審 査 の 結 果 の 要 旨

氏　名　　楊 鵬

本論文は「Provable Security of Identity Based Encryption and Application to Design of Efficient Schemes（IDベース暗号の証明可能安全性と効率的方式設計への応用）」と題し、証明可能安全なIDベース暗号技術について、安全性定義のフレームワークを提案するとともに、最上位秘密情報の安全性を考慮した前進守秘IDベース暗号方式や自然な数学的仮定に基づく信頼性の高いIDベース暗号方式など多様な暗号方式の具体的構成を示しており、さらに効率的な安全性強化手法や効率的鍵カプセル化メカニズムなど完成度および汎用性の高い理論的枠組みを示している。論文の構成は、最初の「Introduction」と最後の「Conclusion」を含め、6章からなる。

第1章は「Introduction（序論）」と題し、本研究の背景を述べ、研究の位置づけを明らかにしている。本章では、IDベース暗号の関連研究について整理し記述している。更に本論文の第2章以降に使われる記号や暗号要素技術などを記述している。

第2章は「Framework of Security Notions（IDベース暗号の安全性定義のフレームワーク）」と題し、IDベース暗号の安全性定義の統合的なフレームワークを提案している。具体的には、情報漏洩対策に関する到達レベルの軸、攻撃対象IDに対する攻撃モデルの軸、平文・暗号文に対する攻撃モデルの軸という三つの軸でIDベース暗号の安全性定義の枠組みを立体的に定義・整理し、更に全ての安全性定義の間の含意関係を明確にし、厳密に証明している。このフレームワークは、第3章以降の研究成果を支えるのみならず、IDベース暗号の安全性理論の基盤となっている。

第3章は「A Forward Secure Scheme with Master Key Update（マスター鍵更新可能な前進守秘IDベース暗号）」と題し、時間が進むとマスター鍵が自動的に更新される前進守秘性の概念と具体的な実現方式を提案している。実際、従来方式では、IDベース暗号の最上位秘密情報であるマスター鍵が固定されており、このマスター鍵が漏洩すれば全システムが破綻してしまう。本章では、その対策としてマスター鍵の自動更新という斬新な概念を提唱している。さらに、提案した具体的な方式は、所望の前進守秘性を達成するだけでなく、より自然な仮定に基づいて安全性証明が可能な方式となっており、暗号理論的に完成度が高い。

第4章は「Means of Security Enhancement（IDベース暗号の安全性強化手法）」と題し、任意の最強ではないIDベース暗号方式に最強な安全性を付与する一般的安全性強化手法の提案と、その評価を行っている。ここで、任意の最強ではない方式とは、第2章で示された含意関係の中で最強の安全性となっている安全性定義とは異なる安全性定義しか満たしていない方式を指し、第3章の提案方式もその一例である。すなわち、本章で示した強化手法により、本論文の異なる章が有機的に結びついてより大きな理論体系をなすことを示唆している。本章の二つ目の成果は、最先端の評価フレームワークを使用し、適切なパラメータマトリクスを選択し、強化手法の定量的な評価も行ったことである。その結果、提案手法によって強化された暗号方式は、計算量に関して既存研究の５倍以上効率的であることが明らかになった。

第5章は「On Design of Efficient Schemes（効率的なIDベース暗号方式の設計）」と題し、ステートフルIDベース暗号という考え方で大幅な高速化を図っている。本章では、IDベース暗号のアーキテクチャ改造に着目し、乱数の再利用で高速化をもたらすIDベース・ステートフル鍵カプセル化メカニズムの概念を提案し、さらに他の暗号要素技術との間で一般的変換法を提案している。しかも、より自然な数学的仮定に基づいて安全性を証明し、極めて信頼性の高い具体的構成方法を示している。本章の研究成果により、第2章から第4章までの方式を含め、ほぼすべての既存のIDベース暗号方式を高速化できる。加えて、IDベース暗号以外の従来の公開鍵暗号の中にも本章のアプローチの適用対象があることを論じ、提案のインパクトの大きさを示している。

第6章は「Conclusion（結言）」と題し、本研究の総括を行い、併せて今後の課題や将来展望などについて述べている。

以上これを要するに、本論文は、単に完成度の高いIDベース暗号方式を個別に提案するだけでなく、より自然な仮定に基づく証明可能安全性を中心とした信頼性の向上を目指し、自ら体系化したIDベース暗号の安全性定義のフレームワークに基づいて統一して取り扱うことが可能な多様な新たなIDベース暗号方式構成、強化手法、高速化手法および諸性質について論じた論文であり、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。