# 審 査 の 結 果 の 要 旨

氏　　名　　大西　健斗

安全な情報通信を行うためには、公開鍵暗号は必要不可欠な技術である。本論文は、長期間の安全性を検証するため、現在の脅威であるサイドチャネル攻撃および近い将来に脅威となり得る量子攻撃に対する公開鍵暗号の安全性について定量的な評価を行うことを目的としている。

本論文は「Security Evaluation of Public-Key Cryptography against Side-Channel Attacks and Quantum Attacks」（公開鍵暗号に対するサイドチャネル攻撃および量子攻撃の安全性評価）と題し、７章からなる。

第１章「Introduction」（序論）では、公開鍵暗号に対するサイドチャネル攻撃および量子攻撃の脅威と、本論文で提案する手法の暗号学的な意味について簡潔な説明を与え、本論文の構成について述べている。

第２章「Preliminaries」（準備）では、３章以降で必要となる、CRT-RSA暗号の実装法、Ring/Module-LWE暗号の実装法、Shorアルゴリズムの実装法に関する準備を与えている。

第３章「Improved CRT-RSA Secret Key Recovery Method from Sliding Window Leakage」（Sliding Window法における漏洩情報を用いたCRT-RSA秘密鍵復元手法の改良）では、Sliding Window 法で実装されたCRT-RSA暗号方式に対する秘密鍵復元手法の改良を行っている。まず、従来手法によって復元される秘密鍵のビット数について定量的な解析を行い、秘密鍵の各ビットの尤度に着目した新たな秘密鍵復元アルゴリズムの提案を行っている。既存手法と比較して、提案手法の方がより多くの秘密鍵が復元されていることを数値的に確認している。

第４章「Recovering CRT-RSA Secret Keys from Noisy Square-and-Multiply Sequences」（ノイズ付きSM時系列に基づくCRT-RSA秘密鍵の復元）では、Sliding Window法で実装されたCRT-RSA 暗号方式に対し、サイドチャネル攻撃によって得られるSM時系列がノイズ付きで得られる状況下での秘密鍵復元手法を提案している。これにより、CRT-RSA暗号方式の安全性評価を行っている。サイドチャネル攻撃で得られる実際の情報にはノイズが含まれているが、SM時系列のノイズを訂正する新たな手法を提案するとともに、多項式時間で訂正可能なノイズ量の定量的な解析を行っている。

第５章「Exact Security Analysis of the Ring-LWE and Module-LWE Based Schemes

against NTT Leakage」（数論変換からの漏洩情報に対するRing-LWE暗号およびModule-LWE暗号の正確な安全性評価）では、数論変換からの漏洩情報を用いた秘密鍵復元手法について正確な評価を行うことで、Ring/Module-LWE暗号方式の基盤となるLPR暗号の安全性評価を行っている。従来の解析手法では、近似的なアルゴリズムを用いており、正確な収束値が考慮されていないため、安全性評価が不十分である。本章では、正確な定量的評価を行うための漏洩モデルを設定したうえで、LPR秘密鍵が完全に復元可能となる情報の漏洩量について定量的な解析を行っている。

第６章「Security Evaluation of RSA Scheme under an Efficient Construction of a Quantum Controlled Modular Adder」（量子計算機上での効率的な制御付き剰余加算回路を踏まえたRSA暗号の安全性評価）では、RSA暗号方式への脅威であるShorアルゴリズムの効率化を行うとともに、RSA暗号の安全性評価を行っている。まず、制御付き剰余加算回路の回路構成を、現在利用されているNISQ計算機および将来の実現が期待されている耐故障性量子計算機のそれぞれについて最適化することで、効率的なShorアルゴリズムの構成法を提案している。さらに、量子計算機の発展計画に基づき、実際にRSA暗号で利用される典型的な鍵長に対して，解読までに要する時間および解読される時期に関する予測を与えている。

第７章「Conclusion」（結論）では、本論文の成果を簡潔にまとめている。

以上を要するに、本論文は、サイドチャネル攻撃に対する公開鍵暗号の安全性を定量的に評価する新たな手法を提案するとともに、量子計算機の現状を踏まえたうえで、量子攻撃の新たな効率化および将来予測を行っている。これらの成果は数理情報学分野の発展に貢献するところが大きい。

よって本論文は博士（情報理工学）の学位請求論文として合格と認められる。