Secure uniform random-number extraction via incoherent strategies

Masahito Hayashi[1,2,*] and Huangjun Zhu[3,†]
[1] *Graduate School of Mathematics, Nagoya University, Nagoya 464-8602, Japan*
[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, 117542 Singapore*
[3] *Institute for Theoretical Physics, University of Cologne, Cologne 50937, Germany*

(Received 22 July 2017; published 4 January 2018)

To guarantee the security of uniform random numbers generated by a quantum random-number generator, we study secure extraction of uniform random numbers when the environment of a given quantum state is controlled by the third party, the eavesdropper. Here we restrict our operations to incoherent strategies that are composed of the measurement on the computational basis and incoherent operations (or incoherence-preserving operations). We show that the maximum secure extraction rate is equal to the relative entropy of coherence. By contrast, the coherence of formation gives the extraction rate when a certain constraint is imposed on the eavesdropper's operations. The condition under which the two extraction rates coincide is then determined. Furthermore, we find that the exponential decreasing rate of the leaked information is characterized by Rényi relative entropies of coherence. These results clarify the power of incoherent strategies in random-number generation, and can be applied to guarantee the quality of random numbers generated by a quantum random-number generator.

DOI: 10.1103/PhysRevA.97.012302

I. INTRODUCTION

Recently, quantum random-number generation has attracted much attention because of many practical applications, such as cryptography, scientific simulation, and foundational studies [1,2]. A quantum random-number generator is a device for extracting secure uniform random numbers from quantum states. Its experimental demonstration has been done with quantum optics [3–6]. Ideally, the random numbers generated should be independent of the third party, the eavesdropper (Eve). In practice, however, the relevant states or random numbers are often correlated to Eve. For this reason, it is crucial to extract secure uniform random numbers from random numbers the side information of which is leaked to Eve. This task is called secure uniform random-number extraction, which has been studied in the framework of information security, and has been considered as a basic tool for quantum key distribution [7–9]. Here the goal of the legitimate user, Alice, is to generate random numbers that are almost independent of Eve. Usually, the initial state is taken to be a classical-quantum (C-Q) state ρ_{AE}, in which, Alice's information is given as a classical random number, while Eve's information is given as a quantum state that is correlated to Alice's random variable. When the n-tensor product state $\rho_{AE}^{\otimes n}$ is given, it is known that the asymptotic secure extraction rate is equal to the conditional entropy $H(A|E)_{\rho_{AE}} := S(\rho_{AE}) - S(\rho_E)$.

To guarantee the quality of the uniform random numbers generated in a quantum uniform random-number generator, it is usually assumed that the environment of Alice's system is controlled by Eve. This convention covers the most powerful Eve and is typical in similar research areas. For example, in the study of quantum key distribution [8,10,11] and private capacity [12], all of the environment is assumed to be under Eve's control. Further, since Alice generates the quantum state on her system, which is under her control, it is natural to treat Alice's initial information as a quantum state in the same way as Eve's state. In fact, there are several formulations of secure uniform random-number extraction with quantum-quantum states (see [13, Sec. 4.3] and [14–16]). However, little is known about the optimal extraction rate. This is because it is not easy to clarify the reasonable range of allowed operations.

To extract random numbers from a quantum state, Alice can apply a projective measurement. However, not all quantum states can produce secure random numbers in this way given that the environment is controlled by Eve. Quantum coherence with respect to the measurement basis is crucial to realizing the independence from the environment and the randomness of the outcome simultaneously [1,2]. In addition, in many practical scenarios, it is not easy to create or increase coherence in quantum systems [17,18]. Understanding the limit of random-number generation in such practical scenarios is thus of paramount interest not only to theoretical study but also to real applications. Although coherence is indispensable in many applications, such as laser and quantum metrology, the resource theory of coherence was not established until recently [18–23]. Under this framework, Yuan *et al.* [24,25] showed that the amount of randomness upon measurement on the computational basis is closely related to several important coherence measures, such as the relative entropy of coherence and coherence of formation. However, the extraction of uniform random numbers under general incoherent operations has not been discussed. The relation between our paper and [24,25] is explained in more detail in Appendix I.

Motivated by the problem mentioned above, in this paper we study the secure extraction of uniform random numbers under incoherent strategies, which include the measurement

*masahito@math.nagoya-u.ac.jp
†hzhu1@uni-koeln.de

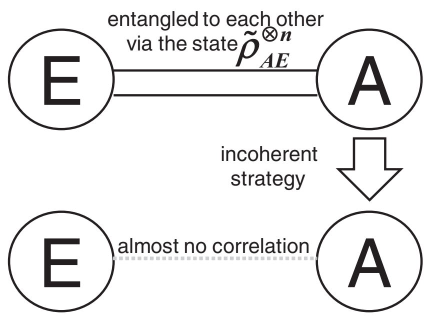

FIG. 1. Extraction of secure uniform random numbers via incoherent strategy.

on the computational basis and general incoherent operations (or incoherence-preserving operations) [18–21]. To guarantee the security of the random numbers generated, we assume that the environment of the relevant quantum state is controlled by Eve, and there is no restriction on Eve's operations on the environment; see Fig. 1. We show that the maximum secure extraction rate is equal to the relative entropy of coherence. In addition, the maximum rate can be achieved by performing the measurement on the computational basis (without other incoherent operations) followed by classical data processing. By contrast, the extraction rate coincides with the coherence of formation if Eve's operations are constrained in a special way. The condition under which the extraction rates in the two scenarios coincide has a simple description. Furthermore, we show that the exponential decreasing rate of the leaked information is characterized by Rényi relative entropies of coherence. These results not only clarify the power of incoherent strategies in extracting random numbers but also endow operational meanings to a number of important coherence measures.

II. RESOURCE THEORY OF COHERENCE

The resource theory of coherence is characterized by the set of incoherent states, denoted by $\mathcal{I}$, and the set of incoherent operations [18–21]. Recall that a state is incoherent if it is diagonal with respect to the reference computational basis. A quantum operation, represented by a completely positive trace-preserving (CPTP) map, is incoherence preserving (also called maximally incoherent) if it maps incoherent states to incoherent states [19]. It is incoherent if, in addition, each Kraus operator in its Kraus representation maps incoherent states to incoherent states up to normalization [20]. An incoherent operation is physically incoherent if it admits an incoherent Stinespring dilation [22]. For unitary transformations, the three types of operations coincide. A unitary operator is incoherent if and only if (iff) each row and each column has only one nonzero entry.

The relative entropy of coherence $C_{\mathrm{r}}(\rho)$ of a quantum state ρ is the minimum relative entropy between the state and incoherent states [19,20]:

$$C_{\mathrm{r}}(\rho) := \min_{\sigma\in\mathcal{I}} S(\rho\|\sigma) = S(\rho^{\mathrm{diag}}) - S(\rho), \tag{1}$$

where $S(\rho\|\sigma) := \operatorname{tr}\rho(\ln\rho - \ln\sigma)$ is the relative entropy between ρ and σ, $S(\rho)$ is the von Neumann entropy of ρ, and ρ^{diag} is the diagonal part of ρ. In this paper "log" has base 2. The coherence of formation $C_{\mathrm{F}}(\rho)$ is the convex roof of $C_{\mathrm{r}}(\rho)$ [19,24]:

$$C_{\mathrm{F}}(\rho) := \min_{\{p_j,|\psi_j\rangle\}} \sum_j p_j C_{\mathrm{r}}(|\psi_j\rangle\langle|\psi_j|), \tag{2}$$

where $\{p_j,|\psi_j\rangle\}$ satisfies $\rho=\sum_j p_j|\psi_j\rangle\langle\psi_j|$. It is known that the relative entropy of coherence $C_{\mathrm{r}}(\rho)$ is equal to the distillable coherence, and the coherence of formation $C_{\mathrm{F}}(\rho)$ is equal to the coherence cost [21].

III. FORMULATION WITH UNLIMITED EVE

In practice, Alice repeatedly generates many copies of identical and independent quantum states. This assumption allows us to write the state of the whole system as a tensor product, so our problem can be formulated as follows. Suppose Alice holds n copies of the quantum state $\tilde{\rho}_A$ on system $\mathcal{H}_A$ the environment of which is controlled by Eve. Here, Eve is assumed to have unlimited power in her system. All the information of Eve about Alice's systems is encoded in a purification, say $\tilde{\rho}^{\otimes n}$, of $\tilde{\rho}_A^{\otimes n}$. Alice is allowed to perform only incoherent strategies, which can be divided into three steps without loss of generality. First, she applies an incoherent unitary operation $U_{\mathrm{i},n}$ on the system and an ancilla system $\mathcal{H}_B$, the initial state of which is $|0\rangle$. Second, she performs the measurement $\mathsf{M}_{\mathrm{c},n}$ on the computational basis, the set of outcomes of which is denoted by $\mathcal{A}^n$. Finally, as postmeasurement processing, she applies a random hash function F_n from $\mathcal{A}^n$ to a suitable set $\mathcal{L}_n$. The cardinality (number of elements) of $\mathcal{L}_n$ is denoted by $|\mathcal{L}_n|$, which also expresses the dimension of the output system. In this paper, a random variable is denoted by an italic capital letter, and its probability space is denoted by the same letter in mathcal font. The incoherent strategy of Alice is characterized by the triple $(U_{\mathrm{i},n},\mathsf{M}_{\mathrm{c},n},F_n)$ and is denoted by M_{F_n} for simplicity. The cardinality $|\mathcal{L}_n|$ is also denoted by $|\mathsf{M}_{F_n}|$.

To determine the maximum extraction rate of secure uniform random numbers, we need a security measure. When the whole system is characterized by a C-Q state ρ_{AE}, a widely accepted measure on secure random numbers is the trace distance (also known as the Schatten 1-norm) between the real state and the ideal state:

$$d_1(\rho_{AE}) := \|\rho_{AE} - \tau_{|\mathcal{A}|}\otimes\rho_E\|_1, \tag{3}$$

where τ_V is the completely mixed state on the V-dimensional system. So, $\tau_{|\mathcal{A}|}$ expresses the completely mixed state on $\mathcal{H}_A$. The significance of this measure lies in the fact that it is universally composable [7,9].

Here, considering the expectation $\mathbb{E}_{F_n}$ with respect to the choice of the random hash function, we employ the security measure of concern $d_1(\mathsf{M}_{F_n}|F_n) := \mathbb{E}_{F_n} d_1[\mathsf{M}_{F_n}(\tilde{\rho}^{\otimes n})]$, where $\mathsf{M}_{F_n}\otimes\iota_E$ is abbreviated to M_{F_n} and ι_E is the identity operation on E. The maximum asymptotic extraction rate of secure uniform random numbers $R(\tilde{\rho}_A)$ from the n-tensor product $\tilde{\rho}_A^{\otimes n}$ is defined as

$$R(\tilde{\rho}_A) := \max_{\{\mathsf{M}_{F_n}\}}\left\{\liminf_{n\to\infty}\frac{\ln|\mathsf{M}_{F_n}|}{n}\,\middle|\, d_1(\mathsf{M}_{F_n}|F_n)\to 0\right\}, \tag{4}$$

where the maximum is taken over sequences of incoherent strategies M_{F_n} which satisfy the given condition.

IV. RELATION WITH RESOURCE THEORY OF COHERENCE

To compute the rate $R(\tilde{\rho}_A)$, we need to study the uncertainty of Alice's system from Eve's viewpoint when the initial state on $\mathcal{H}_A \otimes \mathcal{H}_E$ is a pure state. This uncertainty can be measured by the conditional entropy $H(A|E)_{\tilde{\rho}} = S(\tilde{\rho}) - S(\tilde{\rho}_E)$. To maximize Eve's uncertainty, Alice can introduce an ancilla system $\mathcal{H}_B$ prepared in the incoherent state $|0\rangle\langle 0|$, so that the initial state is $\tilde{\rho} \otimes |0\rangle\langle 0|$. Then she applies an incoherent unitary $U_{\rm i}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$, which leads to the output state $\tilde{\rho}[U_{\rm i}] := U_{\rm i}(\tilde{\rho} \otimes |0\rangle\langle 0|)U_{\rm i}^{\dagger}$. When $d_B := \dim(\mathcal{H}_B) \geqslant d_A := \dim(\mathcal{H}_A)$, a particularly interesting incoherent unitary is the generalized controlled-NOT (CNOT) gate defined as

$$U_{\rm CNOT} := \sum_{x;\, y<d_A} |x,x+y\rangle\langle x,y| + \sum_{x;\, y\geqslant d_A} |x,y\rangle\langle x,y|, \quad (5)$$

where the addition $x+y$ is modulo d_A.

Theorem 1.

$$\frac{1}{n}\max_{U_{\rm i}} H(A|E)_{\tilde{\rho}^{\otimes n}[U_{\rm i}]} = \max_{U_{\rm i}} H(A|E)_{\tilde{\rho}[U_{\rm i}]} = H(A|E)_{\tilde{\rho}[U_{\rm CNOT}]} = C_{\rm r}(\tilde{\rho}_A), \quad (6)$$

where $U_{\rm i}$ is an incoherent unitary.

Proof. Let $U_{\rm i}$ be any incoherent unitary. Then

$$H(A|E)_{\tilde{\rho}[U_{\rm i}]} = -H(A|B)_{\tilde{\rho}[U_{\rm i}]} \leqslant E_{\rm r}(\tilde{\rho}[U_{\rm i}]_{AB}) \leqslant C_{\rm r}(\tilde{\rho}[U_{\rm i}]_{AB}) \leqslant C_{\rm r}(\tilde{\rho}_A), \quad (7)$$

where $E_{\rm r}(\rho) := \min_{\sigma\in\mathcal{S}} S(\rho\|\sigma)$ denotes the relative entropy of entanglement, with $\mathcal{S}$ being the set of separable states. Here the equality follows from the duality relation $H(A|E)_\rho + H(A|B)_\rho = 0$, which holds whenever ρ is pure; the first inequality follows from [26] and [27, Lemma 4], the second inequality follows from the fact that incoherent states for a bipartite system are separable, and the third inequality follows from the fact that the relative entropy of coherence is monotonic under incoherence-preserving operations.

According to the duality relation and [28] and [27, Theorem 1], $H(A|E)_{\tilde{\rho}[U_{\rm CNOT}]} = -H(A|B)_{\tilde{\rho}[U_{\rm CNOT}]} = C_{\rm r}(\tilde{\rho}_A)$, note that $\tilde{\rho}[U_{\rm CNOT}]_{AB}$ is a maximally correlated state [29–31]. Therefore, $\max_{U_{\rm i}} H(A|E)_{\tilde{\rho}[U_{\rm i}]} = C_{\rm r}(\tilde{\rho}_A)$. Now the proof of (6) is completed by the additivity relation $C_{\rm r}(\tilde{\rho}_A^{\otimes n}) = nC_{\rm r}(\tilde{\rho}_A)$ [21,27].

Theorem 1 is helpful for computing the extraction rate $R(\tilde{\rho}_A)$ as follows. If Alice performs the measurement $\mathsf{M}_{\rm c}$ in the computational basis, then $\tilde{\rho}$ is turned into the state $\mathsf{M}_{\rm c}(\tilde{\rho}) := \sum_x |x\rangle\langle x| \otimes \langle x|\tilde{\rho}|x\rangle$, which satisfies

$$H(A|E)_{\mathsf{M}_{\rm c}(\tilde{\rho})} = H(A|E)_{\tilde{\rho}[U_{\rm CNOT}]} = C_{\rm r}(\tilde{\rho}_A). \quad (8)$$

After repeating this procedure and generating the state $\mathsf{M}_{\rm c}(\tilde{\rho})^{\otimes n}$, Alice applies a random hash function F_n to the n measurement outcomes with the extraction rate of uniform random numbers chosen to be R. Here the random hash function F_n is assumed to satisfy the *universal 2 condition* as discussed in Appendix A [32,33], which is conventional in generating secure random numbers from random numbers that might be partially leaked to the eavesdropper. An efficient construction of such hash functions was discussed in [34]. In the independent and identical situation, Proposition 3 in Appendix A shows that the extracted random numbers are secure when the extraction rate R is smaller than the conditional entropy $H(A|E)_{\mathsf{M}_{\rm c}(\tilde{\rho})}$. Therefore, we have $R(\tilde{\rho}_A) \geqslant H(A|E)_{\mathsf{M}_{\rm c}(\tilde{\rho})}$. Since Alice can optimize the incoherent unitary before the measurement $\mathsf{M}_{\rm c}$, it follows that

$$R(\tilde{\rho}_A) \geqslant \max_{U_{\rm i}} H(A|E)_{\tilde{\rho}[U_{\rm i}]}. \quad (9)$$

Conversely, as shown in Appendix B, the opposite inequality

$$R(\tilde{\rho}_A) \leqslant \liminf_{n\to\infty} \frac{1}{n}\max_{U_{\rm i}} H(A|E)_{\tilde{\rho}^{\otimes n}[U_{\rm i}]} \quad (10)$$

holds. Combining (6) of Theorem 1 with (9) and (10), we obtain the following theorem.

Theorem 2. The extraction rate $R(\tilde{\rho}_A)$ is given by

$$R(\tilde{\rho}_A) = \max_{U_{\rm i}} H(A|E)_{\tilde{\rho}[U_{\rm i}]} = C_{\rm r}(\tilde{\rho}_A), \quad (11)$$

where $U_{\rm i}$ is an incoherent unitary.

According to (8)–(10), the maximum extraction rate $C_{\rm r}(\tilde{\rho}_A)$ stated in Theorem 2 can be achieved by the measurement $\mathsf{M}_{\rm c}$ on the computational basis (without other incoherent operations) followed by classical data processing characterized by F_n. This strategy is denoted by $\mathsf{M}^*_{F_n}$ henceforth.

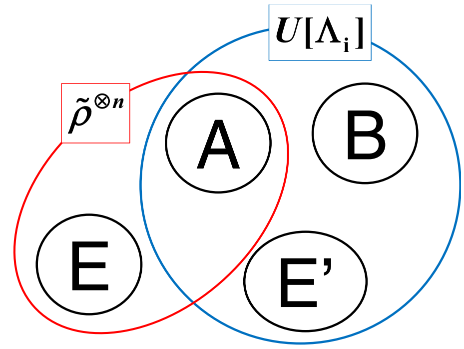

FIG. 2. Extended strategy. Alice can apply a general incoherent (or incoherence-preserving) operation $\Lambda_{\rm i}$. Both $\mathcal{H}_E$ and $\mathcal{H}_{E'}$ are in Eve's hands.

V. EXTENSION TO GENERAL INCOHERENCE-PRESERVING CPTP MAPS

Now, we extend Alice's incoherent unitaries to general incoherence-preserving CPTP maps acting on the system $\mathcal{H}_A \otimes \mathcal{H}_B$ as Fig. 2. If she uses a CPTP map the final state of which is always the specific incoherent state $\sum_{i=0}^{d-1} \frac{1}{d}|i\rangle\langle i|$, the resulting conditional entropy equals $\ln d$, which increases unlimitedly as d increases. To avoid such a trivial advantage for Alice, similar to the study of quantum key distribution [8,10,11] and private capacity [12], we assume that the environment $\mathcal{H}_{E'}$ of the incoherence-preserving CPTP map $\Lambda_{\rm i}$ is also controlled by Eve, so that Eve has the two systems $\mathcal{H}_E$ and $\mathcal{H}_{E'}$ in total. This is because it is not easy to exclude the possibility that Eve accesses a system that interacts with Alice's operation.

To cover such a worst scenario, we take this convention and consider the Stinespring representation $\rho_{E'}[\Lambda_{\rm i}], U[\Lambda_{\rm i}]$ of $\Lambda_{\rm i}$, where $\rho_{E'}[\Lambda_{\rm i}]$ is the initial pure state on the environment and $U[\Lambda_{\rm i}]$ is the unitary on the whole system. Note that $U[\Lambda_{\rm i}]$ may not be incoherent if $\Lambda_{\rm i}$ is not physically incoherent [22], but this fact does not affect the following argument. Now the total output state is $\tilde{\rho}[\Lambda_{\rm i}] := U[\Lambda_{\rm i}](\tilde{\rho}\otimes|0\rangle\langle 0|\otimes\rho_{E'}[\Lambda_{\rm i}])U[\Lambda_{\rm i}]^\dagger$. Since $\tilde{\rho}[\Lambda_{\rm i}]$ is a pure state, we can still use the duality relation on conditional entropies. So, similar to (7), we have

$$H(A|E)_{\tilde{\rho}[\Lambda_{\rm i}]} \leqslant E_{\rm r}(\tilde{\rho}[\Lambda_{\rm i}]_{AB}) \leqslant C_{\rm r}(\tilde{\rho}_A). \quad (12)$$

Again, the two inequalities are saturated when $\Lambda_{\rm i}$ is the generalized CNOT gate. Therefore, Theorems 1 and 2 still hold if incoherent unitaries are replaced by general incoherence-preserving operations.

Here, we need to discuss the relation with the distillable coherence $C_{\rm D}(\tilde{\rho}_A)$ under incoherent operations, which is equal to $C_{\rm r}(\tilde{\rho}_A)$ [21]. Note that coherence distillation may require incoherent operations across many copies, and these operations may not be physically incoherent. By contrast, to implement our optimal protocol, it suffices to perform the measurement $\mathsf{M}_{\rm c}$ followed by classical data processing, i.e., application of universal 2 hash functions, which is much easier.

VI. EXTENSION TO LIMITED EVE

Now, we remember that the criterion d_1 universally covers the distinguishability by Eve's local measurement M_E. Since the criterion d_1 is universally composable, the above discussion covers the case in which Eve chooses any local measurement M_E according to the choice of the hash function f_n. Now, we consider the scenario with Eve having limited power in her system. That is, it is natural from a practical viewpoint to assume that Eve cannot choose her local measurement M_E according to the random choice of the hash function F_n, although she knows which hash function F_n is applied after her measurement M_E. Here f_n denotes a specific hash function, while F_n denotes a random hash function. Given the n tensor product state $\tilde{\rho}^{\otimes n}$, we introduce a new security criterion $\underline{d}_1(\mathsf{M}_{F_n}|F_n)$ as

$$\underline{d}_1(\mathsf{M}_{F_n}|F_n) := \max_{\mathsf{M}_E} \mathbb{E}_{F_n} d_1\big(\mathsf{M}_{F_n}(\mathsf{M}_E(\tilde{\rho})^{\otimes n})\big) \\ = \max_{\mathsf{M}_E} \mathbb{E}_{F_n} d_1(\mathsf{M}_{F_n}(\mathsf{M}_E^{\otimes n}(\tilde{\rho}^{\otimes n}))) \leqslant d_1(\mathsf{M}_{F_n}|F_n), \quad (13)$$

where M_E is Eve's positive operator-valued measure (POVM) on the system $\mathcal{H}_E$. Remember that $\mathsf{M}_{F_n}\otimes\iota_E$ and $\iota_A\otimes\mathsf{M}_E$ are abbreviated to M_{F_n} and M_E, respectively. Then, instead of $R(\tilde{\rho}_A)$, we define

$$\overline{R}(\tilde{\rho}_A) := \max_{\{\mathsf{M}_{F_n}\}} \left\{ \liminf_{n\to\infty} \frac{\ln|\mathsf{M}_{F_n}|}{n} \middle| \underline{d}_1(\mathsf{M}_{F_n}|F_n) \to 0 \right\}, \quad (14)$$

where the maximum is taken over sequences of incoherent strategies M_{F_n} which satisfy the given condition. The relation (13) implies the inequality $\overline{R}(\tilde{\rho}_A) \geqslant R(\tilde{\rho}_A)$. Instead of Theorem 2, we have the following theorem, which is proved in Appendix B.

Theorem 3.

$$\overline{R}(\tilde{\rho}_A) = C_{\rm F}(\tilde{\rho}_A). \quad (15)$$

This theorem offers an operational meaning of the coherence of formation $C_{\rm F}(\tilde{\rho}_A)$. Since the relation $C_{\rm F}(\tilde{\rho}_A) \geqslant C_{\rm r}(\tilde{\rho}_A)$ holds in general and the inequality is generically strict, Theorems 2 and 3 show that Alice can usually extract secure uniform random numbers with a higher rate if Eve chooses her measurement independently of the incoherent strategies of Alice. In conjunction with Theorem 10 in [21], we can deduce the condition under which the rates in the two scenarios coincide.

Theorem 4. The inequality $\overline{R}(\tilde{\rho}_A) \geqslant R(\tilde{\rho}_A)$ is saturated iff $\tilde{\rho}_A$ is pure or its eigenvectors are supported on orthogonal subspaces spanned by a partition of basis states in the reference basis.

The following corollary is an easy consequence of Theorem 4; a direct proof is presented in Appendix G.

Corollary 1. A qubit state $\tilde{\rho}_A$ saturates the inequality $\overline{R}(\tilde{\rho}_A) \geqslant R(\tilde{\rho}_A)$ iff $\tilde{\rho}_A$ is pure or incoherent.

VII. EXPONENTIAL DECREASING RATE

In many topics of quantum information, the Rényi entropies characterize the exponential decreasing rate of the error probability, which determines the speed of convergence [35,36]. Concerning secure uniform random-number generation, it is known that the exponential decreasing rate of the leaked information is characterized by Rényi conditional entropies, as explained in Appendix A. To determine the speed of convergence $d_1(\mathsf{M}_{F_n}|F_n) \to 0$, we introduce the Rényi relative entropy of coherence $\underline{C}_{{\rm r},\alpha}(\rho) := \min_{\sigma\in\mathcal{I}} \underline{S}_\alpha(\rho\|\sigma)$ [27,37] based on the Rényi relative entropy:

$$\underline{S}_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\ln\operatorname{tr}(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}})^\alpha \quad (16)$$

with $\alpha \geqslant 0$ (see [38–40] and [41, Theorem 5.13]). Combining Proposition 2 in Appendix A with a generalization of Theorem 1 in Appendix D, we can derive the following theorem, the proof of which is relegated to Appendix E.

Theorem 5. Suppose that F_n are universal 2 hash and have extraction rate R. For $n \geqslant 6$, we have

$$\frac{-1}{n}\ln\mathbb{E}_{F_n} d_1(\mathsf{M}^*_{F_n}(\tilde{\rho}^{\otimes n})) \\ \geqslant -\frac{\tilde{d}_A}{2n}\ln(n+1) + \max_{s\in[0,1]}\frac{s}{2}[\underline{C}_{{\rm r},\frac{1+s}{1+2s}}(\tilde{\rho}_A) - R]. \quad (17)$$

where $\tilde{d}_A$ is the rank of $\tilde{\rho}_A$.

Taking the limit, we have

$$\liminf_{n\to\infty}\frac{-1}{n}\ln d_1(\mathsf{M}^*_{F_n}|F_n) \geqslant \max_{s\in[0,1]}\frac{s}{2}[\underline{C}_{{\rm r},\frac{1+s}{1+2s}}(\tilde{\rho}_A) - R]. \quad (18)$$

Theorem 5 shows that the exponential decreasing rate of the leaked information of the strategy $\mathsf{M}^*_{F_n}$ is characterized by Rényi relative entropies of coherence. In other words, the quality of the random numbers extracted in this way is controlled by these coherence measures. Further, since (17) holds in a finite-length scenario, it guarantees the security in a practical setting.

In information theory, another useful security measure is the relative entropy between the true state and the ideal state [42], which is known to be the unique measure under several natural assumptions [43, Theorem 8]. In Appendix F, we show that an analog of Theorem 5 holds for this alternative measure.

VIII. CONCLUSION

We studied the extraction of secure uniform random numbers in the quantum-quantum setting under incoherent strategies, assuming that Eve can access all of the environment of the given system. This problem properly reflects the situation of a quantum random-number generator. We showed that the maximum rate of extraction is equal to the relative entropy of coherence. In contrast, the extraction rate with a constrained eavesdropper is equal to the coherence of formation. Furthermore, the exponential decreasing rate of the leaked information is characterized by Rényi relative entropies of coherence. These results not only clarify the capability of incoherent strategies in extracting secure uniform random numbers, but also endow coherence measures mentioned above with operational meanings.

To apply our results to the security evaluation of a quantum random-number generator, we first need to estimate the quantum state $\tilde{\rho}_A$ on Alice's system. Fortunately, as explained in Appendix H, this task can be achieved by quantum state tomography, which has been well established (see [44–46] and [41, Chap. 6]). Even when Alice's quantum system cannot be trusted, we can estimate the quantum state $\tilde{\rho}_A$ of Alice's system by combining the method of self-testing [47–49]. Therefore, our paper is helpful to the design of a quantum random-number generator; see Appendix H for more details.

The Appendices are organized as follows. In Appendix A, we briefly review existing results on secure uniform random-number extraction from a C-Q state. Then, we prove (10) and Theorem 3 in Appendix B. Although one might expect a further extension of Theorem 3 due to the additivity of the coherence of formation, we explain why we cannot make further extension of Theorem 3 in Appendix C. In Appendix D, we generalize Theorem 1, which is needed for the proof of Theorem 5. Then, in Appendix E, we prove Theorem 5. Next, in Appendix F, we make security analysis based on an alternative security criterion. In Appendix G, we prove Corollary 1. In Appendix H, we explain how our paper applies to the design of a quantum random-number generator. Finally, in Appendix I, we discuss the relation between the results in [24,25] and our results.

ACKNOWLEDGMENTS

The authors are very grateful to Prof. Lin Chen for helpful discussions and comments. M.H. was supported in part by Japan Society for the Promotion of Science Grants-in-Aid for Scientific Research (Grants No. 17H01280 and No. 16KT0017) and by Kayamori Foundation of Informational Science Advancement. H.Z. acknowledges financial support from the Excellence Initiative of the German Federal and State Governments (Grant No. ZUK 81) and the Deutsche Forschungsgemeinschaft.

APPENDIX A: SECURE UNIFORM RANDOM-NUMBER EXTRACTION FROM A C-Q STATE

Here, we summarize known results on secure uniform random-number extraction when the state is a C-Q state on the composite system $\mathcal{H}_A \otimes \mathcal{H}_E$, which has the form

$$\rho_{AE} = \sum_a P_A(a)|a\rangle\langle a| \otimes \rho_{E|a}. \tag{A1}$$

Given a function f, we define the state

$$\rho_{f(A)E} := \sum_a P_A(a)|f(a)\rangle\langle f(a)| \otimes \rho_{E|a}. \tag{A2}$$

To study secure uniform random-number extraction from a C-Q state, we need to consider the uncertainty quantified by three types of Rényi conditional entropies:

$$\overline{H}^{\uparrow}_\alpha(A|E)_\rho := -\min_{\sigma_E} \underline{S}_\alpha(\rho_{AE}\|I_A \otimes \sigma_E), \tag{A3}$$

$$\overline{H}^{\downarrow}_\alpha(A|E)_\rho := -\underline{S}_\alpha(\rho_{AE}\|I_A \otimes \rho_E), \tag{A4}$$

$$H^{\uparrow}_\alpha(A|E)_\rho := -\min_{\sigma_E} S_\alpha(\rho_{AE}\|I_A \otimes \sigma_E). \tag{A5}$$

Here the two types of Rényi relative entropies are defined as (see [38,39] and [41, Appendix 3.1])

$$S_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\ln \mathrm{tr}(\rho^\alpha\sigma^{1-\alpha}), \tag{A6}$$

$$\underline{S}_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1}\ln \mathrm{tr}(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}})^\alpha, \tag{A7}$$

which satisfy the inequality $S_\alpha(\rho\|\sigma) \geqslant \underline{S}_\alpha(\rho\|\sigma)$. Both $S_\alpha(\rho\|\sigma)$ and $\underline{S}_\alpha(\rho\|\sigma)$ increase monotonically with α.

To extract secure uniform random numbers, we can employ a universal 2 hash function. A random function F from $\mathcal{A}$ to $\mathcal{Z}$ is called universal 2 hash if

$$\mathbb{P}\{F(a) = F(a')\} \leqslant \frac{1}{|\mathcal{Z}|} \tag{A8}$$

for $a \neq a' \in \mathcal{A}$. This type of hash function satisfies the following leftover hashing lemma.

Proposition 1. (See [7].) Let F be a universal 2 hash function from $\mathcal{A}$ to $\mathcal{Z}$. Then, we have

$$\mathbb{E}_F d_1(\rho_{F(A)E}) \leqslant |\mathcal{Z}|^{\frac{1}{2}} 2^{-\frac{1}{2}\overline{H}^{\uparrow}_2(A|E)_{\rho_{AE}}}. \tag{A9}$$

To characterize the ultimate amount of extracted secure uniform random numbers, we define the rate

$$K(\rho_{AE}) := \sup_{F_n}\left\{\liminf_{n\to\infty}\frac{\ln|F_n|}{n}\,\middle|\,\mathbb{E}_{F_n}d_1[(\rho^{\otimes n})_{F_n(A)E}] \to 0\right\}, \tag{A10}$$

where $|F_n|$ denotes the cardinality of the image of F_n and the supremum is taken over sequences of random hash functions which satisfy the given condition. The quantity $K(\rho_{AE})$ expresses the maximum extraction rate of secure uniform random numbers.

In this setting, the simple application of Proposition 1 cannot guarantee the exponential decrease of the leaked information even when the extraction rate R of uniform random numbers is smaller than the conditional entropy $H(A|E)_{\rho_{AE}}$. To resolve this problem, we employ another proposition based on the discussions in [50], which in turn rely on Proposition 1.

Proposition 2. If a sequence of hash functions F_n from $\mathcal{A}^n$ to $\{1,\dots,2^{nR}\}$ is universal 2 hash, then

$$-\frac{1}{n}\ln \mathbb{E}_{F_n} d_1[(\rho^{\otimes n})_{F_n(A)E}] \geqslant -\frac{d_E}{2n}\ln(n+1) + \max_{s\in[0,1]} \frac{1}{2}\left[s\overline{H}^{\uparrow}_{1+s}(A|E)_{\rho_{AE}} - sR\right] \tag{A11}$$

for $n \geqslant 6$, where d_E is the dimension of system E. In addition,

$$\liminf_{n\to\infty} -\frac{1}{n}\ln \mathbb{E}_{F_n} d_1[(\rho^{\otimes n})_{F_n(A)E}] \geqslant \max_{s\in[0,1]} \frac{1}{2}\left[s\overline{H}^{\uparrow}_{1+s}(A|E)_{\rho_{AE}} - sR\right]. \tag{A12}$$

Proof. First, we introduce the quantity (see [50, Appendix IV])

$$\Delta_{d,2}(M|\rho_{AE}) := \min_{\sigma_E}\min_{\rho'_{AE}}[2\|\rho_{AE}-\rho'_{AE}\|_1 + M^{\frac{1}{2}}2^{\frac{1}{2}\underline{S}_2(\rho'_{AE}\|I_A\otimes\sigma_E)}],$$

where $\min_{\rho'_{AE}}$ denotes the minimum under the condition $\mathrm{tr}\,\rho'_{AE} \leqslant 1$ and $\rho'_{AE} \geqslant 0$, while $\min_{\sigma_E}$ denotes the minimum over normalized states σ_E. Here, the quantity $\underline{S}_2(\rho'\|\sigma)$ is defined in the same way as in (A7), that is, $\underline{S}_2(\rho'\|\sigma) = \frac{1}{\alpha-1}\ln \mathrm{tr}(\sigma^{\frac{1-\alpha}{2\alpha}}\rho'\sigma^{\frac{1-\alpha}{2\alpha}})^{\alpha}$, even when ρ' is not normalized. Then, as shown in [50, (73)], Proposition 1 implies that

$$\mathbb{E}_{F_n} d_1[(\rho^{\otimes n})_{F_n(A)E}] \leqslant \Delta_{d,2}(2^{nR}|\rho_{AE}^{\otimes n}). \tag{A13}$$

Let v_n be the number of distinct eigenvalues of $\sigma_E^{\otimes n}$. Then the inequality [50, the next inequality of (83)] yields that

$$\Delta_{d,2}(2^{nR}|\rho_{AE}^{\otimes n}) \leqslant (4+\sqrt{v_n})2^{\frac{s}{2}nR+\frac{s}{2}S_{1+s}[\mathsf{E}_{\sigma_E^{\otimes n}}(\rho_{AE}^{\otimes n})\|I\otimes\sigma_E^{\otimes n}]} \tag{A14}$$

for $s\in[0,1]$, where the CPTP map E_σ is defined as

$$\mathsf{E}_\sigma(\rho) := \sum_x E_x\rho E_x, \tag{A15}$$

assuming that σ has the spectral decomposition $\sigma = \sum_x \lambda_x E_x$.

Since the rank of σ is no more than the dimension d_E of system E, v_n is $\binom{n+d_E-1}{d_E-1}$ at most. In addition, $\sqrt{\binom{n+d_E-1}{d_E-1}}+4 \leqslant (n+1)^{d_E/2}$ when $n\geqslant 6$, so we have

$$(4+\sqrt{v_n}) \leqslant (n+1)^{d_E/2}. \tag{A16}$$

In addition, the information processing inequality guarantees that

$$S_{1+s}\left[\mathsf{E}_{\sigma_E^{\otimes n}}(\rho_{AE}^{\otimes n})\|I\otimes\sigma_E^{\otimes n}\right] \leqslant n\underline{S}_{1+s}(\rho_{AE}\|I\otimes\sigma_E) \tag{A17}$$

according to [51] and [41, (3.17)]. Combining the four equations (A13), (A14), (A16), and (A17) yields

$$\frac{-1}{n}\ln \mathbb{E}_{F_n} d_1[(\rho^{\otimes n})_{F_n(A)E}] \geqslant -\frac{d_E}{2n}\ln(n+1) + \max_{s\in[0,1]}\frac{1}{2}[-s\underline{S}_{1+s}(\rho_{AE}\|I\otimes\sigma_E) - sR]. \tag{A18}$$

Taking the maximum of the right-hand side (RHS) of (A18) over σ_E, we obtain (A11), which implies (A12).

When $R < H(A|E)$, according to Proposition 2, the amount of leaked information $\mathbb{E}_{F_n} d_1((\rho^{\otimes n})_{F_n(A)E})$ goes to zero. Hence, we have

$$K(\rho_{AE}) \geqslant H(A|E)_{\rho_{AE}}. \tag{A19}$$

Since the opposite inequality also holds (see [7] and [50, (93)]), we deduce the following proposition.

Proposition 3. (See [7] and [50, (94)].)

$$K(\rho_{AE}) = H(A|E)_{\rho_{AE}}. \tag{A20}$$

In the current context, it is common to consider another security criterion $I'(\rho_{AE})$ defined as the relative entropy between the true state and the ideal state (see [50, (29)] and [52, (9)]:

$$I'(\rho_{AE}) := S(\rho_{AE}\|\tau_{|\mathcal{A}|}\otimes\rho_E) = \ln|\mathcal{A}| - H(A|E)_{\rho_{AE}}, \tag{A21}$$

where $\tau_{|\mathcal{A}|}$ denotes the completely mixed state on $\mathcal{H}_A$. Under this security criterion, we have the following analog of Proposition 2.

Proposition 4. (See [52, (33)].) If a sequence of hash functions F_n from $\mathcal{A}^n$ to $\{1,\dots,2^{nR}\}$ is universal 2 hash, then

$$\liminf_{n\to\infty} -\frac{1}{n}\ln \mathbb{E}_{F_n} I'[(\rho^{\otimes n})_{F_n(A)E}] \geqslant \max_{s\in[0,1]}[s\overline{H}^{\downarrow}_{1+s}(A|E)_{\rho_{AE}} - sR]. \tag{A22}$$

APPENDIX B: PROOFS OF (10) AND THEOREM 3

Proof of (10).

Let $\mathsf{M}_{F_n} = (U_{\mathrm{i},n},\mathsf{M}_{\mathrm{c},n},F_n)$ *be a sequence of incoherent strategies that satisfy* $d_1(\mathsf{M}_{F_n}|F_n)\to 0$, *that is,*

$$\mathbb{E}_{F_n}\left\|\mathsf{M}_{F_n}(\tilde{\rho}^{\otimes n}) - \tau_{|\mathsf{M}_{F_n}|}\otimes\mathsf{M}_{F_n}(\tilde{\rho}^{\otimes n})_E\right\|_1 \to 0. \tag{B1}$$

Then

$$\frac{1}{n}\left|H(A|E)_{\mathsf{M}_{F_n}(\tilde{\rho}^{\otimes n})} - H(A|E)_{\tau_{|\mathsf{M}_{F_n}|}\otimes\mathsf{M}_{F_n}(\tilde{\rho}^{\otimes n})_E}\right| \to 0 \tag{B2}$$

according to the Fannes inequality for the conditional entropy (see [41, Exercise 5.38] and [53]). Since $\tau_{|\mathsf{M}_{F_n}|}$ is the completely mixed state on the $|\mathsf{M}_{F_n}|$-dimensional system, we have $H(A|E)_{\tau_{|\mathsf{M}_{F_n}|}\otimes\mathsf{M}_{F_n}(\tilde{\rho}^{\otimes n})_E} = \ln|\mathsf{M}_{F_n}|$, which implies that

$$\liminf_{n\to\infty}\mathbb{E}_{F_n}\frac{1}{n}H(A|E)_{\mathsf{M}_{F_n}(\tilde{\rho}^{\otimes n})} = \liminf_{n\to\infty}\frac{1}{n}\ln|\mathsf{M}_{F_n}|. \tag{B3}$$

Now (10) is a consequence of the following equation:

$$\begin{aligned}\mathbb{E}_{F_n}H(A|E)_{\mathsf{M}_{F_n}(\tilde{\rho}^{\otimes n})} &\leqslant H(A|E)_{\mathsf{M}_{\mathrm{c},n}[U_{\mathrm{i},n}(\tilde{\rho}^{\otimes n}\otimes|0\rangle\langle 0|)U_{\mathrm{i},n}^{\dagger}]}\\ &= H(A|E)_{U_{\mathrm{CNOT}}U_{\mathrm{i},n}(\tilde{\rho}^{\otimes n}\otimes|0\rangle\langle 0|)U_{\mathrm{i},n}^{\dagger}U_{\mathrm{CNOT}}^{\dagger}}\\ &\leqslant \max_{U_{\mathrm{i}}} H(A|E)_{\tilde{\rho}^{\otimes n}[U_{\mathrm{i}}]}.\end{aligned} \tag{B4}$$

Proof of Theorem 3. If $R < \min_{\mathsf{M}_E} H(A|E)_{\mathsf{M}_{\mathrm{c}}[\mathsf{M}_E(\tilde{\rho})]}$, then Alice can extract uniform random numbers using the method described in Appendix A, and Proposition 2 there guarantees that the extracted random numbers are secure. Therefore,

$$\overline{R}(\tilde{\rho}_A) \geqslant \min_{\mathsf{M}_E} H(A|E)_{\mathsf{M}_c[\mathsf{M}_E(\tilde{\rho})]} \stackrel{(a)}{=} \min_{\{p_j,|\psi_j\rangle\}} \sum_j p_j C_r(|\psi_j\rangle\langle\psi_j|) = C_F(\rho_A), \quad \text{(B5)}$$

where (a) follows from the fact that any decomposition of $\tilde{\rho}_A$ can be induced by a suitable POVM on $\mathcal{H}_E$.

Let $\mathsf{M}_{F_n} = (U_{i,n}, \mathsf{M}_{c,n}, F_n)$ be a sequence of incoherent strategies the extraction rate of which is R and which satisfies $\underline{d}_1(\mathsf{M}_{F_n}|F_n) \to 0$. Since $\mathbb{E}_{F_n} d_1(\mathsf{M}_{F_n}(\mathsf{M}_E(\tilde{\rho})^{\otimes n})) \to 0$ for any local measurement M_E of Eve, using the same argument that leads to (B4), we can show the inequality

$$R = \liminf_{n\to\infty} \mathbb{E}_{F_n} \frac{1}{n} H(A|E)_{\mathsf{M}_{F_n}(\mathsf{M}_E(\tilde{\rho})^{\otimes n})} \leqslant \max_{U_i} H(A|E)_{U_i(\mathsf{M}_E(\tilde{\rho})\otimes|0\rangle\langle 0|)U_i^\dagger}. \quad \text{(B6)}$$

Taking the minimum over M_E, we have

$$R \leqslant \min_{\mathsf{M}_E} \max_{U_i} H(A|E)_{U_i(\mathsf{M}_E(\tilde{\rho})\otimes|0\rangle\langle 0|)U_i^\dagger} = \min_{\{p_j,|\psi_j\rangle\}} \sum_j p_j C_r(|\psi_j\rangle\langle\psi_j|) = C_F(\rho_A), \quad \text{(B7)}$$

which yields the opposite inequality to (B5).

APPENDIX C: POSSIBILITY OF EXTENSION OF THEOREM 3

Since the coherence of formation is additive, that is, $C_F(\rho^{\otimes n}) = nC_F(\rho)$ [21], one might expect a further extension of Theorem 3. That is, one might speculate that the relation $\overline{R}(\tilde{\rho}_A) = C_F(\tilde{\rho}_A)$ holds even when the condition $\underline{d}_1(\mathsf{M}_{F_n}|F_n) \to 0$ is replaced by the stronger condition $\max_{\mathsf{M}_{E,n}} \mathbb{E}_{F_n} d_1(\mathsf{M}_{F_n}(\mathsf{M}_{E,n}(\tilde{\rho}^{\otimes n}))) \to 0$. Here, note that $\mathsf{M}_{E,n}$ is a POVM on the n-tensor product system; by contrast, in the definition of $\underline{d}_1(\mathsf{M}_{F_n}|F_n)$, Eve's POVMs are restricted to tensor powers of POVMs on individual systems. However, the additivity of C_F alone does not imply this stronger statement.

This stronger statement would follow from a stronger condition as described as follows. Given $\alpha > 0$, define the Rényi coherence of formation as

$$C_{F,1/\alpha}(\rho) := \min_{\{p_j,|\psi_j\rangle\}} \frac{1}{1-\alpha} \ln \sum_j p_j 2^{(1-\alpha)C_{r,1/\alpha}(|\psi_j\rangle\langle\psi_j|)}, \quad \text{(C1)}$$

where $\{p_j,|\psi_j\rangle\}$ satisfies $\rho = \sum_j p_j|\psi_j\rangle\langle\psi_j|$. As shown later,

$$\lim_{\alpha\to 1} C_{F,\alpha}(\rho) = C_F(\rho). \quad \text{(C2)}$$

In addition, if the classical Rényi conditional entropy satisfied the chain rule, i.e.,

$$H_\alpha^\downarrow(A_1A_2|E)_\rho = H_\alpha^\downarrow(A_1|E)_\rho + H_\alpha^\downarrow(A_2|A_1E)_\rho, \quad \text{(C3)}$$

then the Rényi coherence of formation would be additive,

$$C_{F,1/\alpha}(\rho_1\otimes\rho_2) = C_{F,1/\alpha}(\rho_1) + C_{F,1/\alpha}(\rho_2) \quad \text{(C4)}$$

for any pair of density matrices ρ_1 and ρ_2 on A_1 and A_2. Assuming this additivity relation, we can show the inequality

$$\max_{\mathsf{M}_{E,n}} \mathbb{E}_{F_n} d_1\left(\mathsf{M}^*_{F_n}(\mathsf{M}_{E,n}(\tilde{\rho}^{\otimes n}))\right) \leqslant 3\times 2^{sn[R-C_{F,1-s}(\tilde{\rho}_A)]} \quad \text{(C5)}$$

for $s\in[0,1/2]$, where $\mathsf{M}^*_{F_n}$ denotes the optimal incoherent strategy composed of the computational-basis measurement and the application of the universal 2 hash function F_n. In this way, the combination of (C2) and (C5) implies that $\max_{\mathsf{M}_{E,n}} \mathbb{E}_{F_n} d_1(\mathsf{M}^*_{F_n}(\mathsf{M}_{E,n}(\tilde{\rho}^{\otimes n}))) \to 0$ if $R < C_F(\tilde{\rho}_A)$.

However, it is known that the Rényi conditional entropy does not satisfy the chain rule satisfied by the usual conditional entropy even in the classical case [54,55]. This quantity satisfies only a weaker version of the chain rule (see [54, Theorem 1], [56, Corollary 87], and [55, Theorem 3]. Hence, it is not easy to show the relation $\overline{R}(\tilde{\rho}_A) = C_F(\tilde{\rho}_A)$ with the above replacement.

Proof of (C2). For a given $\{p_j,|\psi_j\rangle\}$, the value $\sum_j p_j 2^{(1-\alpha)C_{r,1/\alpha}(|\psi_j\rangle\langle\psi_j|)}$ equals 1 when $\alpha = 1$. So, the formula of the logarithmic derivative $\frac{d}{dx}\ln f(x) = \frac{1}{\ln 2}\frac{df}{dx}(x)/f(x)$ yields that

$$\begin{aligned}
&\lim_{\alpha\to 1}\frac{1}{1-\alpha}\ln\sum_j p_j 2^{(1-\alpha)C_{r,1/\alpha}(|\psi_j\rangle\langle\psi_j|)} \\
&= \frac{1}{\ln 2}\lim_{s\to 0}\frac{\sum_j p_j 2^{sC_{r,1/(1-s)}(|\psi_j\rangle\langle\psi_j|)}-1}{s} \\
&= \sum_j p_j \lim_{s\to 0}\frac{sC_{r,1/(1-s)}(|\psi_j\rangle\langle\psi_j|)}{s} \\
&= \sum_j p_j C_r(|\psi_j\rangle\langle\psi_j|),
\end{aligned}$$

which implies (C2).

Derivation of (C4) assuming the chain rule (C3). When ρ is pure, according to [27,37], we have

$$C_{F,1/\alpha}(\rho) = C_{r,1/\alpha}(\rho) = S_\alpha(\rho^{\text{diag}}) = S_\alpha[\mathsf{M}_c(\rho)], \quad \text{(C6)}$$

where

$$S_\alpha(\rho) = \frac{1}{1-\alpha}\ln \operatorname{tr}(\rho^\alpha) \quad \text{(C7)}$$

is the Rényi α entropy. So the Rényi coherence of formation can be expressed as

$$C_{F,1/\alpha}(\rho) = \min_{\{p_j,\bar{\rho}_j\}}\frac{1}{1-\alpha}\ln\sum_j p_j 2^{(1-\alpha)S_\alpha[\mathsf{M}_c(\bar{\rho}_j)]} = \min_{\{p_j,\bar{\rho}_j\}} H_\alpha^\downarrow(A|J)_{\mathsf{M}_c(\sum_j p_j\bar{\rho}_j\otimes|j\rangle\langle j|)}, \quad \text{(C8)}$$

where $\{p_j,\bar{\rho}_j\}$ satisfies $\rho = \sum_j p_j\bar{\rho}_j$, and J denotes the classical system of the register. The expression (C8) follows from the fact that the minimum is attained when all $\bar{\rho}_j$ are pure.

To prove (C4), suppose $\rho_1\otimes\rho_2$ has an optimal pure-state decomposition $\rho_1\otimes\rho_2 = \sum_j p_j\bar{\rho}_j$ such that

$$C_{F,1/\alpha}(\rho_1\otimes\rho_2) = \frac{1}{1-\alpha}\ln\sum_j p_j 2^{(1-\alpha)C_{r,1/\alpha}(\bar{\rho}_j)}. \quad \text{(C9)}$$

Let $\sigma := \sum_j p_j\bar{\rho}_j\otimes|j\rangle\langle j|$; then

$$C_{F,1/\alpha}(\rho_1\otimes\rho_2) = H_\alpha^\downarrow(A_1A_2|J)_{\mathsf{M}_{c,1}\otimes\mathsf{M}_{c,2}(\sigma)}, \quad \text{(C10)}$$

where $\mathsf{M}_{c,1}$ and $\mathsf{M}_{c,2}$ express the computational-basis measurements on A_1 and A_2, respectively. Now, the chain rule (C3) implies that

$$\begin{aligned} &C_{F,1/\alpha}(\rho_1\otimes\rho_2)\\ &= H_\alpha^{\downarrow}(A_1A_2|J)_{\mathsf{M}_{c,1}\otimes\mathsf{M}_{c,2}(\sigma)}\\ &= H_\alpha^{\downarrow}(A_1|J)_{\mathsf{M}_{c,1}\otimes\mathsf{M}_{c,2}(\sigma)} + H_\alpha^{\downarrow}(A_2|A_1J)_{\mathsf{M}_{c,1}\otimes\mathsf{M}_{c,2}(\sigma)}\\ &\geqslant C_{F,1/\alpha}(\rho_1)+C_{F,1/\alpha}(\rho_2). \end{aligned} \tag{C11}$$

Since the opposite inequality

$$C_{F,1/\alpha}(\rho_1\otimes\rho_2)\leqslant C_{F,1/\alpha}(\rho_1)+C_{F,1/\alpha}(\rho_2) \tag{C12}$$

is an easy consequence of the definition, we deduce (C4), assuming that the chain rule (C3) holds.

Derivation of (C5) assuming the additivity relation (C4). When ρ is a diagonal density matrix, the paper [43, Proposition 21] showed that

$$\Delta_{d,2}(2^R|\rho)\leqslant 3\times 2^{sR-sH^{\uparrow}_{\frac{1}{1-s}}(A|E)_\rho}\leqslant 3\times 2^{sR-sH^{\downarrow}_{\frac{1}{1-s}}(A|E)_\rho} \tag{C13}$$

for $s\in[0,1/2]$. Therefore,

$$\begin{aligned} &\max_{\mathsf{M}_{E,n}} \mathbb{E}_{F_n} d_1\big(\mathsf{M}^*_{F_n}(\mathsf{M}_{E,n}(\tilde\rho^{\otimes n}))\big)\\ &\overset{(a)}{\leqslant} 3\times 2^{snR-sC_{F,1-s}(\tilde\rho_A^{\otimes n})}\overset{(b)}{=}3\times 2^{sn[R-C_{F,1-s}(\tilde\rho_A)]} \end{aligned}$$

if $s\in[0,1/2]$ and F_n is universal 2 hash. Here (a) follows from the combination of (A13), (C8), and (C13), while (b) follows from the assumption that the Rényi coherence of formation is additive.

APPENDIX D: GENERALIZATION OF THEOREM 1

Before proving Theorem 5, which characterizes the exponential decreasing rate of the leaked information, we need to generalize Theorem 1 in terms of Rényi conditional entropies and Rényi relative entropies of coherence.

The two types of Rényi relative entropies defined in (A6) and (A7) can be used to define two types of coherence measures [27,37]:

$$C_{r,\alpha}(\rho):=\min_{\sigma\in\mathcal{I}} S_\alpha(\rho\|\sigma),\quad \underline{C}_{r,\alpha}(\rho):=\min_{\sigma\in\mathcal{I}} \underline{S}_\alpha(\rho\|\sigma), \tag{D1}$$

both of which increase monotonically with α. The following theorem generalizes Theorem 1 and thereby demonstrates the significance of these Rényi relative entropies of coherence.

Theorem 6.

$$\begin{aligned} &\frac{1}{n}\max_{\Lambda_i} \overline{H}_\alpha^{\uparrow}(A|E)_{\tilde\rho^{\otimes n}[\Lambda_i]} = \max_{\Lambda_i} \overline{H}_\alpha^{\uparrow}(A|E)_{\tilde\rho[\Lambda_i]}\\ &= \max_{U_i} \overline{H}_\alpha^{\uparrow}(A|E)_{\tilde\rho[U_i]} = \overline{H}_\alpha^{\uparrow}(A|E)_{\tilde\rho[U_{\rm CNOT}]} = \underline{C}_{r,\beta}(\tilde\rho_A), \end{aligned} \tag{D2}$$

$$\begin{aligned} &\frac{1}{n}\max_{\Lambda_i} \overline{H}_\alpha^{\downarrow}(A|E)_{\tilde\rho^{\otimes n}[\Lambda_i]} = \max_{\Lambda_i} \overline{H}_\alpha^{\downarrow}(A|E)_{\tilde\rho[\Lambda_i]}\\ &= \max_{U_i} \overline{H}_\alpha^{\downarrow}(A|E)_{\tilde\rho[U_i]} = \overline{H}_\alpha^{\downarrow}(A|E)_{\tilde\rho[U_{\rm CNOT}]} = C_{r,\beta}(\tilde\rho_A), \end{aligned} \tag{D3}$$

where U_i is an incoherent unitary, Λ_i is an incoherence-preserving operation, (D2) holds for $\alpha,\beta\in[\frac{1}{2},\infty]$ with $\frac{1}{\alpha}+\frac{1}{\beta}=2$, while (D3) holds for $\alpha\in[\frac{1}{2},\infty]$ and $\beta\in[0,2]$ with $\alpha\beta=1$.

The proof of Theorem 6 relies on the duality relations between Rényi conditional entropies. When ρ is a pure state across the three systems $\mathcal{H}_A,\mathcal{H}_B$, and $\mathcal{H}_E$, these conditional entropies obey the following duality relations (see [38,40,57] and [41, Theorem 5.13]):

$$\overline{H}_\alpha^{\uparrow}(A|E)_\rho+\overline{H}_\beta^{\uparrow}(A|B)_\rho=0, \tag{D4}$$

$$\overline{H}_\alpha^{\downarrow}(A|E)_\rho+H_\beta^{\uparrow}(A|B)_\rho=0, \tag{D5}$$

where (D4) holds for $\alpha,\beta\in[\frac{1}{2},\infty]$ with $\frac{1}{\alpha}+\frac{1}{\beta}=2$ and (D5) holds for $\alpha,\beta\in[0,\infty]$ with $\alpha\beta=1$.

Proof of Theorem 6. Let $\beta=\alpha/(2\alpha-1)$; then $\frac{1}{\alpha}+\frac{1}{\beta}=2$. Let U_i be any incoherent unitary acting on $\mathcal{H}_A\otimes\mathcal{H}_B$; then

$$\begin{aligned} \overline{H}_\alpha^{\uparrow}(A|E)_{\tilde\rho[U_i]} &= -\overline{H}_\beta^{\uparrow}(A|B)_{\tilde\rho[U_i]}\leqslant \underline{E}_{r,\beta}(\tilde\rho[U_i]_{AB})\\ &\leqslant \underline{C}_{r,\beta}(\tilde\rho[U_i]_{AB})\leqslant \underline{C}_{r,\beta}(\tilde\rho_A). \end{aligned} \tag{D6}$$

Here the equality follows from (D4), the first inequality follows from [27, Lemma 4], and the other two inequalities are trivial. According to [27, Theorem 1], the upper bound in the RHS of (D6) is attained when U_i is the generalized CNOT gate, in which case $\tilde\rho[U_i]_{AB}$ is maximally correlated.

By the same reasoning as above, we deduce the equality $\max_{\Lambda_i}\overline{H}_\alpha^{\uparrow}(A|E)_{\tilde\rho[\Lambda_i]}=\underline{C}_{r,\beta}(\tilde\rho_A)$, which in turn implies that $\max_{\Lambda_i}\overline{H}_\alpha^{\uparrow}(A|E)_{\tilde\rho^{\otimes n}[\Lambda_i]}=\underline{C}_{r,\beta}(\tilde\rho_A^{\otimes n})$. Now the proof of (D2) is completed by the additivity relation $\underline{C}_{r,\beta}(\tilde\rho_A^{\otimes n})=n\underline{C}_{r,\beta}(\tilde\rho_A)$, which is shown in [27, Theorem 3].

Finally, (D3) can be proved in a similar way.

APPENDIX E: PROOF OF THEOREM 5

Proof of Theorem 5. Applying Proposition 2 in Appendix A with $n\geqslant 6$, we deduce that

$$\begin{aligned} &\frac{-1}{n}\ln\mathbb{E}_{F_n}d_1\big[\mathsf{M}^*_{F_n}(\tilde\rho^{\otimes n})\big]\\ &\geqslant -\frac{\tilde d_A}{2n}\ln(n+1)+\max_{s\in[0,1]}\frac{1}{2}[s\overline{H}^{\uparrow}_{1+s}(A|E)_{\mathsf{M}_c(\tilde\rho)}-sR], \end{aligned} \tag{E1}$$

where $\tilde d_A$ is the rank of $\tilde\rho_A$ because the dimension of system E can be reduced to the rank $\tilde d_A$. Now Theorem 5 is a corollary of the following equation:

$$\overline{H}^{\uparrow}_{1+s}(A|E)_{\mathsf{M}_c(\tilde\rho)}=\overline{H}^{\uparrow}_{1+s}(A|E)_{\tilde\rho[U_{\rm CNOT}]}=\underline{C}_{r,\frac{1+s}{1+2s}}(\tilde\rho_A), \tag{E2}$$

where the second equality follows from (D2) in Theorem 6.

APPENDIX F: SECURITY ANALYSIS BASED ON AN ALTERNATIVE CRITERION

Here we analyze the exponential decreasing rate of the alternative security measure $I'(\rho_{AE})$ defined in (A21), which denotes the relative entropy between the true state and the ideal state [42]. Similar to Theorem 5, we have

$$\liminf_{n\to\infty} \frac{-1}{n} \ln \mathbb{E}_{F_n} I'\big[\mathsf{M}^*_{F_n}(\tilde{\rho}^{\otimes n})\big] \geqslant \max_{s\in[0,1]} [s C_{\mathrm{r},\frac{1}{1+s}}(\tilde{\rho}_A) - sR]. \tag{F1}$$

Again, the exponential decreasing rate of the leaked information is controlled by Rényi relative entropies of coherence. To prove (F1), note that

$$\liminf_{n\to\infty} \frac{-1}{n} \ln \mathbb{E}_{F_n} I'\big[\mathsf{M}^*_{F_n}(\tilde{\rho}^{\otimes n})\big] \geqslant \max_{s\in[0,1]} [s \overline{H}^{\downarrow}_{1+s}(A|E)_{\mathsf{M}_\mathrm{c}(\tilde{\rho})} - sR] \tag{F2}$$

according to Proposition 4 in Appendix A. Now (F1) is a corollary of the following equation:

$$\overline{H}^{\downarrow}_{1+s}(A|E)_{\mathsf{M}_\mathrm{c}(\tilde{\rho})} = \overline{H}^{\downarrow}_{1+s}(A|E)_{\tilde{\rho}[U_{\mathrm{CNOT}}]} = C_{\mathrm{r},\frac{1}{1+s}}(\tilde{\rho}_A), \tag{F3}$$

where the second equality follows from (D3) in Theorem 6.

APPENDIX G: PROOF OF COROLLARY 1

In view of Theorems 2 and 3, Corollary 1 is an immediate consequence of the following lemma.

Lemma 1. A qubit state ρ saturates the inequality $C_\mathrm{F}(\rho) \geqslant C_\mathrm{r}(\rho)$ iff ρ is pure or incoherent.

Proof. The inequality $C_\mathrm{F} \geqslant C_\mathrm{r}$ holds in general because C_F is the convex roof of C_r, and C_r is convex.

Any qubit state can be written as follows:

$$\rho = \frac{1}{2}(I + x\sigma_x + y\sigma_y + z\sigma_z), \quad x^2 + y^2 + z^2 \leqslant 1, \tag{G1}$$

where $\sigma_x, \sigma_y, \sigma_z$ are standard Pauli matrices and (x,y,z) is the Bloch vector. Let $r = \sqrt{x^2+y^2+z^2}$; then

$$C_\mathrm{r}(\rho) = H\left(\frac{1+z}{2}\right) - H\left(\frac{1+r}{2}\right), \tag{G2}$$

$$C_\mathrm{F}(\rho) = H\left(\frac{1+\sqrt{1-x^2-y^2}}{2}\right), \tag{G3}$$

where $H(p) = -p\ln p - (1-p)\ln(1-p)$, and the formula for $C_\mathrm{F}(\rho)$ was derived in [24]. The relation between C_r and C_F was illustrated in Fig. 3 of [25].

If ρ is pure, then $x^2+y^2+z^2 = 1$, so that $C_\mathrm{F}(\rho) = C_\mathrm{r}(\rho) = H(\frac{1+z}{2})$. If ρ is incoherent, then $x = y = 0$, so that $C_\mathrm{F} = C_\mathrm{r} = 0$.

To determine the condition for saturating the inequality $C_\mathrm{F} \geqslant C_\mathrm{r}$, first consider the case $y = z = 0$, so that $C_\mathrm{r}(\rho) = 1 - H(\frac{1+x}{2})$ and $C_\mathrm{F}(\rho) = H(\frac{1+\sqrt{1-x^2}}{2})$. By computing the first and second derivatives of $C_\mathrm{F}(\rho) - C_\mathrm{r}(\rho)$ with x, it is not difficult to prove that $C_\mathrm{F}(\rho) = C_\mathrm{r}(\rho)$ iff $x = 0$ or ± 1.

Next, consider the case $0 < x < 1$, $y = 0$, $z \geqslant 0$, and $x^2 + z^2 < 1$. Let ρ_1, ρ_2 be two qubit states with Bloch vectors $(x,0,0)$ and $(x,0,\sqrt{1-x^2})$, respectively. Then ρ is a convex combination of ρ_1 and ρ_2, that is, $\rho = p_1\rho_1 + p_2\rho_2$ with $p_1 > 0$. In addition,

$$C_\mathrm{F}(\rho) = C_\mathrm{F}(\rho_1) = C_\mathrm{F}(\rho_2) = C_\mathrm{r}(\rho_2), \quad C_\mathrm{F}(\rho_1) > C_\mathrm{r}(\rho_1). \tag{G4}$$

Given that C_r is convex, we conclude that

$$C_\mathrm{r}(\rho) \leqslant p_1 C_\mathrm{r}(\rho_1) + p_2 C_\mathrm{r}(\rho_2) < p_1 C_\mathrm{F}(\rho_1) + p_2 C_\mathrm{F}(\rho_2) = C_\mathrm{F}(\rho). \tag{G5}$$

By symmetry $C_\mathrm{r}(\rho) < C_\mathrm{F}(\rho)$ whenever $x^2 + y^2 + z^2 < 1$ and $x^2 + y^2 > 0$. Therefore, the inequality $C_\mathrm{F}(\rho) \geqslant C_\mathrm{r}(\rho)$ is saturated iff the qubit state ρ is pure or incoherent.

APPENDIX H: APPLICATION TO QUANTUM RANDOM-NUMBER GENERATORS

Here, we explain the application of our paper to the design of a quantum random-number generator in a realistic scenario. The main text assumes that the underlying state and all the devices have known independent and identical structure and are fully trusted. Now, this assumption is weakened to the assumption that the underlying state and devices have independent and identical structure, but are not trusted. The assumption of independent and identical structure is relevant in a practical scenario. Remember that our optimal incoherent strategy can be realized by the measurement M_c in the computational basis followed by classical data processing. A quantum random-number generator consists of the following ingredients: an internal quantum system, the device that performs the computational-basis measurement, and the data processor that extracts secure uniform random numbers. To make a quantum random-number generator as an industrial product, the supplier needs to specify the method for preparing the state of the internal system, which can be identified by quantum state tomography (see [44–46] and [41, Chap. 6]).

To implement quantum state tomography, the supplier can perform suitable measurements on the quantum system and reconstruct the quantum state based on the measurement statistics. Since quantum measurements are destructive, to achieve sufficient precision in this procedure, usually many identically prepared quantum states are needed to gather enough information. In addition, quantum state tomography may require operations that are not incoherent, but this is not a problem. Note that in the design stage of the random-number generator it is reasonable to assume that the supplier can access certain advanced equipment and is not restricted to incoherent operations, in contrast with the user stage of the device.

Once the internal state $\tilde{\rho}_A$ of the random-number generator is determined, the supplier can choose the parameter n and the extraction rate R based on the upper bound determined by Theorem 5, so that the amount of leaked information $d_1(\mathsf{M}^*_{F_n}|F_n)$ is less than a given threshold. Note that Theorem 5 allows one to perform a finite-length analysis. Since $d_1(\mathsf{M}^*_{F_n}|F_n)$ decreases exponentially with n, this task can be achieved with a suitable choice of the parameters as long as $\tilde{\rho}_A$ is sufficiently coherent. In addition, the supplier needs to design universal 2 hash functions so as to perform randomness extraction. Although random numbers are needed to apply random hash functions, the security is not compromised even if Eve knows which specific hash function is applied each time. Therefore, the supplier needs to design universal 2 hash functions only once, which can then be employed repeatedly. The user does not have to invest random numbers to operate the random-number generator.

So far we have assumed that the measurement device for estimating the quantum state of the internal system is trustworthy. This assumption is not absolutely necessary. Even when the measurement device cannot be trusted, the supplier can identify the measurement device by applying the method of self-testing [47–49]. The self-testing was originally proposed using the Clauser-Horne-Shimony-Holt (CHSH) test, which requires the preparation of a Bell state [47,48]. Recently, the paper [49] improved it by proposing a hybrid method of the CHSH test and the Bell state test, i.e., the stabilizer test. Applying this method before quantum state tomography, the supplier can identify the measurement device so that the quantum state of the internal system can be guaranteed. Similarly, the measurement device for generating random numbers may not be trustworthy. In that case, the supplier can apply the self-testing to this measurement device. In this way, the supplier can guarantee the security of the random numbers generated by the random-number generator.

APPENDIX I: RELATION WITH [24,25]

Here, we need to discuss the relation with the papers [24,25], which studied related but different problems. The focus of the current paper is the extraction of uniform random numbers by incoherent strategies, which include the measurement on the computational basis and general incoherent operations (or incoherence-preserving operations). The focus of [25] is the discussion of the uncertainty of Alice's random numbers conditioned on Eve's information. It did not consider the extraction of secure uniform random numbers nor the secrecy measure d_1 or $\underline{d}_1$, which is definitely needed for the security analysis of extracted uniform random numbers.

The focus of [24] is the connection between intrinsic randomness and coherence measures. In information theory, the term "intrinsic randomness" usually means the extraction of uniform random numbers [58,59]. In [24], the term has a related but different meaning, that is, the randomness of measurement outcomes conditioned on Eve's prediction. With this latter interpretation, [24] showed that the intrinsic randomness of measurement outcomes with respect to the computational basis is equal to the coherence of formation, without discussing general protocols for extracting uniform random numbers.

[1] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, Quantum random number generation, npj Quantum Information **2**, 16021 (2016).

[2] M. Herrero-Collantes and J. C. Garcia-Escartin, Quantum random number generators, Rev. Mod. Phys. **89**, 015004 (2017).

[3] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, A fast and compact quantum random number generator, Rev. Sci. Instrum. **71**, 1675 (2000).

[4] M. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, High speed optical quantum random number generation, Opt. Express **18**, 13029 (2010).

[5] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, Quantum random-number generator based on a photon-number-resolving detector, Phys. Rev. A **83**, 023820 (2011).

[6] W. Wei and H. Guo, Quantum random number generator based on the photon number decision of weak laser pulses, in *2009 Conference on Lasers and Electro Optics and The Pacific Rim Conference on Lasers and Electro-Optics* (IEEE, New York, 2009), pp. 1–2.

[7] R. Renner, Security of quantum key distribution, Ph.D. dissertation, ETH Zurich, 2005.

[8] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nat. Commun. **3**, 634 (2012).

[9] R. Renner and S. Wolf, Simple and tight bounds for information reconciliation and privacy amplification, in *Advances in Cryptology*, Lecture Notes in Computer Science Vol. 3788 (Springer-Verlag, Berlin, 2005), pp. 199–216.

[10] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[11] M. Hayashi, Practical evaluation of security for quantum key distribution, Phys. Rev. A **74**, 022307 (2006).

[12] K. Li, A. Winter, X. B. Zou, and G. C. Guo, The Private Capacity of Quantum Channels is not Additive, Phys. Rev. Lett. **103**, 120501 (2009).

[13] M. Berta, Quantum side information: Uncertainty relations, extractors, channel simulations, Ph.D. thesis, ETH Zurich, 2013, arXiv:1310.4581.

[14] M. Berta, O. Fawzi, and S. Wehner, Quantum to classical randomness extractors, in *Advances in Cryptology CRYPTO 2012*, edited by R. Safavi-Naini and R. Canetti, Lecture Notes in Computer Science Vol. 7417 (Springer, Berlin, 2012), pp. 776–793.

[15] M. Berta, O. Fawzi, and S. Wehner, Quantum to classical randomness extractors, IEEE Trans. Inf. Theory **60**, 1168 (2014).

[16] O. Fawzi, Uncertainty relations for multiple measurements with applications, Ph.D. thesis, McGill University, 2012, arXiv:1208.5918.

[17] I. Marvian, and R. W. Spekkens, How to quantify coherence: Distinguishing speakable and unspeakable notions, Phys. Rev. A **94**, 052324 (2016).

[18] A. Streltsov, G. Adesso, and M. B. Plenio, Quantum Coherence as a Resource, Rev. Mod. Phys. **89**, 041003 (2017).

[19] J. Aberg, Quantifying superposition, arXiv:quant-ph/0612146.

[20] T. Baumgratz, M. Cramer, and M. B. Plenio, Quantifying Coherence, Phys. Rev. Lett. **113**, 140401 (2014).

[21] A. Winter and D. Yang, Operational Resource Theory of Coherence, Phys. Rev. Lett. **116**, 120404 (2016).

[22] E. Chitambar and G. Gour, Critical Examination of Incoherent Operations and a Physically Consistent Resource Theory of Quantum Coherence, Phys. Rev. Lett. **117**, 030401 (2016).

[23] M.-L. Hu, X. Hu, J.-C. Wang, Y. Peng, Y.-R. Zhang, and H. Fan, Quantum coherence and quantum correlations, arXiv:1703.01852.

[24] X. Yuan, H. Zhou, Z. Cao, and X. Ma, Intrinsic randomness as a measure of quantum coherence, Phys. Rev. A **92**, 022124 (2015).

[25] X. Yuan, Q. Zhao, D. Girolami, and X. Ma, Interplay between local quantum randomness and non-local information access, arXiv:1605.07818v2.

[26] M. B. Plenio, S. Virmani, and P. Papadopoulos, Operator monotones, the reduction criterion and the relative entropy, J. Phys. A **33**, L193 (2000).

[27] H. Zhu, M. Hayashi, and L. Chen, Coherence and entanglement measures based on Rényi relative entropies, J. Phys. A **50**, 475303 (2017).

[28] A. Streltsov, U. Singh, H. S. Dhar, M. N. Bera, and G. Adesso, Measuring Quantum Coherence with Entanglement, Phys. Rev. Lett. **115**, 020403 (2015).

[29] E. M. Rains, Bound on distillable entanglement, Phys. Rev. A **60**, 179 (1999).

[30] H. Zhu, Z. Ma, Z. Cao, S.-M. Fei, and V. Vedral, Operational one-to-one mapping between coherence and entanglement measures, Phys. Rev. A **96**, 032316 (2017).

[31] H. Zhu, M. Hayashi, and L. Chen, Axiomatic and operational connections between l_1-norm of coherence and negativity, arXiv:1704.02896.

[32] L. Carter and M. Wegman, Universal classes of hash functions, J. Comput. System Sci. **18**, 143 (1979).

[33] M. N. Wegman and J. L. Carter, New hash functions and their use in authentication and set inequality, J. Comput. System Sci. **22**, 265 (1981).

[34] M. Hayashi and T. Tsurumaru, More efficient privacy amplification with less random seeds via dual universal hash function, IEEE Trans. Inf. Theory **62**, 2213 (2016).

[35] M. Hayashi, Exponents of quantum fixed-length pure state source coding, Phys. Rev. A **66**, 032321 (2002).

[36] M. Hayashi, M. Koashi, K. Matsumoto, F. Morikoshi, and A. Winter, Error exponents for entanglement concentration, J. Phys. A **36**, 527 (2003).

[37] E. Chitambar and G. Gour, Comparison of incoherent operations and measures of coherence, Phys. Rev. A **94**, 052336 (2016); Comparison of incoherent operations and measures of coherence, **95**, 019902(E) (2017).

[38] M. Müller-Lennert, F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel, On quantum Rényi entropies: A new generalization and some properties, J. Math. Phys. **54**, 122203 (2013).

[39] M. M. Wilde, A. Winter, and D. Yang, Strong converse for the classical capacity of entanglement-breaking and Hadamard channels, Commun. Math. Phys. **331**, 593 (2014).

[40] M. Tomamichel, M. Berta, and M. Hayashi, Relating different quantum generalizations of the conditional Rényi entropy, J. Math. Phys. **55**, 082206 (2014).

[41] M. Hayashi, *Quantum Information Theory*, Graduate Texts in Physics (Springer, New York, 2017).

[42] I. Csiszár and P. Narayan, Secrecy capacities for multiple terminals, IEEE Trans. Inf. Theory **50**, 3047 (2004).

[43] M. Hayashi, Security analysis of ε-almost dual universal$_2$ hash functions: Smoothing of min entropy versus smoothing of Rényi entropy of order 2, IEEE Trans. Inf. Theory **62**, 3451 (2016).

[44] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982), (originally published in Russian, 1980).

[45] R. D. Gill and S. Massar, State estimation for large ensembles, Phys. Rev. A **61**, 042312 (2000).

[46] M. Hayashi editor *Asymptotic Theory in Quantum Statistical Inference: Selected Papers* (World Scientific, Singapore, 2005).

[47] D. Mayers and A. Yao, Self testing quantum apparatus, Quantum Inf. Comput. **4**, 273 (2004).

[48] M. McKague, T. H. Yang, and V. Scarani, Robust self-testing of the singlet, J. Phys. A **45**, 455304 (2012).

[49] M. Hayashi and M. Hajdusek, Self-guaranteed measurement-based quantum computation, arXiv:1603.02195 (2016).

[50] M. Hayashi, Large deviation analysis for quantum security via smoothing of Rényi entropy of order 2, IEEE Trans. Inf. Theory **60**, 6702 (2014).

[51] M. Mosonyi and T. Ogawa, Quantum hypothesis testing and the operational interpretation of the quantum Rényi relative entropies, Commun. Math. Phys. **334**, 1617 (2015).

[52] M. Hayashi, Precise evaluation of leaked information with secure randomness extraction in the presence of quantum attacker, Commun. Math. Phys. **333**, 335 (2015).

[53] R. Alicki and M. Fannes, Continuity of quantum conditional information, J. Phys. A **37**, L55 (2004).

[54] F. Dupuis, Chain rules for quantum Rényi entropies, J. Math. Phys. **56**, 022203 (2015).

[55] S. Fehr and S. Berens, On the conditional Rényi entropy, IEEE Trans. Inf. Theory **60**, 6801 (2014).

[56] M. Hayashi and R. Matsumoto, Secure multiplex coding with dependent and non-uniform multiple messages, IEEE Trans. Inf. Theory **62**, 2355 (2016).

[57] S. Beigi, Sandwiched Rényi divergence satisfies data processing inequality, J. Math. Phys. **54**, 122202 (2013).

[58] M. Hayashi, Second-order asymptotics in fixed-length source coding and intrinsic randomness, IEEE Trans. Inf. Theory **54**, 4619 (2008).

[59] T. S. Han, *Information-Spectrum Methods in Information Theory* (Springer, Berlin, 2002) (originally appeared in Japanese in 1998).