triple encryption and a framework for code-based game-playing proofs. In Serge Vaudenay, editor, *Advances in Cryptology - EUROCRYPT 2006, 25th Annual International Conference on the Theory and Applications of Cryptographic Techniques, St. Petersburg, Russia, May 28 - June 1, 2006, Proceedings*, volume 4004 of *Lecture Notes in Computer Science*, pages 409–426. Springer, 2006.

[BZ13] Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In Thomas Johansson and Phong Q. Nguyen, editors, *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, volume 7881 of *Lecture Notes in Computer Science*, pages 592–608. Springer, 2013.

[CBH+18] Jan Czajkowski, Leon Groot Bruinderink, Andreas Hülsing, Christian Schaffner, and Dominique Unruh. Post-quantum security of the sponge construction. In Tanja Lange and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 9th International Conference, PQCrypto 2018, Fort Lauderdale, FL, USA, April 9-11, 2018, Proceedings*, volume 10786 of *Lecture Notes in Computer Science*, pages 185–204. Springer, 2018.

[CDMP05] Jean-Sébastien Coron, Yevgeniy Dodis, Cécile Malinaud, and Prashant Puniya. Merkle-Damgård revisited: How to construct a hash function. In Victor Shoup, editor, *Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference, Santa Barbara, California, USA, August 14-18, 2005, Proceedings*, volume 3621 of *Lecture Notes in Computer Science*, pages 430–448. Springer, 2005.

[CHS19] Jan Czajkowski, Andreas Hülsing, and Christian Schaffner. Quantum indistinguishability of random sponges. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 296–325. Springer, 2019.

[CNL+08] Donghoon Chang, Mridul Nandi, Jesang Lee, Jaechul Sung, Seokhie Hong, Jongin Lim, Haeryong Park, and Kilsoo Chun. Compression function design principles supporting variable output lengths from a single small function. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 91-A(9):2607–2614, 2008.

[Cza21] Jan Czajkowski. Quantum indifferentiability of SHA-3. IACR Cryptology ePrint Archive, Report 2021/192, 2021.

[GLRS16] Markus Grassl, Brandon Langenberg, Martin Roetteler, and Rainer Steinwandt. Applying Grover's algorithm to AES: quantum resource estimates. In Tsuyoshi Takagi, editor, *Post-Quantum Cryptography - 7th International Workshop, PQCrypto 2016, Fukuoka, Japan, February 24-26, 2016, Proceedings*, volume 9606 of *Lecture Notes in Computer Science*, pages 29–43. Springer, 2016.

[GPR14] Peter Gazi, Krzysztof Pietrzak, and Michal Rybár. The exact PRF-security of NMAC and HMAC. In Juan A. Garay and Rosario Gennaro, editors, *Advances in Cryptology - CRYPTO 2014 - 34th Annual Cryptology Conference, Santa Barbara, CA, USA, August 17-21, 2014, Proceedings, Part I*, volume 8616 of *Lecture Notes in Computer Science*, pages 113–130. Springer, 2014.

[Gro96] Lov K. Grover. A fast quantum mechanical algorithm for database search. In Gary L. Miller, editor, *Proceedings of the Twenty-Eighth Annual ACM Symposium on the Theory of Computing, Philadelphia, Pennsylvania, USA, May 22-24, 1996*, pages 212–219. ACM, 1996.

[GYZ17] Sumegha Garg, Henry Yuen, and Mark Zhandry. New security notions and feasibility results for authentication of quantum data. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 342–371. Springer, 2017.

[HK14] Shoichi Hirose and Hidenori Kuwakado. A block-cipher-based hash function using an MMO-type double-block compression function. In Sherman S. M. Chow, Joseph K. Liu, Lucas Chi Kwong Hui, and Siu-Ming Yiu, editors, *Provable Security - 8th International Conference, ProvSec 2014, Hong Kong, China, October 9-10, 2014. Proceedings*, volume 8782 of *Lecture Notes in Computer Science*, pages 71–86. Springer, 2014.

[HS18] Akinori Hosoyamada and Yu Sasaki. Quantum Demiric-Selçuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions. In Dario Catalano and Roberto De Prisco, editors, *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, volume 11035 of *Lecture Notes in Computer Science*, pages 386–403. Springer, 2018.

[HY18] Akinori Hosoyamada and Kan Yasuda. Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 275–304. Springer, 2018.

[IHM+19] Gembu Ito, Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki, and Tetsu Iwata. Quantum chosen-ciphertext attacks against Feistel ciphers. In Mitsuru Matsui, editor, *Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings*, volume 11405 of *Lecture Notes in Computer Science*, pages 391–411. Springer, 2019.

[IK03] Tetsu Iwata and Kaoru Kurosawa. OMAC: one-key CBC MAC. In Thomas Johansson, editor, *Fast Software Encryption, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers*, volume 2887 of *Lecture Notes in Computer Science*, pages 129–153. Springer, 2003.

[IKMP20] Tetsu Iwata, Mustafa Khairallah, Kazuhiko Minematsu, and Thomas Peyrin. Duel of the titans: The Romulus and Remus families of lightweight AEAD algorithms. *IACR Trans. Symmetric Cryptol.*, 2020(1):43–120, 2020.

[IMPS17] Tetsu Iwata, Kazuhiko Minematsu, Thomas Peyrin, and Yannick Seurin. ZMAC: A fast tweakable block cipher mode for highly secure message authentication. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part III*, volume 10403 of *Lecture Notes in Computer Science*, pages 34–65. Springer, 2017.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. In Hovav Shacham and Alexandra Boldyreva, editors, *Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part III*, volume 10993 of *Lecture Notes in Computer Science*, pages 126–152. Springer, 2018.

[JNRV20] Samuel Jaques, Michael Naehrig, Martin Roetteler, and Fernando Virdia. Implementing Grover oracles for quantum key search on AES and LowMC. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 280–310. Springer, 2020.

[KLLN16a] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part II*, volume 9815 of *Lecture Notes in Computer Science*, pages 207–237. Springer, 2016.

[KLLN16b] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Trans. Symmetric Cryptol.*, 2016(1):71–94, 2016.

[KM10] Hidenori Kuwakado and Masakatu Morii. Quantum distinguisher between the 3-round Feistel cipher and the random permutation. In *IEEE International Symposium on Information Theory, ISIT 2010, June 13-18, 2010, Austin, Texas, USA, Proceedings*, pages 2682–2685. IEEE, 2010.

[KM12] Hidenori Kuwakado and Masakatu Morii. Security on the quantum-type Even-Mansour cipher. In *Proceedings of the International Symposium on Information Theory and its Applications, ISITA 2012, Honolulu, HI, USA, October 28-31, 2012*, pages 312–316. IEEE, 2012.

[LR85] Michael Luby and Charles Rackoff. How to construct pseudo-random permutations from pseudo-random functions (abstract). In Hugh C. Williams, editor, *Advances in Cryptology - CRYPTO '85, Santa Barbara, California, USA, August 18-22, 1985, Proceedings*, volume 218 of *Lecture Notes in Computer Science*, page 447. Springer, 1985.

[LRW02] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. In Moti Yung, editor, *Advances in Cryptology - CRYPTO 2002, 22nd Annual International Cryptology Conference, Santa Barbara, California, USA, August 18-22, 2002, Proceedings*, volume 2442 of *Lecture Notes in Computer Science*, pages 31–46. Springer, 2002.

[LRW11] Moses D. Liskov, Ronald L. Rivest, and David A. Wagner. Tweakable block ciphers. *J. Cryptol.*, 24(3):588–613, 2011.

[LS13] Rodolphe Lampe and Yannick Seurin. Tweakable blockciphers with asymptotically optimal security. In Shiho Moriai, editor, *Fast Software Encryption - 20th International Workshop, FSE 2013, Singapore, March 11-13, 2013. Revised Selected Papers*, volume 8424 of *Lecture Notes in Computer Science*, pages 133–151. Springer, 2013.

[LST12] Will Landecker, Thomas Shrimpton, and R. Seth Terashima. Tweakable blockciphers with beyond birthday-bound security. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 14–30. Springer, 2012.

[LZ19a] Qipeng Liu and Mark Zhandry. On finding quantum multi-collisions. In Yuval Ishai and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2019 - 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, May 19-23, 2019, Proceedings, Part III*, volume 11478 of *Lecture Notes in Computer Science*, pages 189–218. Springer, 2019.

[LZ19b] Qipeng Liu and Mark Zhandry. Revisiting post-quantum Fiat-Shamir. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 326–355. Springer, 2019.

[Min14] Kazuhiko Minematsu. Parallelizable rate-1 authenticated encryption from pseudorandom functions. In Phong Q. Nguyen and Elisabeth Oswald, editors, *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, volume 8441 of *Lecture Notes in Computer Science*, pages 275–292. Springer, 2014.

[MRH04] Ueli M. Maurer, Renato Renner, and Clemens Holenstein. Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology. In Moni Naor, editor, *Theory of Cryptography, First Theory of Cryptography Conference, TCC 2004, Cambridge, MA, USA, February 19-21, 2004, Proceedings*, volume 2951 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2004.

[MS17] Bart Mennink and Alan Szepieniec. XOR of PRPs in a quantum world. In Tanja Lange and Tsuyoshi Takagi, editors, *Post-Quantum Cryptography - 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings*, volume 10346 of *Lecture Notes in Computer Science*, pages 367–383. Springer, 2017.

[MV04] David A. McGrew and John Viega. The security and performance of the Galois/Counter Mode (GCM) of operation. In Anne Canteaut and Kapalee Viswanathan, editors, *Progress in Cryptology - INDOCRYPT 2004, 5th International Conference on Cryptology in India, Chennai, India, December 20-22, 2004, Proceedings*, volume 3348 of *Lecture Notes in Computer Science*, pages 343–355. Springer, 2004.

[Nai11] Yusuke Naito. Blockcipher-based double-length hash functions for pseudorandom oracles. In Ali Miri and Serge Vaudenay, editors, *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*, volume 7118 of *Lecture Notes in Computer Science*, pages 338–355. Springer, 2011.

[Nat77] National Bureau of Standards. Data encryption standard. 1977.

[Nat01] National Institute of Standards and Technology. Advanced encryption standard (AES). NIST FIPS PUB 197, 2001.

[Nat15a] National Institute of Standards and Technology. Secure Hash Standard (SHS). NIST FIPS PUB 180-4, 2015.

[Nat15b] National Institute of Standards and Technology. SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions. NIST FIPS PUB 202, 2015.

[Nat16] National Institute of Standards and Technology. Announcing request for nominations for public-key post-quantum cryptographic algorithms. 2016.

[Nat20] National Institute of Standards and Technology. Round 2 candidates of the lightweight cryptography standardization process, 2020. See https://csrc.nist.gov/projects/lightweight-cryptography/round-2-candidates.

[NC10] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[Pat91] Jacques Patarin. New results on pseudorandom permutation generators based on the DES scheme. In Joan Feigenbaum, editor, *Advances in Cryptology - CRYPTO '91, 11th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1991, Proceedings*, volume 576 of *Lecture Notes in Computer Science*, pages 301–312. Springer, 1991.

[Pat08] Jacques Patarin. The "Coefficients H" technique. In Roberto Maria Avanzi, Liam Keliher, and Francesco Sica, editors, *Selected Areas in Cryptography, 15th International Workshop, SAC 2008, Sackville, New Brunswick, Canada, August 14-15, Revised Selected Papers*, volume 5381 of *Lecture Notes in Computer Science*, pages 328–345. Springer, 2008.

[Rog04] Phillip Rogaway. Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In Pil Joong Lee, editor, *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, volume 3329 of *Lecture Notes in Computer Science*, pages 16–31. Springer, 2004.

[Ros21] Ansis Rosmanis. Tight bounds for inverting permutations via compressed oracle arguments. *CoRR*, abs/2103.08975, 2021.

[RSS11] Thomas Ristenpart, Hovav Shacham, and Thomas Shrimpton. Careful with composition: Limitations of the indifferentiability framework. In Kenneth G. Paterson, editor, *Advances in Cryptology - EUROCRYPT 2011 - 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tallinn, Estonia, May 15-19, 2011. Proceedings*, volume 6632 of *Lecture Notes in Computer Science*, pages 487–506. Springer, 2011.

[SF12] Ignacio Aguilar Sanchez and Daniel Fischer. Authenticated encryption in civilian space missions: context and requirements. DIAC - Directions in Authenticated Ciphers, 2012.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 124–134. IEEE Computer Society, 1994.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, 1997.

[Sim94] Daniel R. Simon. On the power of quantum computation. In *35th Annual Symposium on Foundations of Computer Science, Santa Fe, New Mexico, USA, 20-22 November 1994*, pages 116–123. IEEE Computer Society, 1994.

[Sim97] Daniel R. Simon. On the power of quantum computation. *SIAM J. Comput.*, 26(5):1474–1483, 1997.

[SXY18] Tsunekazu Saito, Keita Xagawa, and Takashi Yamakawa. Tightly-secure key-encapsulation mechanism in the quantum random oracle model. In Jesper Buus Nielsen and Vincent Rijmen, editors, *Advances in Cryptology - EUROCRYPT 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part III*, volume 10822 of *Lecture Notes in Computer Science*, pages 520–551. Springer, 2018.

[SY17] Fang Song and Aaram Yun. Quantum security of NMAC and related constructions - PRF domain extension against quantum attacks. In Jonathan Katz and Hovav Shacham, editors, *Advances in Cryptology - CRYPTO 2017 - 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 20-24, 2017, Proceedings, Part II*, volume 10402 of *Lecture Notes in Computer Science*, pages 283–309. Springer, 2017.

[WHF02] Doug Whiting, Russ Housley, and Niels Ferguson. Counter with CBC-MAC (CCM). Submission to NIST. Available at https://csrc.nist.gov/Projects/block-cipher-techniques/BCM, 2002.

[Zha12a] Mark Zhandry. How to construct quantum random functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 679–687. IEEE Computer Society, 2012.

[Zha12b] Mark Zhandry. Secure identity-based encryption in the quantum random oracle model. In Reihaneh Safavi-Naini and Ran Canetti, editors, *Advances in Cryptology - CRYPTO 2012 - 32nd Annual Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2012. Proceedings*, volume 7417 of *Lecture Notes in Computer Science*, pages 758–775. Springer, 2012.

[Zha15] Mark Zhandry. A note on the quantum collision and set equality problems. *Quantum Inf. Comput.*, 15(7&8):557–567, 2015.

[Zha16] Mark Zhandry. A note on quantum-secure PRPs. IACR Cryptology ePrint Archive, Report 2016/1076, 2016.

[Zha18] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. IACR Cryptology ePrint Archive, Report 2018/276, 2018. version 20180814:183812.

[Zha19] Mark Zhandry. How to record quantum queries, and applications to quantum indifferentiability. In Alexandra Boldyreva and Daniele Micciancio, editors, *Advances in Cryptology - CRYPTO 2019 - 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2019, Proceedings, Part II*, volume 11693 of *Lecture Notes in Computer Science*, pages 239–268. Springer, 2019.

Appendix A

Technical Terms, Abbreviations, and Notations

Term	Abbreviation / Notation	Explanation
-	$\{0,1\}^*$	The set of all the bit strings (including the empty string).
-	$(\{0,1\}^m)^+$	The set of all the bit strings of which length is a multiple of m (the empty string is not included).
-	$\|\| \cdot \|\|$	The Euclidean norm of vectors.
-	$\|\| \cdot \|\|_{\mathsf{tr}}$	The trace norm of matrices.
-	**Adv**	Advantage of adversaries for various security notions. See Section 2.6 for concrete definitions.
-	Func(X,Y)	The set of all functions from X to Y.
-	$GF(2^m)$	The Galois field of order 2^m.
-	H	The Hadamard transform.
-	I	The identity operator.
-	Perm(X)	The set of all permutations on X.
-	$\mathsf{td}(\cdot,\cdot)$	The trace distance function.
-	x_L	The left-half $n/2$ bit of the n-bit string $x \in \{0,1\}^n$.
-	x_R	The right-half $n/2$ bit of the n-bit string $x \in \{0,1\}^n$.
-	$x \oplus y$	(Bit-wise) XOR operation of bit strings x and y of the same length.
-	$x\|\|y$	Concatenation of the bit strings x and y.
Block cipher	BC	A keyed function $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ such that $E(K,\cdot)$ is a permutation on $\{0,1\}^n$ for each $K \in \{0,1\}^k$.
Chosen ciphertext attack	CCA	An attack on a cipher by making queries to the encryption and the decryption oracles.
Chosen plaintext attack	CPA	An attack on a cipher by making queries to the encryption oracle.
HMAC	HMAC	A construction to convert hash functions of the Merkle-Damgård construction into MACs as in (1.2).
Initialization vector	IV	A fixed constant to initialize the state of a scheme.
Keyed function	-	A function $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$.
Least significant m bits (of $x \in \{0,1\}^n$)	lsb[x]	The sub-string $x_{n-m+1} \cdots x_n$ of the bit string $x = x_1 \cdots x_n$, where $x_i \in \{0,1\}$ for all i.
LRW constructions	LRW2 / LRW1	The constructions to convert secure BCs into secure TBCs by Liskov, Rivest, and Wagner [LRW02, LRW11]. (See Fig. 5.1.)
LRWQ construction	LRWQ	Our new construction to convert quantum-secure BCs into quantum-secure TBCs. (See Fig. 5.2.)

Term	Abbreviation / Notation	Explanation
Merkle-Damgård construction	MD^h	A construction to convert a compression function h of fixed input-output length into a cryptographic hash function that supports variable length inputs, which is defined as in Section 1.4.1
Message authentication code	MAC	a symmetric cryptographic scheme that provides authenticity.
Most significant m bits (of $x \in \{0,1\}^n$)	msb$[x]$	The sub-string $x_1 \cdots x_m$ of the bit string $x = x_1 \cdots x_n$, where $x_i \in \{0,1\}$ for all i.
NMAC	NMAC	A two-key variant of HMAC defined as in (1.3).
Pseudorandom function	PRF	A keyed function that is (computationally) indistinguishable from a random function for classical adversaries (i.e., a secure keyed function).
Pseudorandom permutation	PRP	A keyed permutation that is (computationally) indistinguishable from a random permutation for classical adversaries that perform CPAs (i.e., a BC that is secure against CPAs).
Quantum chosen plaintext attack	qCCA	An attack on a cipher that makes quantum queries to the encryption and decryption oracles.
Quantum chosen plaintext attack	qCPA	An attack on a cipher that makes quantum queries to the encryption oracle.
Quantum-secure pseudorandom function	qPRF	A PRF that is secure against adversaries that makes quantum queries (i.e., a keyed function that is secure against quantum query attacks).
Quantum-secure pseudorandom permutation	qPRP	A PRP that is secure against adversaries that makes quantum queries (i.e., a BC that is secure against qCPAs).
Quantum-secure tweakable pseudorandom permutation	q$\widetilde{\mathsf{PRP}}$	A $\widetilde{\mathsf{PRP}}$ that is secure against adversaries that makes quantum queries (i.e., a TBC that is secure against qCPAs that query not only plaintexts but also tweaks to the encryption oracle).
Quantum random oracle	QRO	The quantum oracle of a public random function. (See Section 2.4.1 for the definition of the quantum oracle of a random function)
Quantum random oracle model	QROM	The ideal security proof model where a QRO exists.
Random oracle	RO	The oracle of a public random function
Recording standard oracle with errors	RstOE	The oracle defined in Definition 2
r-round Luby-Rackoff construction	LR_r	A construction to convert keyed functions into keyed permutations (block ciphers) defined as in (1.1).
SKINNY-HASH	-	The instantiation of the sponge construction designed by Bierle et al. [BJK+20].
SKINNY-HASH internal function	SHI	The internal function used in the SKINNY-HASH which is based on the TBC SKINNY, and its generalization that converts TBCs into functions of fixed input-output length. (See Fig. 1.6)
Sponge construction	-	A construction to convert a function F of fixed input-output length into a cryptographic hash function that supports variable length inputs. We call F an internal function. (See Fig. 1.5.)
Standard oracle	stO	The oracle defined as in (3.1).
Tweakable block cipher	TBC	A function $E : \{0,1\}^k \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ such that $E(\cdot, T, \cdot)$ is a block cipher for $T \in \{0,1\}^t$.

Term	Abbreviation / Notation	Explanation
Tweakable pseudorandom permutation	$\widetilde{\text{PRP}}$	A tweakable keyed permutation (i.e., a tweakable block cipher) that is (computationally) indistinguishable from a tweakable random permutation against classical adversaries that queries messages and tweaks to the oracle.

Appendix B

List of Publications

The contents of this paper are based on 4, 5, 13, 19, and 20 in the following list. The information of copyright and DOI of the orginal papers are as follows. DOI is indicated only for the papers that have already been published at the time of writing this paper (July 2021).

Journals

1. Akinori Hosoyamada and Kazumaro Aoki. On quantum related-key attacks on iterated Even-Mansour ciphers. *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 102-A(1):27–34, 2019.
2. Akinori Hosoyamada, Yu Sasaki, Seiichiro Tani, and Keita Xagawa. Quantum algorithm for the multicollision problem. *Theor. Comput. Sci.*, 842:100–117, 2020.
3. Akinori Hosoyamada, María Naya-Plasencia, and Yu Sasaki. Improved attacks on sliscp permutation and tight bound of limited birthday distinguishers. *IACR Trans. Symmetric Cryptol.*, 2020(4):147–172, 2020.
4. Akinori Hosoyamada and Tetsu Iwata. Provably quantum-secure tweakable block ciphers. *IACR Trans. Symmetric Cryptol.*, 2021(1):337–377, 2021.
5. Akinori Hosoyamada and Tetsu Iwata. Indifferentiability of SKINNY-HASH Internal Functions. Accepted to IEICE Trans. Fundam. Electron. Commun. Comput. Sci., 2021.

International Conferences

6. Akinori Hosoyamada and Kazumaro Aoki. On quantum related-key attacks on iterated Even-Mansour ciphers. In Satoshi Obana and Koji Chida, editors, *Advances in Information and Computer Security - 12th International Workshop on Security, IWSEC 2017, Hiroshima, Japan, August 30 - September 1, 2017, Proceedings*, volume 10418 of *Lecture Notes in Computer Science*, pages 3–18. Springer, 2017.
7. Akinori Hosoyamada, Yu Sasaki, and Keita Xagawa. Quantum multicollision-finding algorithm. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part II*, volume 10625 of *Lecture Notes in Computer Science*, pages 179–210. Springer, 2017.

8. Akinori Hosoyamada and Yu Sasaki. Cryptanalysis against symmetric-key schemes with online classical queries and offline quantum computations. In Nigel P. Smart, editor, *Topics in Cryptology - CT-RSA 2018 - The Cryptographers' Track at the RSA Conference 2018, San Francisco, CA, USA, April 16-20, 2018, Proceedings*, volume 10808 of *Lecture Notes in Computer Science*, pages 198–218. Springer, 2018.

9. Akinori Hosoyamada and Yu Sasaki. Quantum Demiric-Selçuk meet-in-the-middle attacks: Applications to 6-round generic Feistel constructions. In Dario Catalano and Roberto De Prisco, editors, *Security and Cryptography for Networks - 11th International Conference, SCN 2018, Amalfi, Italy, September 5-7, 2018, Proceedings*, volume 11035 of *Lecture Notes in Computer Science*, pages 386–403. Springer, 2018.

10. Akinori Hosoyamada and Kan Yasuda. Building quantum-one-way functions from block ciphers: Davies-Meyer and Merkle-Damgård constructions. In Thomas Peyrin and Steven D. Galbraith, editors, *Advances in Cryptology - ASIACRYPT 2018 - 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2-6, 2018, Proceedings, Part I*, volume 11272 of *Lecture Notes in Computer Science*, pages 275–304. Springer, 2018.

11. Gembu Ito, Akinori Hosoyamada, Ryutaroh Matsumoto, Yu Sasaki, and Tetsu Iwata. Quantum chosen-ciphertext attacks against Feistel ciphers. In Mitsuru Matsui, editor, *Topics in Cryptology - CT-RSA 2019 - The Cryptographers' Track at the RSA Conference 2019, San Francisco, CA, USA, March 4-8, 2019, Proceedings*, volume 11405 of *Lecture Notes in Computer Science*, pages 391–411. Springer, 2019.

12. Akinori Hosoyamada, Yu Sasaki, Seiichiro Tani, and Keita Xagawa. Improved quantum multicollision-finding algorithm. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography - 10th International Conference, PQCrypto 2019, Chongqing, China, May 8-10, 2019 Revised Selected Papers*, volume 11505 of *Lecture Notes in Computer Science*, pages 350–367. Springer, 2019.

13. Akinori Hosoyamada and Tetsu Iwata. 4-round Luby-Rackoff construction is a qPRP. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 145–174. Springer, 2019.

14. Xavier Bonnetain, Akinori Hosoyamada, María Naya-Plasencia, Yu Sasaki, and André Schrottenloher. Quantum attacks without superposition queries: The offline Simon's algorithm. In Steven D. Galbraith and Shiho Moriai, editors, *Advances in Cryptology - ASIACRYPT 2019 - 25th International Conference on the Theory and Application of Cryptology and Information Security, Kobe, Japan, December 8-12, 2019, Proceedings, Part I*, volume 11921 of *Lecture Notes in Computer Science*, pages 552–583. Springer, 2019.

15. Akinori Hosoyamada and Yu Sasaki. Finding hash collisions with quantum computers by using differential trails with smaller probability than birthday bound. In Anne Canteaut and Yuval Ishai, editors, *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*, volume 12106 of *Lecture Notes in Computer Science*, pages 249–279. Springer, 2020.

16. Akinori Hosoyamada and Takashi Yamakawa. Finding collisions in a quantum world: Quantum black-box separation of collision-resistance and one-wayness. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part I*, volume 12491 of *Lecture Notes in Computer Science*, pages 3–32. Springer, 2020.

17. Carlos Cid, Akinori Hosoyamada, Yunwen Liu, and Siang Meng Sim. Quantum cryptanalysis on contracting Feistel structures and observation on related-key settings. In Karthikeyan Bhargavan, Elisabeth Oswald, and Manoj Prabhakaran, editors, *Progress in Cryptology - INDOCRYPT 2020 - 21st International Conference on Cryptology in India, Bangalore, India, December 13-16, 2020, Proceedings*, volume 12578 of *Lecture Notes in Computer Science*, pages 373–394. Springer, 2020.

18. Akinori Hosoyamada and Yu Sasaki. Quantum collision attacks on reduced SHA-256 and SHA-512. To appear at CRYPTO 2021.

19. Akinori Hosoyamada and Tetsu Iwata. On tight quantum security of HMAC and NMAC in the quantum random oracle model. To appear at CRYPTO 2021.

Preprints

20. Akinori Hosoyamada and Tetsu Iwata. 4-round Luby-Rackoff construction is a qRPP: Tight quantum security bound. IACR Cryptology ePrint Archive, Report 2019/243, versions 20200625:112823 and later, 2020.