論文の内容の要旨

論文題目： 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)

氏　　名： 阿部　正幸

電子現金や電子投票のような高度なネットワークアプリケーションを設計するには、それらが要求する一見不可能とも思えるような安全性の要件を満たす先進的な暗号方式や暗号プロトコルを開発することが不可欠である。計算に関するどのようなタスクもマルチパーティーコンピュテーションによって、情報理論的あるいは計算量的に安全に実行できることが理論的には知られているが、そのような一般的な解決法が個々の実用的なアプリケーションに要求される効率を満たすことは少ない。従って、暗号研究においては、厳密な安全性と同時に実用的な環境における実現可能性と効率を追求することが望まれる。

本研究の目的は、様々な暗号アプリケーションの設計に役立つ新しい機能や概念を考案し、それを効率よく実現する具体的な方法を開発することである。暗号アプリケーションを構成する要素は、秘匿や認証といった単一の機能を提供する低位のものから、その利用形態がアプリケーションに直結する高度な要素まで、様々である。本研究では、比較的高位の要素として、利用者の匿名性に関する機能を提供するものと、比較的低位の要素として、データの秘匿性に関する機能を提供する、以下の具体的な構成要素の定式化、構成、安全性の検証に取り組む。

- 部分ブラインド署名： ブラインド署名は電子現金等で利用者の匿名性を確保するために用いられる署名方式である。通常の署名行為においては、署名対象文書中に有効期限などの情報を明示的に含めることが可能であるが、ブラインド署名では署名者は署名対象文書に関する情報を一切知り得ないため、署名の有効性や流通性を効率的に制御することができない。この問題に鑑み、本稿では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、効率的な部分ブラインド署名方式の具体的な構成を示し、その安全性の検証を行う。部分ブラインド署名では、署名者と署名要求者の合意の下で、予め定めた属性を示す一定のビット列が署名対象文書の一部

に含まれることを、署名者が確認できる署名方式である。この方式によって、署名者は署名要求者の匿名性を侵害することなく、発行する署名に一定の属性を付与して、署名の有効性、流通性を効率よく制御することが可能となる。

- 全体検証可能なミックスネット：ミックスネットは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、実質的に匿名通信路を実現する方式である。無記名電子投票において、各投票者から送信された暗号投票文をシャッフルする場合や、一般的なマルチパーティーコンピュテーション等で利用される。各サーバの動作の正当性の証明とその検証における計算量は、n 入力の場合に単純には $O(n^2)$ となるため、その効率化が技術的課題である。本研究では、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方式、および各サーバにおける計算量を $n \log n$ に低減する方式の 2 方式を提案し、安全性の定式化および詳細な評価を行う。

- 知識の証明を用いた公開鍵暗号：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証明されている。本研究では、同様に知識の証明を利用して暗号の強度を高める方法であるが、より弱い仮定に基づいて安全性の証明が可能である方法を提案し、その安全性を詳細に評価する。

- 頑健かつ非対話的な分散乗算プロトコル：複数のプレイヤーに秘密分散された 2 入力の積を秘密分散す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。従来、頑健性を持つ方式においては、ランダムオラクル仮定を用いない標準的な計算量的仮定に基づく場合は少なくとも 4 交信、ランダムオラクル仮定による場合でも 3 交信の対話が必要であった。本研究では、頑健性、非対話性を備えるとともに、安全性の証明が標準的な仮定に基づいて可能である方式を提案する。

上記各テーマにおける結果に共通する特徴は、提案の方式がすべて離散対数問題とその派生問題の困難性に基づいて構成されていることである。離散対数問題に基づく構成とする利点は以下のようにまとめられる。

- 「安全性の研究が長期間活発に行われている」 1976 年の W. Diffie と M. Hellman による離散対数問題の困難性に基づく公開鍵配送方式の発明以来、研究対象として長い歴史を持ち、その困難性（安全性）に関する多数の結果が知られている。楕円曲線上の有理点の群における離散対数問題も近年活発に研究されており、安全性の検討が進んでいる。

- 「攻撃が非普遍的」 特定の群の要素の表現に依存せず、群構造だけを利用して普遍的に動作する攻撃法の計算量の下限は、問題のサイズ q に対して $\sqrt{q}$ の時間を要することが知られている。従って、ある特定の群に対して効率の良い特殊な攻撃法が発見されたとしても、他の群において同様の攻撃法が適用できる保証はない。

- 「構造が単純」 特に注意を払うべき特異ケースが少ないため、プロトコル構成上、思わぬミスを犯す危険性が少ない上、安全性の解析が比較的容易になる場合もある。

- 「群の共通利用が可能」 一つの群をすべての利用者で共通とすることができる。共通の群を用いることで、暗号、署名等に必要な演算の一部を一体化して、演算効率、メモリ効率の良い方式を構成することができる場合がある。また、安全性が向上する場合もある。例えば、 同報通信のために、単一の文書を異なる公開鍵でそれぞれ暗号化する場合、公開鍵が異なる群から選択されるよりも、共通の群から選択される場合の方がより安全となることが知られている。

- 「短い鍵を利用可能」 楕円曲線上の群に対する効率の良い攻撃法が知られていないため、楕円離散対数問題に基づいて方式を構成する場合には、位数 160 ビット程度の比較的小さな群から選んだ公開鍵を用いても、数キロビット程度の合成数の素因数分解問題に基づく場合とほぼ同等の困難性が期待でき、計算量、メモリ量の点で有利である。

本研究で提案する方式はいずれも比較的容易に組み合わせて利用することが可能であり、従来から知られている、離散対数問題に基づく多数の方式や技法とも親和性がある。そのため、匿名性や秘匿性、あるいはより一般的な分散プロトコルが必要となるアプリケーションを離散対数問題に基づいて構成する際に、本研究の提案する構成要素をモジュラー的に利用する事で、設計の複雑さが軽減されることが期待できる。