代数曲線暗号

有田 正剛 (NEC)、松尾 和人 (中央大・研究開発機構)、趙 晋輝 (中央大・理工)

1 はじめに

何らかの効率的な群演算アルゴリズムが知られている有限群 G があるとする。群 G の要素 g と $h(\ h \in < g >)$ に対して、$h^m = g$ となる整数 m を求める問題は離散対数問題と呼ばれる。

群 G として有限体の乗法群を用いると、離散対数問題は整数の素因数分解問題と同じ程度に困難であることが知られている。この困難性を利用して ElGamal 暗号と呼ばれる公開鍵暗号が構成される。

昨今話題の楕円曲線暗号は群 G として楕円曲線上の点のなす群を用いて、ElGamal 暗号と同様な仕方で構成される公開鍵暗号である。楕円曲線に限らず、一般の代数曲線に対しても、そのヤコビ多様体上の点は群をなす (以下、ヤコビ群) ので、代数曲線暗号を考えることができる。ある代数曲線のクラス C を用いて代数曲線暗号を構成するには、以下の 2 つの基本的課題を解決する必要がある。

課題 I クラス C に属する任意の曲線に対して、そのヤコビ群の加算を実行する効率的なアルゴリズムを求めること。

課題 II クラス C に属する曲線の中から、 安全な曲線、特に、ヤコビ群の位数が大きな素因子をもつ曲線を探索する効率的なアルゴリズムを求めること。

超楕円曲線、superelliptic 曲線、C_{ab} 曲線に対して、課題 I、II を解決しようと、様々な研究がなされている。本論文では、特に、課題 I に対する研究動向について手短に紹介する。各々の課題の詳細については [8] を参照されたい。

2 ヤコビ群上の加算アルゴリズム

2.1 超楕円曲線上の加算アルゴリズム

ヤコビ群をヤコビ多様体上の点群と述べたが、加算アルゴリズムを構成する上では、因子類群とみなした方が都合がよい。ヤコビ群を因子類群として扱うとき、その加算アルゴリズムを考察するには、因子類群の代表系を定める必要がある。超楕円曲線に対しては、reduced divisors が因子類群の代表系を与えることはみやすい。ここで、reduced divisor とは $D = \sum_i m_i P_i - (\sum_i m_i)\, P_\infty,\ m_i \geq 0$ という形の因子 D で $\sum_i m_i$ が種数以下のものである (P_∞ は唯一の無限遠点)。reduced divisor は $U = \prod (X - x(P_i))^{m_i}$ および $F - V^2 \equiv 0 \bmod U, \deg V < \deg U$ なる 2 つの多項式 $(U(X), V(X))$ で表される (Mumford 表現)。Gauss の整係数虚 2 次形式に対する composition と reduction アルゴリズムを、この Mumford 表現を利用した多項式の 2 次形式に自然に拡張することで、超楕円曲線のヤコビ群における加算アルゴリズムである Cantor アルゴリズム

本研究の一部は，通信・放送機構「情報セキュリティ高度化のための第 3 世代暗号技術の研究開発」プロジェクトの一環として行われた.

[3] が得られる。しかし、Cantor アルゴリズムを用いた超楕円曲線暗号は楕円曲線暗号に比べ数倍以上低速である。最近、種数 2 の超楕円曲線に対し、Harley によってより高速なアルゴリズム (Harley アルゴリズム) が与えられた [5]。Harley アルゴリズムでは、入力因子を詳細に分類し各々に対して最適化された計算手順を用いることで、高速化が実現されている。Harely アルゴリズムはさらに高速化され、楕円曲線暗号と同程度の速度にまで達している [9]。また、種数 3 の場合にも拡張されている [7]。

2.2 Superelliptic 曲線や C_{ab} 曲線上の加算アルゴリズム

Superelliptic 曲線や C_{ab} 曲線においては、因子類群の代表系を求めるのに工夫が必要である。それらの曲線では、無限遠点が一点しかないことから、ヤコビ群と座標環のイデアル類群が自然に同型となる。そのため、ヤコビ群における加算をイデアル類群における乗算として実行できる。座標環 R のイデアル I に含まれる 0 でない多項式で無限遠点での極位数が最小のものを f_I とし、$I^* = (f_I) : I = \{r \in R | rI \subset (f)\}$ とする。イデアル類の代表系は、$I = I^{**}$ となるイデアル I によって与えられる [1]。この代表系によって加算アルゴリズムを記述する上で、効率上重要なのは、与えられたイデアルに含まれる極位数が最小の多項式を求めることである。そのために、[4, 6] では LLL アルゴリズムを、[1] では Buchberger アルゴリズムを用いているが、これらはいずれも「万能」アルゴリズムに頼ったものであり、より効率的な手法が待たれるところである。C_{34} 曲線に対しては、Buchberger アルゴリズムに頼らない、より効率的なアルゴリズムが知られている [2]。

参考文献

[1] 有田正剛, C_{ab} 曲線のヤコビアン群加算アルゴリズムとその離散対数型暗号への応用, 電子情報通信学会論文誌 A, J82-A (1999),1291–1299.

[2] S. Arita, An Addition Algorithm in Jacobian of C_{34} Curve, ACISP 2003, LNCS 2727, pp.93–105, Wollongong, Australia, 2003.

[3] D. G. Cantor, Computing in the Jacobian of hyperelliptic curve, Math. Comp., 48 (1987), 95–101.

[4] S. D. Galbraith, S. Paulus, and N. P. Smart, Arithmetic on Superelliptic Curves, J. Cryptology, 12 (1999), 193-196.

[5] P. Gaudry and R. Harley, Counting points on hyperelliptic curves over finite fields, ANTS-IV, Springer-Verlag LNCS 1838, 2000, 297–312.

[6] R. Harasawa and J. Suzuki, A Fast Jacobian Group Arithmetic Scheme for Algebraic Curve Cryptography, IEICE TRANS. FOUND., E84-A (2001), 130-139.

[7] J. Kuroki, M. Gonda, K. Matsuo, J. Chao, and S. Tsujii, Fast genus three hyperelliptic curve cryptosystems, Proc. of SCIS2002, 2002, 503–507.

[8] K. Matsuo, S. Arita, and J. Chao, A Survey on Algebraic Curve Cryptosystems, 日本応用数理学会論文誌, Vol. 13, No. 2, pp. 231-247.

[9] K. Matsuo, J. Chao, and S. Tsujii, Fast genus two hyperelliptic curve cryptosystems, IEICE Technical Report ISEC2001-31, 2001.