# 審査の結果の要旨

論文提出者氏名　　阿部　正幸

本論文は「Efficient Components for Cryptographic Applications in the Discrete-Log Setting（離散対数問題に基づく暗号アプリケーションの効率的な構成要素に関する研究）」と題し，電子現金，電子投票などの高度な暗号アプリケーションにおいて頻繁に要求される，匿名性，秘匿性，分散計算性を提供する独立した4つの構成要素に対して①安全性要件の定式化，②効率的な方式の提案，③安全性の厳密な評価，といった観点から検討している．高度な暗号アプリケーションを構成するには，匿名性と相手認証の両立など，一見不可能とも思われる安全性の要件を満たす構成要素の開発が不可欠である．そのため，各構成要素に対する複雑な安全性要件をどのように定式化するかを検討し，それを満たす安全な方式が構成可能であることを示すと共に，妥当な仮定の下で十分な効率を達成することが実用上重要である．本論文は，これらの問題に対する有効な解決策を示したものであり，「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「Preliminaries（準備）」で，以下の各章で用いる基本的な計算モデル，証明技法，暗号技術について説明している．

第3章は「Partially Blind Signatures（部分ブラインド署名）」と題し，電子現金等において利用者に匿名性を提供しつつ，署名者が自らの署名を効率的に管理できる手法を示している．従来知られているブラインド署名では，署名者（銀行）は発行した署名（銀行券）に関する情報を一切得られないため，署名に有効期限を設けることができないなど，署名の流通を効率的に管理する手段がなかった．本章では，有効期限などの特定の情報が署名に含まれることを署名者と利用者の双方が確認できる，部分ブラインド署名という新しい署名のクラスを提唱し，安全性要件の定式化を行うとともに，効率的な方式を具体的に示して，その安全性の検証を行っている．

第4章は「Mix-net（ミックスネット）」と題し，匿名性のないネットワーク上で，分散した複数台のサーバの協調により，実質的な匿名通信路を実現する手法を示している．ミックスネットは，無記名電子投票において各投票者から送信された多数の投票文をシャッフルする場合などに利用できる．n 入力に対して，各サーバが正しく動作したことを検証する為の計算量は，単純には $n^2$ オーダとなるため，その効率化が技術的課題である．本章では，検証者の計算量がサーバの数と独立となるよう低減する手法および，各サーバにおける計算量を $n \log n$ に低減する手法をそれぞれ示し，それらの安全性を検証している．

第5章は「Encryption with a Proof of Knowledge（知識の証明を用いた公開鍵暗号）」と題し，知識の証明を利用して暗号の強度を高める方法を示している．

一方向性のみが保証されている弱い暗号を，適応的選択暗号文攻撃の下で識別不可能性を保証する強い暗号に変換する方法として，暗号文中に含まれる平文に関する知識の証明を利用する方法が知られているが，その安全性は非常に強い仮定に基づいている．本章では，より弱い仮定に基づいて安全性の証明が可能である手法を示し，その安全性を詳細に評価している．

第6章は「Non-interactive Distributed Multiplication（非対話的分散乗算）」と題し，複数のプレイヤーに秘密分散された2つの値の積を秘密分散する効率のよい手法を示している．この分散乗算と呼ばれるプロトコルを効率よく構成することは一般的マルチパーティーコンピュテーションにおける中心的課題である．1/2 未満のプレイヤーの不正に対して頑健性を持つ方式は、離散対数問題などの標準的な計算量的仮定に基づく構成では少なくとも 4 交信、より強いランダムオラクル仮定に基づく構成でも3交信の対話がプレイヤー間で必要であった．本章では，離散対数問題に基づき，プレイヤー間の対話が1交信に最適化できる手法を示している．

各章で示された手法は，いずれも離散対数問題の困難性に基づいて構成されている．そのため，同様の仮定に基づく多数の従来技術と組み合わせて利用することが可能であり，匿名性や秘匿性、あるいは一般的な分散計算を必要とするアプリケーションの設計の効率化に寄与する．

以上これを要するに，本論文は，暗号アプリケーションに対して，従来にない機能や，より高い安全性あるいは効率を提供する構成要素を具体的に明示し，それらの安全性について厳密な評価・検討を行ったものであり，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．