論文の内容の要旨

論文題目　Unconditionally Secure Electronic Cash
（情報量的に安全な電子現金方式に関する研究）

氏　名　　大塚　　玲

現代暗号は計算量的な困難性に基づくことで、ネットワーク社会を形成する上で欠くことのできない多くの有益な暗号技術を生み出してきた。電子現金方式も現代暗号の重要な成果の一つであり、将来のネットワーク社会のインフラストラクチャを担う技術として期待されている。しかし、情報技術の驚くべき進展と量子コンピュータの出現により、特に10年以上の長期的な安全性が求められるアプリケーションでは、すでに計算量的な安全性では不十分なことが指摘されている。従って、計算量的な困難性に代わる新たな理論的枠組みが必要となりつつある。

本博士論文の主な目的は、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実現を目標に置くことで、個々のプロトコルに要求される課題を発見し、それらの解決を通じて、最終的な目標である情報量的な安全性に基づく暗号理論の体系化に近づくことにある。

本研究の第一の成果は、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存在を初めて示したことにある。既に情報量的に匿名で、かつ計算量的に偽造が難しい電子現金方式は存在しており、本成果はその双対に位置づけられる。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、Descional 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した方式である。但し、情報量的な安全性を実現するために、極めて複雑な計算を実行する必要があるため現在の情報技術では実用的ではない。本成果は博士論文の第二章にまとめられている。

第二の成果は、情報量的に安全な非交信型の検証可能な秘密分散方式(Non-interactive Verifiable Secret Sharing)の存在を示したことにある。従来から情報量的に安全な交信型秘密分散方式と、計算量的に安全な非交信型秘密分散方式は存在した。交信型秘密分散方式では、各利用者に分散保持された秘密の正当性確認を他の利用者との交信によって実現し、これによって分散保持された秘密の全体的な一貫性が保証される方式である。この種の方式はブロードキャスト通信路が存在する仮定の下で、半数以上の利用者が正しく振る舞う場合に機能することが証明されている。他方、計算量的な安全性に基づく非交信型秘密分散方式は、秘密の正当性確認は利用者が単独で行える方式である。従って、非交信型秘密分散方式では過半数が不正利用者の場合でも、分散保持された秘密の全体的な一貫性を保

証できる特徴がある。ただし、従来の手法では、各利用者の計算能力は多項式時間で抑えられる必要があった。本成果は、鍵事前配布モデルに基づくことで、情報量的な安全性を保証した上で、非交信型の秘密分散方式を初めて実現した。これにより、過半数の利用者が不正かつ無限の計算能力を持つ場合にも正しく動作させることが可能である。さらに、提案方式は各利用者が1,000人規模で1000個の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、各利用者が数 GB 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。本成果は博士論文の第三章にまとめられている。

第三の成果は、情報量的に安全かつ過半数の不正利用者に対応したマルチパーティ計算プロトコル(Multiparty Computation)の存在を示したことにある。マルチパーティ計算プロトコルは、n人の利用者がそれぞれ秘密の入力 Xi を持ち、あらかじめ定められた関数F(X1,X2,...,Xn)を実行するプロトコルである。ここで関数Fは任意の計算可能関数である。ただし、個々の利用者の入力Xiと出力Yiに関する情報は他の利用者には一切漏れない。従って、マルチパーティ計算プロトコルが存在すれば、複数の利用者で実行されるすべてのプロトコルが存在することになる。従来の方式は、検証可能秘密分散方式の場合と同じくブロードキャスト通信路が存在する場合に、半数以上の利用者が正しく振る舞う場合にマルチパーティ計算プロトコルが実現できることが知られている。また、計算量的な仮定である Oblivious Transfer の存在を仮定すれば、過半数が不正利用者の場合でも、マルチパーティ計算プロトコルが存在することが知られている。本研究の成果は、鍵事前配布モデルに基づくことにより、過半数が不正利用者の場合でも、情報量的に安全なマルチパーティ計算プロトコルが存在することを示したことにある。さらに、本成果は前述の非交信型の検証可能な秘密分散方式を利用しているため、従来の情報量的に安全な方式が$O(n^4)$の通信量を必要としたのに対して、本方式では$O(n^2)$の通信量で情報量的な安全性を実現している。本方式を1,000人規模で利用し、1,000程度の積演算を含むマルチパーティ計算を実行するようなアプリケーションを想定すると、各利用者が保持するべき秘密鍵のサイズは数十 GB になり、現在の技術水準ではやや実用性に欠ける。但し、利用者数を 100 人規模にした場合には、秘密鍵のサイズは数百 MB に抑えられる。本研究の成果は、博士論文の第四章にまとめられている。

最後の成果として、本研究では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存在を示した。ここで示した方式は、(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。ここで示した方式は、前述のマルチパーティ計算プロトコルと情報量的に安全な署名方式を組み合わせることによって実現されている。具体的には、マルチパーティ計算プロトコルの特別な場合として、2-パーティ計算プロトコルを構成し、関数F(x1,x2)として情報量的に安全な電子署名方式の署名関数を設定し、利用者1の入力にはコインのシリアル番号を入力し、利

用者２（銀行）の入力には署名用秘密鍵の情報を入力し、利用者１の出力に銀行のデジタル署名を出力する。マルチパーティ計算プロトコルの特徴により、利用者１の得たコインのシリアル番号と署名は、利用者２（銀行）から情報量的に隠蔽される。従って、このコインを使用しても、利用者２（銀行）はコインの利用者を追跡することは情報量的に不可能である。