別紙1－1

論文審査の結果の要旨および担当者

報告番号	※　甲　　第　　13789　　号

氏　　名　細山田　光倫

論　文　題　目

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)

論文審査担当者

主査	名古屋大学	工学研究科	准教授	岩田　哲
委員	名古屋大学	未来社会創造機構	教授	河口　信夫
委員	名古屋大学	工学研究科	教授	道木　慎二
委員	京都大学	基礎物理学研究所	准教授	森前　智行

別紙１－２

論文審査の結果の要旨

細山田光倫君提出の論文「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）」は、量子計算機が実現した環境における共通鍵暗号技術の安全性を解析したものであり、主要な共通鍵暗号技術を取り上げ、量子攻撃に対する安全性を証明可能安全性の観点から議論している。各章の概要は以下のとおりである。

第1章では、本論文の背景および解決すべき未解決問題を整理している。公開鍵暗号技術と共通鍵暗号技術の違いを整理し、証明可能安全性の重要性を説明している。また、ブロック暗号、tweakableブロック暗号、メッセージ認証コード、暗号学的ハッシュ関数等の主要な共通鍵暗号技術の位置づけを明らかにし、量子攻撃の数学的モデル化について述べ、本論文の結果の概要を述べるとともに、関連研究を整理している。

第2章では、本論文で使用する記法を定めている。

第3章では、量子攻撃に対する安全性証明における重要なツールであり、2019年にZhandryにより提案されたcompressed oracle techniqueについてまとめている。

第4章では、ブロック暗号の最も基本的で重要な構成法であるLuby-Rackoff暗号について、4ラウンド繰り返し構造が量子選択平文攻撃に対して安全であることを証明している。3ラウンド繰り返し構造が量子攻撃に対して脆弱であることが知られており、ラウンド数を増やした際に安全性が証明できるか、という未解決問題に対する肯定的な解を与えるとともに、古典攻撃に対する安全性を有する自然なブロック暗号の構成が、量子攻撃に対する安全性をも有しているような構成例を与えている。

第5章では、量子攻撃に対して安全性を証明できるtweakableブロック暗号として、LRWQ方式を設計、提案し、その安全性を証明している。古典攻撃に対して安全性を証明可能なLRW方式に対し効率的な量子攻撃が存在するのに対し、LRWQ方式は量子攻撃に対する証明可能安全性を有しており、量子攻撃に対して証明可能安全なtweakableブロック暗号は存在するのか、という未解決問題に対する解を与えている。

第6章では、メッセージ認証コードHMACとNMACについて、これらの方式が量子攻撃に対して安全であるという証明が従来研究であったのに対し、既知の結果を大幅に改善してより高い安全性を有している、ということを証明している。得られた安全性限界式は既知の汎用的な量子攻撃と一致しており、厳密な安全性証明を与えている。理論面のみならず、実用上も極めて重要な知見を与えている。

第7章では暗号学的ハッシュ関数SKINNY-HASHの内部関数が強識別不可能性という古典的に強い安全性定義を満たすことを証明している。

第8章において研究を総括するとともに、今後の展望について述べている。

以上のように、本論文は主要な共通鍵暗号技術を取り上げ、これらの量子攻撃に対する未解決問題を、証明可能安全性の枠組みで解決したものである。これらの成果は、共通鍵暗号技術の量子攻撃に対する安全性解析の先駆的な研究結果であり、理論的にも実用的にも重要な知見を与えており、工学の発展に寄与するところが大きいと判断できる。よって、本論文の提出者である細山田光倫君は博士（工学）の学位を受けるに十分な資格があると判断した。