審 査 の 結 果 の 要 旨

氏　　名　　古川　　潤

本論文は、「Efficiency Enhancement of Secure Multi-Party Protocols for Privacy and Privilege Protection (プライバシーと権限を守るための安全な多者間プロトコルの効率化に関する研究)」と題し、複数の重要な多者間プロトコルに対して、その安全かつ効率的な構成方法を提案している。論文の構成は「Preliminaries（序論）」を含め、9 章からなる。

第 1 章は「Preliminaries（序論）」である。本研究の背景を明らかにした上で、代表的な多者間プロトコルである mix-net（ミックスネット）、broadcast encryption （放送型暗号）、及び group signature（グループ署名） の概要と、それらの有効な応用先が述べられている。特に、ミックスネットは安全な電子投票の実現に欠かせないこと、放送型暗号は著作権のあるコンテンツの放送や記録メディアによる配布に有効な手段を与えることが述べられている。その後に、これらの効率的な具体的方式を構成することの難しさと、その重要性が整理されている。

第 2 章は「Publicly Verifiable Shuffle, Shuffle and Decryption（第三者検証可能なシャッフル、シャッフルと復号）」と題し、第三者検証可能な効率的なシャッフルプロトコル、および、シャッフルと復号を併せたプロトコルの提案を行っている。シャッフルはミックスネットの中核となるプロトコルであるため、ひとえに本プロトコルが効率的に構成できるかによって、安全な電子投票を現実的な時間で実行できるかどうかが決まる。本章では、従来の方式と比べて最大で 50 倍程度の効率化を達成することにより、初めて安全な大規模電子投票の実行に現実性を持たせた方式を提案している。

第 3 章は、「Hybrid Mix-net （ハイブリッド　ミックスネット）」と題し、暗号文の長さが長い場合においても、第 2 章にて提案されたシャッフルを用いたミックスネットと同程度の効率を持つミックスネットを提案している。選挙などでは候補者を指定するに十分な長さを持つ暗号文を扱えれば十分であるが、匿名性を保ちかつ集計の正当性を保証するアンケートを実施する場合には、長い暗号文を扱える第三者検証可能なミックスネットが必要となる。従来はこのような方式は提案されていなかった。本章では、第 2 章で提案した方式を発展させて、多重暗号と組み合わせることにより、効率的かつ第三者検証可能で、しかも任意の長さの暗号文を扱えるミックスネットを提案している。本提案は、ミックスネットの応用範囲を大きく広げる効果を持っている。

第 4 章は、「Aggregate Shuffle Argument Scheme（統合的シャッフル証明方式）」と題し、ミックスネットの正当性を検証する第三者の計算コストが、ミックスネットを構成するミキサーの数に依存しない方式を提案している。ミックスネットは、複数のミキサーと呼ばれる参加者が、順番に暗号文の集合をシャッフルすることで成り立っており、その匿名性はミキサーの数が多いほど高くなる。しかし、従来は、ミキサーの数が増えると検証コストが高くなる方式か、少数ミキサーですら検証コストの高い方式しか知られていなかった。本章では、ミキサーの数と無関係に、検証者のコストが第 2 章のシャッフルの検証者と同程度にとどまる方式を提案している。本方式は、より安全性の高いミックスネットの実現を容易にする効果を持つ。

第 5 章は、「Compiler from Σ-Protocol to Deniable Zero-Knowledge（Σ-プロトコルから否認可能零知識証明へのコンパイラ）」と題し、一般のΣ-プロトコルからその効率をほとんど落とすことなく否認可能零知識証明を構成する方法を与えている。電子投票において、その効率の悪さ以外で最も実用化の障害となる問題は、票の売買が容易となることである。これを防止するために、投票者が誰に投票したかを証明できなくする必要がある。これは、一般に否認可能性と呼ばれる性質である。本章では、この否認可能性を持ちかつ効率的なプロトコルを容易に構成する一般論を与えた。

第 6 章では、「Black-Box Traitor Revocable Broadcast Encryption with Short Private Keys（短い個人鍵による、ブラックボックス不正者失効可能放送型暗号方式）」と題し、放送型暗号方式で、その受信者が復号装置の海賊版を作った場合に、その海賊版とブラックボックス的に相互作用することにより、以降この海賊版の復号装置が放送型暗号文を復号できなくさせる方法を提案している。本方式では、潜在的な受信者全ての数を N としたとき、暗号文の長さが N の平方根、許される不正者の数が N、各受信者のもつ鍵の長さが定数である。これは、世界で初めて達成された画期的な効率である。

第 7 章では、「Group Signature for Separate and Distributed Authorities（分割かつ分散した権限者を実現するグループ署名方式）」と題し、メンバーの追加権限とメンバーの追跡権限を独立させて異なる権限者に付与することが可能で、さらに各権限者を効率的に分散することが可能なグループ署名を提案している。

第 8 章では、「Group Signature from Bilinear Mappings（双線形写像を用いたグループ署名）」と題し、双線形写像を用いることで、署名の生成および検証に必要な計算量が少なく、署名長が小さいグループ署名方式を提案している。第 7 章の成果とともに、多くの多者間プロトコルでの応用が期待できる。

最後に第 9 章は、「Conclusion（結言）」で、本研究の総括を行い、併せてその意義を述べている。

以上これを要するに、本論文は、ミックスネット、放送型暗号、グループ署名と、代表的かつ有用な多者間プロトコルの安全かつ効率的な実現方法を具体的に示したものであり、これらの技術は上記プロトコルを現実に利用していく道を開いており、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。