審査の結果の要旨

論文提出者氏名　　花岡 悟一郎

本論文は「Unconditionally Secure Cryptosystems, Authentication Schemes and Their Applications （情報量的に安全な暗号・認証方式およびその応用に関する研究）」と題し，正しく鍵管理がなされる限りいかなる攻撃者も決して破ることができない暗号技術を提案し，その安全性および必要となる記憶容量に関する厳密な特性を明らかとするとともに，実運用における有効性の検証を行ったものである．これにより，従来の暗号技術においてなしえなかったような長期にわたる安全性を達成するとともに，現実的に許容できる容量の記憶装置を用いてこのような安全性をもつ暗号技術を実現できることを示している．論文の構成は「論文の概要」を含めて８章からなる．

第１章は「Overview of This Thesis （論文の概要）」で，本研究の背景を明らかにした上で，研究の動機と目的について言及し，研究の位置付けについて整理している．

第２章は「Unconditionally Secure Signatures Admitting Transferability （情報量的に安全な電子署名方式）」と題し，長期的な安全性が要求される場合においては，現在通常利用されている電子署名方式では十分な対応が困難であることを明確にし，いかなる計算能力をもつ攻撃者であっても決して破ることができないことが証明可能な電子署名方式の提案を行っている．また，同方式を実装するうえで必要となる記憶容量についても明らかにし，その有用性について考察している．

第３章は「Unconditionally Secure One-Time Signatures （情報量的に安全な One-Time 署名方式）」と題し，電子署名の発行回数に関する条件を緩めた場合，第２章において提案されて方式と比べて非常に少ない記憶容量のみを用いて同等の安全性が実現可能であることを示している．併せて，Safavi-Naini と Wang によって提案された認証方式に対する攻撃方法を示し，同方式においては他者へのなりすましが容易であることを明らかにしている．また，その修正方法も示している．

第４章は「Hierarchical Key Predistribution Systems （階層的鍵事前配送方式）」と題し，既存の情報量的に安全な鍵配送方式である Key Predistribution Systems(KPS)の改良方法を提案し，放送通信などの通信形態において，従来の KPS に比べ必要となる記憶容量を大幅に削減することが可能であることを明らかにした．

第５章は「Optimization of Unconditionally Secure Key Distribution Schemes for Large Scaled Networks （大規模ネットワークにおける鍵事前配送方式の最適化）」と題し，第４章にて提案を行った KPS の改良手法を一般化し，併せて情報理論を用いた考察により大規模ネット

ワークにおいて KPS を利用する際必要となる記憶容量の理論的な下界を導出し提案方式が記憶容量に関して最適であることを明らかにしている．

第 6 章は「Electronic Toll Collection Systems Based on Optimized Key Predistribution Systems（最適化された KPS を応用した有料道路料金自動収受システム）」と題し，KPS を用いた効率的な有料道路料金自動収受システム（ETC）のためのプロトコルを設計し，ETC の利用における同プロトコルの有用性を示すとともに，第 4 章および第 5 章において提案を行った KPS の最適化手法を応用することで利用者の保持する秘密情報に必要となる記憶容量に関しさらなる大幅な効率化が図れることを明らかとした．

第 7 章は「Traitor Traceable Conference System with Dynamic Sender （不正漏洩者追跡可能な会議方式）」と題し，多数の参加者が存在する暗号通信において不正な参加者が通信内容を漏洩させた場合，この不正な漏洩者を特定可能な情報量的に安全な暗号方式の提案を行っている．併せて，同暗号方式を利用する際に適した認証方式を提案している．これらの方式に関し，いずれも安全の証明が示されている．

第 8 章は「Unconditionally Secure Asymmetric Encryption and Authentication Code （情報量的に安全な非対称暗号およびグループ認証）」と題し，情報送信者の匿名性を重視した暗号・認証方式の提案を行い，また，情報理論より導かれるさまざまな理論的な下界を導出し，提案した方式が記憶容量に関して最適であることを示している．これらの方式に関し，いかなる計算能力をもつ攻撃者に対しても安全であることが証明されている．

以上これを要するに，本論文は，情報量的に安全な暗号・認証方式の基礎理論を確立するとともに，その効率的な実現手法および実運用性を明示したものであり，情報セキュリティ工学，特に暗号研究分野において貢献するところが少なくない．

よって本論文は博士（工学）の学位請求論文として合格と認められる．