審査の結果の要旨

論文提出者氏名　　大塚 玲

本論文は「Unconditionally Secure Electronic Cash(情報量的に安全性な電子現金方式に関する研究)」と題し、究極的な安全性である情報量的な安全性と情報量的な匿名性を同時に実現できる電子現金方式の構成法と、その実現にあたっての基礎となる情報量的な安全性に基づく種々の暗号プリミティブの構成法を示している。本論文は「Introduction」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, 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「Hybrid Approach: Combination with Computational Assumption(計算量的仮定との融合方式)」と題し, 情報量的に偽造が難しく、計算量的に匿名性が守られるハイブリッド型電子現金方式の構成法を示している。本方式は花岡、四方、鄭、今井らによって考案された情報量的な安全性に基づく署名方式を基礎に、Decisional Diffie-Hellmann問題(以下、DDH)が計算量的に解けないという仮定を導入し、この仮定の下で支払いの匿名性、すなわち電子現金の追跡不能性を実現する手法を提案している。

第3章は「Robust Verifiable Secret Sharing(ロバストな検証可能秘密分散法」と題し, 過半数のプレイヤーが不正でかつ無限の計算力を持つ場合においても正しく動作する安全な検証可能秘密分散法の構成法を示している。この成果は鍵事前配布モデルに基づくことで、従来は計算量的な仮定を置かなければ実現不可能だったロバストネスを計算量的な仮定なしに満たす手法を示している。さらに、提案方式は各利用者が 1,000 人規模で秘密を保持するような規模のアプリケーションを想定した場合に、各利用者は約 20MB の秘密鍵を保持する必要があるが、通信量や計算量は低く、現在の技術水準でも十分に実用的である。

第4章は「Robust Multiparty Computation(ロバストなマルチパーティ計算)」と題し, 鍵事前配布モデルに基づくことにより、過半数のプレイヤーが不正でかつ無限の計算力を持つ場合においても正しく動作する安全なマルチパーティ計算プロトコルの構成法を示している。マルチパーティ計算は、複数のプレイヤーで事前に決められた任意の計算を実行し、その際に各プレイヤーの入力と出力が他のプレイヤーから秘匿される特徴を備える暗号プロトコルである。提案手法は、従来計算量的な仮定を置かなければ実現できなかったロバストネスを計算量的な仮定なしに実現する手法を与えている。必要な秘密鍵のサイズも 100 人規模で、1,000 程度の積演算を含むマルチパーティ計算の場合であれば数百 MB であり、規模の小さいアプリケーションを選べば十分に実用可能と認められる。

第5章は「Unconditionally Secure Electronic Cash(情報量的に安全な電子現金方式)」と題し、情報量的に安全かつ情報量的に匿名性が保護される電子現金方式の構成法を示している。提案手法は (1) 無限の計算能力を持つ不正利

用者が存在しても電子現金の偽造は不可能であり、(2) 無限の計算能力を持つ組織が存在しても、個人の支払いに関するプライバシーが完全に保護される、という特徴を持つ。提案方式は、情報量的に安全な署名方式と前章のロバストなマルチパーティ計算に基づいて構成されており、コインの偽造に関する情報量的な安全性と、マルチパーティ計算の入出力に関する秘匿性を利用して電子現金の偽造不能性と匿名性を同時に実現している。

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，情報量的な安全性に基づく暗号理論に関する基礎検討を行うとともに，重要な暗号プリミティブと電子現金方式の構成法を明示したものであり，電子情報工学，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(工学)の学位請求論文として合格と認められる.