マルチメディアネットワークのための高度情報セキュリティ技術

Advanced Information Security Techniques for Multimedia Networks

（研究プロジェクト番号：JSPS-RFTF 96P00604）

プロジェクトリーダー
今井　秀樹　　東京大学生産技術研究所・教授
コアメンバー
辻井　重男　　中央大学理工学部・教授
笠原　正雄　　大阪学院大学情報学部・教授

1　研究目的

本研究プロジェクトでは、マルチメディアネットワークのための情報セキュリティ技術の高度化に関する研究を行ってきた。中でも、「情報量的安全性に基づく認証基盤構築技術」に関しては非常に注目すべき成果が得られたためその研究成果を紹介する。研究内容の詳細については研究成果報告書［1］をご参照頂きたい。

2　研究成果概要

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。

本研究の主要な成果の一つとして、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（図１参照）。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 $(i = 1, \cdots, n)$とする）に対し署名鍵（便宜上、$f(U_i, y, z)$ $(i = 1, \cdots, n)$とする）、乱数（便宜上、R_i $(i = 1, \cdots, n)$とする）および検証鍵（便宜上、$f(x, R_i, z)$ $(i = 1, \cdots, n)$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_{i_0} は M を U_{i_0} の署名鍵に入力することで、U_{i_0} の M に対する電子署名（便宜上、$f(U_{i_0}, y, M)$とする）を作成する。この電子署名を受け取った利用者 U_{i_1} は、与えられた乱数 R_{i_1} を電子署名に入力し、また、U_{i_1} の検証鍵に U_{i_0} 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_{i_1} は受け取った電子署名が U_{i_0} 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、$f(U_{i_0}, y, M) \mid_{y=R_{i_1}} = f(x, R_{i_1}, z) \mid_{x=U_{i_0}, z=M}$ となる場合、U_{i_1} は $f(U_{i_0}, y,$

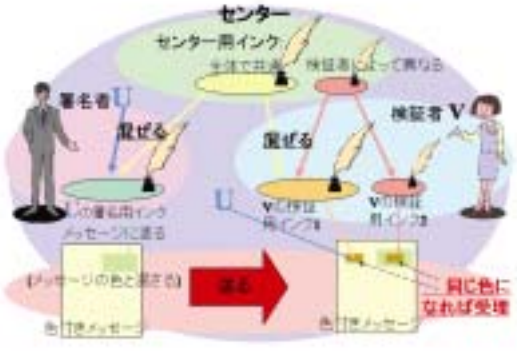

図１　情報量的安全性に基づく電子署名方式の概念図

M)を受理する。）表１に、最初に配布する情報量と提案方式を用いて一人のユーザが安全に発行できる署名の数の関係を示す。

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。

表１：一人のユーザが安全に発行できる署名数（n はユーザ数を示す）。

Amount of Info. \n	10^3	10^4	10^5	10^6
2HD disk(1.44MB)	71	6	0	0
ZIP(100MB)	4,999	499	49	4
CD-R(650MB)	32,499	3,249	324	31
DVD-RAM(5.2GB)	259,999	25,999	2,599	259

３　結論

提案方式は、情報量的安全性をもつ電子署名方式といえる初めてのものである。この方式を利用することで、将来にわたる安全性の保証を必要とするさまざまなアプリケーションの技術的要求に応えることが可能となる。この成果は、長期的な安全性の保証という広く議論されてきた課題を解決するものであり、非常に意義深いものである。また、提案方式においては、電子署名の検証の際、検証者は署名者の公開情報として署名者の識別子のみを利用している。したがって、通常の公開鍵暗号系と異なり、検証者は署名者の公開鍵の正当性を検証する必要がないため、より簡潔な処理が可能となる。

主な発表論文

[1] “マルチメディアネットワークのための高度情報セ　キュリティ技術,” 日本学術振興会未来開拓学術研究推進事業研究　成果報告書, 理工領域-６, マルチメディア高度情報通信システム,2001.

[2] G. Hanaoka, J. Shikata, Y. Zheng and H. Imai, “Unconditionally secure digital signature schemes admittingtransferability,” Advances in Cryptology--ASIACRYPT2000, Lecture Note in Computer Science, vol. 1976, Springer-Verlag,pp. 130-142, 2000.

[3] G. Hanaoka, Y. Zheng and H. Imai, “Unconditionally secure ID-based digital signature scheme,” Proc. of the 22nd Symposium on Information Theory and Its Applications (SITA'99), pp.283-286, 1999.