別紙様式第２号

学位論文及び審査結果の要旨

横浜国立大学

氏名	佐藤 慎悟
学位の種類	博士（情報学）
学位記番号	環情博甲第 2139 号
学位授与年月日	令和 2 年 3 月 24 日
学位授与の根拠	学位規則（昭和 28 年 4 月 1 日文部省令第 9 号）第 4 条第 1 項及び横浜国立大学学位規則第 5 条第 1 項
学府・専攻名	環境情報学府　情報メディア環境学専攻
学位論文題目	A Study on Cryptography Resistant to Quantum Computing（量子計算に耐性のある暗号技術に関する研究）
論文審査委員	主査　横浜国立大学　教授　四方順司 横浜国立大学　教授　松本　勉 横浜国立大学　教授　森　辰則 横浜国立大学　准教授　吉岡克成 横浜国立大学　講師　白川真一

論文及び審査結果の要旨

近年、量子コンピュータ技術の研究開発が進展する中、この技術を攻撃者が利用できる環境においても、情報セキュリティの安全性が確保されることが求められている。こうした観点から、世界では、現代のコンピュータに対してだけでなく、量子コンピュータに対しても安全性を保証できる暗号技術の研究開発が活発化している。時間計算量の観点から量子コンピュータに対する安全な暗号技術は「耐量子計算機暗号（Post-Quantum Cryptography）」とよばれる。本論文は、耐量子計算機暗号における様々な暗号基礎技術（暗号、認証、認証つき暗号の機能をもつ技術）を提案するとともに、提案方式の安全性証明を数理的に与えている。このように、本論文は耐量子計算機暗号に関する理論研究成果を広くまとめたものであり、本論文は序論（第 1 章）と結論（第 6 章）を含めて全 6 章から構成され、全文が英語で書かれた博士論文である。

第 1 章の Introduction では、量子コンピュータの開発状況や、それに対する米国政府の取り組み等、社会的背景も含めて耐量子計算機暗号の重要性を説明している。また、耐量子計算機暗号の安全性を記述するモデルとして、攻撃者は計算には量子コンピュータを利用するがデータ取得には古典的クエリだけを利用するモデル、攻撃者は量子コンピュータによる計算に加えて量子クエリを利用してデータ取得を行うモデルの 2 種類のモデルを説明している。攻撃モデルとしては後者の方が強力であり、そのため後者に対する安全性を実現する方が高度な技術が必要とされるため、本論文はこの立場からの安全性（量子安全性）をみたす暗号基礎技術の構築に焦点を当てている。そして、量子安全性に関する暗号基礎技術の既存研究を概観すると共に、本論文の貢献の概要を説明している。

第 2 章の Preliminaries では、量子計算に関わる基礎的内容を説明している。また、量子コンピュータでも多項式時間の解法が存在しないと予想されている格子問題の代表例として、Shortest Vector Problem (SVP), Learning With Errors (LWE), Small Integer Solution (SIS) について説明している。さらに、現代暗号の基礎技術である、疑似乱数生成器、擬似ランダム関数、公開鍵暗号、鍵カプセル化メカニズム（KEM）、データカプセル化メカニズム（DEM）、デジタル署名、メッセージ認証コード（MAC）、Lossy Identification 等について解説している。

第 3 章の Quantum-Secure Public Key Encryption では、量子コンピュータに対して安全な公開鍵暗号に関する成果をまとめている。公開鍵暗号の標準的な安全性である CCA（Chosen Ciphertext Attack）安全性をみたす構成法は既存研究において提案されているものの、本論文では更に強い安全性である SO-CCA（Selecting-Opening against Chosen Ciphertext Attack）安全性をみたす公開鍵暗

号の構成法を新たに提案している。SO-CCA 安全性は、複数ユーザがいるネットワーク環境において、一部のユーザが暗号文生成に使用した平文や乱数が漏洩しても、その他のユーザが生成した暗号文の安全性を保証する概念である。本論文では SO-CCA 安全性をみたす 2 種類の構成法を提案している。1 つ目は KEM と DEM による構成、2 つ目は KEM と MAC による構成であり、構成された公開鍵暗号が SO-CCA 安全性をみたすための KEM、DEM、MAC に求められる条件を示し、安全性の証明を数理的に与えている。

第 4 章の Quantum-Secure Message Authentication with Aggregation では、量子コンピュータに対して安全かつ複数の認証子データを圧縮可能な MAC に関する成果をまとめている。量子安全性をみたす MAC については既存研究において報告されているが、本論文では多くのデバイスがネットワークに繋がる環境を想定して、複数の MAC の認証子を安全に圧縮する技術に関して提案している。本論文では、複数のデータコンテンツの完全性を保証するアグリゲート認証技術に対する量子安全性の定式化を行い、既存の方式（Katz-Lindell 方式）がその安全性をみたすことを数理的に証明している。また、複数のデータコンテンツおよびそれらの順序の完全性を保証する順序付きアグリゲート認証技術に対する量子安全性の定式化を行い、既存方式がその安全性を達成できないことを示した上で、その安全性をみたす 2 方式を新たに提案している。1 つ目は量子安全性をもつ疑似ランダム関数から構成し、2 つ目は確率的疑似乱数生成器から構成されており、それらの量子安全性に関する証明を数理的に与えている。

第 5 章の Quantum-Secure Signcryption では、量子コンピュータに対して安全な認証つき暗号に関する成果をまとめている。Signcryption はデータ秘匿性とデータ完全性を同時に達成するため、公開鍵暗号とデジタル署名の両機能を備えた技術である。本論文では、複数ユーザがいるネットワーク環境において、一部のユーザの秘密鍵が漏洩しても、その他のユーザのデータに対する安全性を保証できる方式として新たに 2 方式を提案している。1 つ目の方式は格子問題（LWE および SIS）の計算困難性を仮定して直接的に構成されている。また、2 つ目の方式は量子安全性をもつ公開鍵暗号、Lossy Identification、量子ランダム関数から一般的に構成されている。そして、これら方式の安全性の証明を数理的に与えている。これまでの既存研究においても量子コンピュータに対して安全な認証つき暗号は提案されているが、本論文での提案方式は、既存方式よりも暗号文サイズや鍵サイズ（公開鍵サイズ、秘密鍵サイズ）が小さいという意味で効率的であることが示されている。

最後の第 6 章の Conclusion では、本論文の成果を総括するとともに、当該分野において今後さらに発展が望まれる技術的課題に関しても論じている。

上記のように、本論文は、暗号理論分野の中で耐量子計算機暗号技術に関わる研究成果を高い完成度でまとめたものであり、独創性が高く当該分野への学術的貢献度の高い論文である。

以上から、本論文は博士（情報学）の学位論文として十分な価値を有すると審査委員全員一致して認めるものである。

注　論文及び審査結果の要旨欄に不足が生じる場合には、同欄の様式に準じ裏面又は別紙によること。