論文の内容の要旨

論文題目 Unconditionally Secure Cryptosystems, Authentication Schemes and Their Applications
(和訳 情報量的に安全な暗号・認証方式およびその応用に関する研究)

氏名　　花岡 悟一郎

近年、計算機や計算アルゴリズムの研究および開発は急激な進歩をみせている。これに伴い、現在利用されている暗号・認証方式の将来における安全性は必ずしも保証されないものとなってきている。とくに、将来完成するであろう量子計算機はこれらの暗号・認証方式の安全性を著しく脅かすものであることがわかっている。このような問題は、素因数分解や離散対数問題といった計算量的な困難性の仮定を用いる限り、不可避であるといえる。したがって、長期にわたる安全性が必要とされる状況においては、計算量的な仮定を必要とする方式の利用は適切ではない。将来にわたる高い安全性を実現するためのアプローチとして情報量的安全性に基づいて暗号・認証方式を設計することが考えられる。

いかなる計算能力をもつ攻撃者に対しても安全性を証明できる場合、情報量的に安全であるという。情報量的安全性とはそのようなもっとも高いレベルの安全性を指す。情報量的安全性は、無条件な安全性(unconditional security)とも呼ばれている。情報量的に安全な暗号・認証方式に関し、これまでさまざまな研究が行なわれているが、ここまでに提案された方式の多くは、従来の計算量的な仮定を用いる方式に比べ、機能性および効率性が低くなっている。とくに、必要となる記憶容量が膨大となるため、実用的には計算量的安全性に基づく方式が用いられている。しかし、近年における計算機および計算アルゴリズムの進歩による計算量的安全性に対する不安と記憶装置の大容量・低価格化のため、情報量的安全性に基づく方式の有効性が相対的に認識されてきている。とくに、電子署名のような長期的な安全性を必要とする技術に関しては、情報量的安全性の重要性は高い。

電子署名はデジタルデータの偽造、改ざんなどの不正行為を防止する技術であり、電子決済をはじめとするさまざまなアプリケーションにおいて重要な役割を担っている。現在利用されている電子署名の安全性は、素因数分解や離散対数問題などの計算困難とされている数学的問題の困難性に依拠しており、現時点においては本質的な攻撃方法は存在していない。しかし、このような計算量的な困難性を仮定した電子署名方式に対し、計算機および計算アルゴリズムの進歩による将来にお

ける安全性への不安が指摘されている。たとえば、インターネット上の電子商取引の95¥%において512bitの合成数によるRSA暗号系を用いた電子署名が利用されていたが、これは1999年八月に破られている。また、量子計算機を用いて素因数分解や離散対数問題を多項式時間で解くアルゴリズムが提案されており、将来量子計算機が完成することで、それまでに作成されたすべての電子署名が一切の効力を失ってしまうおそれがある。つまり、現在利用されている電子署名方式を用いて将来にわたる安全性を保証する事は困難である。この事実は、これらの電子署名が長期的な安全性の保証を必要とするアプリケーションに対し利用することができないことを意味している。

本論文においては、いかなる計算量的な困難性も仮定せずに、想定されるすべての攻撃に対し安全性を証明することが可能な電子署名方式を提案を行なっている。従来の電子署名方式の一般的なモデルにおいて、このような高い安全性を実現することは原理的に非常に困難であるため、提案方式においては、まず、電子署名方式のモデルそのものの見直しを行なっている。具体的には、情報量的安全性を導入するためには、従来のモデルとは異なり、検証者は電子署名の検証に用いる情報の一部を秘密にする必要があることを示している。ただし、検証者は同一の秘密情報を用いて、いかなる署名者によって作成された電子署名も検証が可能である。

この新たな電子署名方式のモデルにおける、具体的な情報量的安全性をもつ電子署名方式の構成方法の要点を次に述べる。まず、信頼できる機関が多変数多項式（便宜上、$f(x, y, z)$とする）を作成する。信頼できる機関は、作成した多変数多項式に対し各利用者の識別子および乱数を入力することで、各利用者（便宜上、U_i $(i=1, ..., n)$とする）に対し署名鍵（便宜上、$f(U_i, y, z)$ $(i=1, ..., n)$とする）、乱数（便宜上、R_i $(i=1, ..., n)$とする）および検証鍵（便宜上、$f(x, R_i, z)$ $(i=1, ..., n)$とする）をそれぞれ作成し、配布する。なお、これらの情報を配布した後、信頼できる機関は最初に作成した多変数多項式を消去してもよい。デジタルデータMに対し、利用者U_{i0}はMをU_{i0}の署名鍵に入力することで、U_{i0}のMに対する電子署名（便宜上、$f(U_{i0}, y, M)$とする）を作成する。この電子署名を受け取った利用者U_{i1}は、与えられた乱数R_{i1}を電子署名に入力し、また、U_{i1}の検証鍵にU_{i0}およびMを入力する。これら二つの操作により得られる値が等しい場合、U_{i1}は受け取った電子署名がU_{i0}によりMに対して作成されたものであるとみなす。（すなわち、$f(U_{i0}, y, M)|_{y=Ri1}=f(x, R_{i1}, z)|_{x=Ui0, z=M}$となる場合、$U_{i1}$は$f(U_{i0}, y, M)$を受理する。）

提案した電子署名方式のモデルにおいて、攻撃者が試みるすべての不正行為は、なりすまし攻撃、置換攻撃および罠つき転送攻撃と呼ばれるの三つの攻撃に分類することができる。上記の電子署名方式の構成においては、信頼できる機関によって作成される多変数多項式を適切に設計することで、いかなる計算能力をもつ攻撃者に対しても、これらすべての攻撃に関して安全であることを証明することができる。すなわち、提案方式が適切に設計された場合、なりすまし攻撃、置換攻撃および罠つき転送攻撃の成功確率が、予め定められたある値を越えないことを示すことが可能である。なお、これらの攻撃を複数の攻撃者が結託して行なう場合もありうるが、提案方式においてはこの点についても考慮がなされている。

本研究においては、さらに用途を限定した場合における、上記の電子署名方式の改良方法も示している。具体的には、電子署名の発行回数に制限を与える場合、提案した電子署名方式に対し直接的にそのような制限を与えたものに比べ、必要となる記憶容量を大幅に削減することが可能な方式を提案している。数値例として、利用者の総数を100,000人とし、システム全体における電子署名の発行回数を1回とすると、上記の方式に対し直接的に制限を与えた場合、利用者のもつ秘密情報に必要となる記憶容量が4,493Kbyteになるのに対し、提案手法においてはこれは464Kbyteまで削減されている。したがって、利用可能な記憶容量が厳しく制限される環境（たとえばスマートカード上における実装）において、提案方式が非常に適しているといえる。

本論文では、情報量的に安全な電子署名方式方式に加え、情報量的に安全な鍵配送方式に関する研究も行なっている。暗号通信を行なう際、送信者と受信者は予め鍵を共有しておく必要がある。予備通信なしに送信者・受信者間で鍵を共有する方式は鍵事前配送方式（KPS: Key Predistribution

Systems)と総称される。情報量的に安全なKPSは早くから知られており、また、利用者のもつ秘密情報に必要となる記憶容量が最適となるような方式もすでに提案がなされている。つまり、これは機能と安全性を保ったまま既存のKPSに必要となる記憶容量を削減できないことを意味している。しかし、実際にはKPSによって提供されるすべての機能が必要となるわけではない。具体的には、KPSによってシステム内の任意の二者間の共有鍵が生成可能となるが、実際にはまったく通信を行なわないことが予め想定される送信者・受信者のペアも存在している。このような通信機能を取り除くことで、必要となる記憶容量を削減することが可能となる。ただし、KPSにおいては通常すべての鍵共有機能を統括的に実現しているため、一部の通信機能のみを選択して取り除くことは困難であることに注意されたい。提案方式においては、放送通信のように少数のproviderと多数のconsumerが存在し、provider-consumer間およびprovider-provider間でのみ通信を行なうものと想定している。このとき、提案方式を用いた場合、各consumerの秘密情報に必要となる記憶容量を大幅に削減することが可能となる。提案方式においては、さらにserverとよばれる種類のエンティティの存在を導入することで必要となる記憶容量を一層削減している。具体的な数値例として、consumerの総数が10,000,000人であるとき、従来のKPSを用いた場合各consumerの秘密情報に必要となる記憶容量が64Kbyteとなるのに対し、提案方式を用いた場合これは4Kbyteに削減される。

上記のKPSの効率化手法は放送通信およびそれに類似した通信形態のみに対して適用可能であり、一般的な手法ではない。本研究においては、さらに、任意の通信機能を取り除いた場合に必要となる記憶容量の下界を情報理論を用いた議論により導出し、この下界を達成するような一般的手法の提案を行なっている。提案手法においては、非対称鍵配送方式という新たな鍵配送のための基本ツールを導入し、従来のKPSと最適な非対称鍵配送方式を組み合わせて用いることにより、任意の通信形態に応じたKPSの最適な効率化が可能であることを示している。また、最適な非対称鍵配送方式の構成方法も示している。

本論文においては、これらの研究結果を軸として、この他さまざまな情報量的に安全な暗号プリミティブの提案・解析を行なっている。