審 査 の 結 果 の 要 旨

氏　　名　　シュルツ　ヤコブ

本論文は「Security Models and Provable Security of Enhanced Signature and Signcryption Schemes（高機能な電子署名及びサインクリプションの安全性モデルと証明可能安全性）」と題し、社会の様々な機能の高度なデジタル化に貢献する電子署名技術、とくに、拡張された機能を持つという意味で高機能な電子署名技術について、効率だけでなく安全性モデルの観点および安全性証明を実用上望ましい仮定に基づかせるという観点で完成度の高い方式を具体的に提案し、厳密に評価している。論文の構成は、「Introduction（序論）」と「Tools and Definitions（諸定義）」を含め、７章からなる。

第1章は「Introduction（序論）」で、本研究の背景と動機を述べ、成果の概要をまとめている。とくに、電子署名の検証可能性を制御する二種類の機能、署名発行の権限を委譲する機能、メッセージの秘匿性を同時に効率的に提供する機能を拡張機能としてそれぞれ概説し、完成度の高い証明可能安全性とともに、意義を明らかにしている。

第2章は「Tools and Definitions（諸定義）」で、暗号理論における証明可能安全性を一般的に説明するほか、拡張機能を持たない基本的な電子署名、安全性の根拠となる計算困難性の仮定などを厳密に記述している。

第3章は「Undeniable Signature（否認不可署名）」と題し、電子署名の検証可能性を柔軟に制御できる変換可能否認不可署名を探究している。否認不可署名では、署名発行者の意図する時に意図する第三者しか署名を検証してその署名と署名者を関連づけることができない、という制御機能が実現される。変換可能否認不可署名では、発行済みの否認不可署名から署名者がこの制御機能を解除するという変換が可能である。本章ではまず、変換可能否認不可署名に本質的に必要であるにもかかわらず見過ごされてきた安全性要件を捉えた新しい安全性モデルを提案している。そして、この安全性モデルの下で証明可能安全性を持つ効率の良い方式を具体的に構成している。提案方式では、変換可能否認不可署名を最初に示した論文では実現されていたにもかかわらず後発の多くの論文では見過ごされてきた機能、すなわち、信頼性が不完全な第三者へ署名者が変換権限を委譲できる機能も実現されている。しかも、ハッシュ関数に過度の仮定を設けない標準モデルにおいて安全性証明可能な方式の中で最も効率がよいという意味で完成度が高く、検証者指定署名など他の拡張機能を実現する基礎になるという意味で構造が柔軟性に長けている。

第4章は「On-line Non-transferable Signatures（オンライン転送不可署名）」と題し、本論文の定義では機能と安全性要件の両面で変換可能否認不可署名の一般化と見なせる電子署名技術を取り上げている。オンライン転送不可署名では、署名者が検証者との接続を拒むなどして署名検証を阻むことができるほか、阻む前の通信を悪用する強力なオンライン攻撃に対する安全性も提供される。既存研究は、機能、安全性、効率を限定的にしか提供できないため実用性に乏しかった。本章では、オンライン転送不可署名方式の一般的構成手法を提案してから、標準モデルで安全性証明可能な効率的方式の構成方法を示している。さらに、前章で提案した否認不可署名の一方式を部品として用いた具体的な方式を与えている。こうした体系的アプローチにより、オンライン転送不可署名において初めて機能、安全性、効率を揃えることに成功した。

第5章は「Proxy Signature（代理署名）」と題し、署名の生成権限を代理人へ移譲できる機能を持つ電子署名技術を、場合によっては委譲される権限を限定することすらできる形で、探究している。代理署名は、高機能電子署名の中でもとくに幅広い応用が期待されているにもかかわらず、近年まで証明可能安全性が研究されていなかった。本章では、実際の脅威分析に基づいた安全性モデルを明らかにし、このモデルにおいて安全性証明可能な一般的構成法を提案している。この提案は、通常の公開鍵基盤における公開鍵の代わりに署名者のIDを検証鍵として用いることができるタイプの技術へと拡張できる。

第6章は「Signcryption（サインクリプション）」と題し、メッセージの秘匿性を同時に効率的に提供する技術の構成法を議論している。否認不可性の観点で前章までの電子署名技術とは一線を画し、効率性も機能要件に入ることから、サインクリプションという独立した名称の要素技術として扱われている。本章では、いくつかの枠組みのもとで最適化する理論を示し、従来は整理不十分であった様々なレベルの安全性を持つ効率的なサインクリプション方式につなげている。さらに、構成要素が特定の構造を持つサインクリプションの構成可能性理論という体系的アプローチを編み出し、標準モデルで最も強い安全性を達成しかつ最も効率的なサインクリプション方式を具体的に得ている。

第7章は「Conclusion（結論）」で、本研究の総括を行い、併せて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、高機能な電子署名及びサインクリプションに関して、安全性モデルから掘り起こすアプローチで高い効率と安全性を両立させつつ所定の拡張機能を達成する具体的構成を示し、完成度の高さで実用上の意義を大きく高める成果として体系的にまとめた論文であり、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。