審 査 の 結 果 の 要 旨

氏　名　　崔　　洋

本論文は、「Efficient Constructions and Provable Security of Public-Key Encryptions（公開鍵暗号の効率的構成法および証明可能安全性に関する研究）」と題し、情報通信の強秘匿性や個人情報の保護などを達成するために用いられる暗号技術について、安全性の不十分な公開鍵暗号を十分に高い安全性を備えた方式へ効率的に変換する方式の提案と、公開鍵暗号と共通鍵暗号を組み合わせてより強力な暗号を構成するハイブリッド暗号の提案、及び NP 問題に基づく暗号方式の解読と実験、改良を行っている。論文の構成は「Introduction（序論）」を含め 6 章からなる。

第 1 章は「Introduction（序論）」で、本研究の背景を明らかにした上で、現代暗号と情報セキュリティにおける公開鍵暗号の重大な意義を述べ、研究の位置づけについて整理している。

第 2 章は「Security Definitions（安全性定義）」と題し、本論文に必要である暗号学的安全性の諸概念を導入して明確な定義を示し、提案方式に用いられるプリミティブなど準備知識を説明している。特に、安全性が不十分である一方向性や、最強の安全性と言われる強秘匿性に関して、受動攻撃や能動攻撃のもとでのそれぞれの安全性を詳しく分析している。

第 3 章は「Efficient and Generic Conversions for Public-Key Encryptions（公開鍵暗号用の効率的かつ汎用的な変換方式）」と題し、受動攻撃にしか耐性を持たない公開鍵暗号方式から、能動攻撃に対しても強秘匿性を持ついわば「最も安全な」方式への変換法の具体的構成法を二つ提案している。公開鍵暗号において最強の安全性を満たすためには、元の暗号にランダムなパディング方式を組み合わせるのが有効な手法である。しかし実際には、理想的なランダムネスを利用するのは困難である。例えば、NIST により標準化されるなど高く評価されている最も有名な OAEP（最適化非対称暗号パディング）方式ですら、標準化当時に「最適」と強調したことが誤りである。すなわち、強力な攻撃を受けると、多数の冗長ビットが加えられない限り、安全性が損なわれる。また、冗長ビットの助けを受けたその安全性も、RSA 暗号を用いた時には保証されるが、それ以外の場合はほとんど保証されない。本章の新たな提案 1 においては、これらの問題を解決すると共に、ランダムネスの最適な汎用パディング方式を初めて提示している。さらに、この方式が理論的な限界を達成したことを証明し、結果として、最適な通信オーバーヘッドで暗号化することが一般的に可能であることを示している。また、提案方式 2 の変換方式では、量子アルゴリズムによる攻撃に耐える上で有望な公開鍵暗号にランダムなパディングの手法を用いて、特殊な復号攻撃に対する耐性を与えることに成功している。この結果は、将来のポスト量子公開鍵暗号として重大な意味を持つ。

第 4 章は「Efficient Hybrid Encryption（効率的なハイブリッド暗号）」と題し、公開鍵暗号と共通鍵暗号を組み合わせて効率を向上させる技法について、既存のフレームワークを分析し、新たなハイブリッド暗号方式を提案している。本章では、最近提案されたハイブリッド暗号のひとつの概念である Tag-KEM フレームワークに基づいて、最も効率のよい Tag-KEM を提案したものである。広く知

られている Bellare-Rogaway 方式が今回の提案の特殊な場合となっていることも示している。また、より弱い仮定の下で、ID ベース暗号を用いて、効率的なハイブリッド暗号とそのしきい値暗号の拡張を行っている。弱い仮定に基づく安全性証明も示されており、暗号理論の分野において大きなインパクトを持っている。

第 5 章は「Use of Public-Key Encryptions in Lightweight Cryptography（公開鍵暗号の軽量暗号への応用）」と題し、リソースが制限され軽量化が求められる環境において効率的に公開鍵暗号を応用する技術について、プロトコルの安全性分析と現実的で実行可能な改良方式の提案を行っている。具体的には、広く知られている Hopper-Blum 暗号プロトコルを解読する最も強力なアルゴリズムを提案し、包括的な解読攻撃実験を行い、その解読確率を見積もっている。また、リソースの制限された環境において、公開鍵暗号の手法を用いて実用的なプロトコルを提案し、しかも厳密な安全性証明を与えている。

最後に第 6 章は「Conclusion（結言）」で、本研究の総括を行い、併せて当該分野の将来展望について述べている。

以上これを要するに、本論文は、安全な公開鍵暗号の設計に必要な暗号強度評価のための安全性概念定義と変換方式などに関する証明を整備し、既存の暗号にはない実用上有意義な特徴をもつ安全かつ効率的な暗号の設計と、具体的な応用方式の構成を体系的に行ったものであり、電子情報学、特に情報セキュリティ工学上貢献するところが少なくない。

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。