審査の結果の要旨

氏　　名　　大畑 幸矢

本論文は、「Provable Security of Applied Public Key Cryptosystems and Heuristically Secure Protocols （高機能公開鍵暗号技術と経験的なセキュリティプロトコルの証明可能安全性）」と題し、高度な機能を伴い情報保護や信頼構築のための複雑な要件を満たす公開鍵暗号技術と情報セキュリティのプロトコルに関して、多様な方式を提案するとともに、システムの安全性評価に関する新たな枠組みを開拓する理論と実装を示している。論文の構成は「Introduction」を含め７章からなる。

第１章は「Introduction（序論）」で、本研究の背景として情報セキュリティにおける厳密な安全性評価の重要性と証明可能安全性について述べ、研究の位置付けを明らかにしている。とくに、暗号技術においてはその安全性モデルを適切に設定することが重要であること、および、経験的な安全性評価しかされていない情報セキュリティ技術に対しては証明可能安全性の導入に大きな意義があることが、明らかにされている。

第２章は「Preliminaries（準備）」と題し、安全性証明の対象とするシステムを構成する暗号要素技術とその諸性質の定義、さらに、証明の帰着先となる数論仮定について記述している。

第３章は「Re-splittable Threshold Public Key Encryption（鍵再分割可能な閾値公開鍵暗号）」と題し、復号権限を分割可能な閾値公開鍵暗号に鍵再分割可能性と呼ばれる性質を持たせた高機能公開鍵暗号技術について論じている。とくに、鍵再分割可能性によって公開鍵を変更せず分割秘密鍵のリフレッシュが可能になり実用的な安全性の向上に寄与することが説明され、４つの方式が提案されている。これらは、アルゴリズムの効率や、安全性の根拠となる数論仮定が全て異なり、効率と仮定の強さの間にトレードオフが存在することが示され、具体的な設計の指針となる評価結果が体系的にまとめられている。

第４章は「Proxy Re-encryption with Re-encryption Verifiability（再暗号化検証可能な代理再暗号化技術）」と題し、暗号化したまま宛先を変更可能という性質を持つ高機能公開鍵暗号技術である代理再暗号化技術において、代理人が再暗号化作業を正しく行ったかどうかが検証可能な方式について論じている。第３章の成果を要素技術として利用する一般的構成である方式を提案し、再暗号化検証可能性を含む厳密な安全性定義と安全性証明の理論を展開して実践的な安全性向上に貢献するだけでなく、それら一連の理論が、従来は未統一であった様々な安全性定義を包含するという意味で暗号学的体系化に貢献することを明らかにしている。

第５章は「Proxy Re-encryption from Indistinguishability Obfuscation（識別不可

性難読化器に基づく代理再暗号化技術）」と題し、識別不可性と呼ばれる安全性を満たす難読化器を構成要素に用いた代理再暗号化技術について論じている。提案している方式は、実用に耐える効率は持っていないが、再暗号化が一方向にのみ可能で、かつ複数回再暗号化が可能という性質を持つ最初の方式である。また、再暗号化によって暗号文の大きさが増大しない、復号を高速にできる、などの長所を有する。

第6章は「Provably Secure Password Reset Protocols（証明可能安全なパスワード再発行プロトコル）」と題し、これまで安全性評価が経験的にしかなされてこなかったパスワード再発行プロトコルに証明可能安全性を導入し、実際に厳密な安全性証明を伴うプロトコルを提案している。パスワード再発行のための鍵を適切に管理することが求められるという制約があるものの、モデルと安全性の定式化に始まる理論を展開する先駆的な理論研究としての貢献と、プロトタイプ実装による性能評価を示す実践的な研究としての貢献とを併せ持ち、システムセキュリティに新たな潮流を起こす内容となっている。

最後に第7章は「Conclusion（結言）」で、本研究の総括を行い、併せて将来展望について述べている。

以上これを要するに、本論文は厳密な安全性評価手法である証明可能安全性を高機能公開鍵暗号技術とセキュリティプロトコルの両面で論じたものであり、前者では安全性モデル修正の繰り返しから脱却するための完成度の高さにより、後者では経験的な安全性評価から脱却するための先駆的な技術の開拓により、そして両者合わせて情報セキュリティ工学に極めて有益な将来展望を与えることにより、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。