公開鍵暗号の安全性

概要

電気通信において、盗聴を防ぎ、改ざんを検出する暗号化技術は不可欠である。特に、鍵管理の簡便な公開鍵暗号が有効であり、広く使われつつある。従来の公開鍵暗号よりも安全かつ高速な公開鍵暗号を目指して、楕円曲線上の公開鍵暗号とその安全性評価の研究を行なってきた。主な成果は以下の通り。

合成数を法とした楕円曲線の位数計算問題と素因数分解の等価性

楕円曲線および 3 次曲線を用いた公開鍵暗号が数多く提案されている [1][2]。これらの暗号は安全性の根拠を楕円離散対数問題の困難さに置く ElGamal 型楕円暗号と素因数分解の困難さに置く RSA 型楕円暗号の二つに大別することができる。RSA 型楕円暗号は、用いる合成数の素因数分解自体はできなくても、使用する楕円曲線の位数がわかる場合には解読される。これまで、この二つの困難さ、1) 合成数 n を法とした楕円曲線の位数を計算する困難さ、2) 合成数 n の素因数分解を行なう困難さ、の違いについて何も知られていなかった。我々は、この二つの困難さが計算量的に等価であることを証明した [3]。すなわち、素因数分解ができれば、位数計算を行なうことができ、逆に、楕円曲線の位数計算ができれば、素因数分解ができることを示した。この結果から明らかなように、素因数分解の困難さに安全性の根拠を置く楕円曲線暗号の設計において、用いる楕円曲線の位数が知られないように工夫をする必要がある [4]。さらに、合成数を法とした楕円離散対数問題と、素因数分解との関係を明らかにした。すなわち、1) 合成数を法とした楕円離散対数問題が解ければ、素因数分解ができる、2) 素因数分解問題および素数を法とした楕円離散対数問題が両方できれば、合成数を法とした離散対数問題は解けることを示した。この研究の成果は、公開鍵暗号系の安全性の新たな基準に加わった。

不定方程式に基づく RSA 型楕円暗号の安全性解析

RSA 型楕円暗号に対する解読法が 1997 年に提案された [5]。同報通信に対する解読法は、一定数の同報暗号文の組から連立合同式を立て、これを不定方程式を変換し、不定方程式を解くことで平文を計算するものである。[5] の解読法は平文空間を適当に設定することで容易に回避できる。一方我々は、楕円曲線の整点を求めることにより平文を得る、新たな解読法を示した [6]。新解読法は、楕円曲線の係数とランクが小さいときに有効である。特にこの解読法に弱い平文が存在すること示し、その判別法を明らかにした。そのような平文の個数は平文全体に比べ少数であり暗号の安全性が損なわれることはない。一般の平文を解読するためには係数の非常に大きな楕円曲線の整点を求めなければならず、数値実験および計算量の理論評価を進めている。

（連絡先: 鶴岡 行雄　Email: tsuru@cslab.kecl.ntt.co.jp）

[1] Koyama, K., Maurer, U. M., Okamoto, T. and Vanstone, S. A.: New Public-Key Schemes Based on Elliptic Curves over the Ring Z_n, *Advances in Cryptology — CRYPTO'91*, LNCS 576, pp. 252–266 (1991).

[2] Koyama, K.: Fast RSA-type schemes based on singular cubic curves $y^2 + axy \equiv x^3 \pmod{n}$, *Advances in Cryptology - EUROCRYPT'95*, LNCS 921, pp. 329–340 (1995).

[3] Kunihiro, N. and Koyama, K.: Equivalence of Counting the Number of Points on Elliptic Curve over the Ring Z_n and Factoring n, *Advances in Cryptology — EUROCRYPT'98,* (1998)(to appear).

[4] Okamoto, T. and Uchiyama, S.: Security of an Identity-Based Cryptosystems and the Related Reductions, to appear in *Advances in Cryptology — EUROCRYPT'98,* (1998).

[5] Bleichenbacher, D.: On the Security of the KMOV Public Key Cryptosystem, *Advances in Cryptology — CRYPTO'97*, LNCS 1294, pp. 235–248 (1997).

[6] 鶴岡行雄, 小山謙二: 不定方程式に基づく RSA 型楕円暗号の安全性解析, 1998 年暗号と情報セキュリティシンポジウム, SCIS'98-4.1.E (1998).