ISS-P-046

楕円曲線法の高速化に関する検討

佐藤 海斗† 畑 良知†
† 津山工業高等専門学校総合理工学科

1. はじめに

情報化の進展が著しい今日にあって，情報セキュリティ技術の重要性はますます高まっている．なかでも，情報セキュリティの基盤を担う暗号理論の役割は大きい． 代表的な公開鍵暗号である RSA 暗号は，大きな自然数を現実的な時間で素因数分解することは難しいという事実に安全性を依拠している．したがって，素因数分解問題の高速化について研究することは，RSA 暗号の安全性を評価することに直結すると言える．

入力された自然数の素因数の大きさに依存するような時間計算量を持つもののうち，最速であるものが楕円曲線素因数分解法(ECM)である．本研究では，ECMの虚数乗法を用いた高速化手法の検討を行う．

2. ECM の原理

ECM は，楕円曲線のなす Abel 群の構造を利用したアルゴリズムである．入力は，素因数分解の対象となる合成数 n である．E を $\mathbb{Z}/\mathrm{n}\mathbb{Z}$ 上の楕円曲線とし，$\#E$ をその位数とする．また，P を E の元，O を E の単位元とする．このとき，Lagrange の定理により，$\#\ E\ P\ =\ O$ となる．これは，$\#EP$ の計算においてはゼロ除算が発生することに対応する．すなわち，$\#EP$ の x 座標の分母を m とすると，$p = GCD(n,m) \neq 1$ となる． このとき，高い確率で p は n の非自明な約数であり，n の素因数 p が求まる．

3. 虚数乗法を用いた高速化の原理

入力の合成数 n が $4p = 1 + Dv^2$ と書けるような素因数 p を持つと仮定する．判別式が $-D$ である Hilbert 類多項式を $H_D(\mathrm{x})$ とし，その根の一つを j_0 とする．このとき，j-不変量が j_0 であるような楕円曲線 E は，$1/2$ の確率で $\#E = p$ となることが知られている[2]．したがって，E 上の点 P を一つ選び，nP を計算すると，n の非自明な約数 p を得る．

この高速化においては，j-不変量が j_0 であるような楕円曲線Eを生成すること，E 上の有理点 P を探索することの 2 つが主要な課題となる．

4. 提案手法

相川[1]では，生成した楕円曲線E上の有理点を探索する問題を迂回するために，点の計算を終結式の計算に帰着させていた．この手法は一般化が容易であるという利点を持つが，式が複雑になり実装が込み入るという問題点もある．

本研究では，楕円曲線のツイストに着目し，有理点の探索を解決する平易な新規手法を提案する．

j-不変量が j_0 に等しい楕円曲線 E を Weierstrass 標準形 $y^2 = x^3 + ax + b$ で表すと仮定する．このとき，u を任意の整数として，$y^2 = x^3 + au^2x + bx^3$ で E のツイスト E' が与えられる．$\#E'$ は $1/2$ の確率で p となる．したがって，$u = b$ と取れば，$(0, b^2)$ は E' 上の有理点となる．

以上の有理点計算を導入した提案アルゴリズムを図 1 に示す．

Input: 合成数 n， Hilbert 類多項式の判別式 $-D$
Output: n を割り切る素数
$H_D(\mathrm{x})$を計算する．
$j_0 \leftarrow H_D(\mathrm{x})$の根
$E \leftarrow y^2 = x^3 + ab^2x + b^3x$で表される楕円曲線
$P \leftarrow (0, b^2)$
nP を計算し，その x 座標の分母を m とする．
Return $\mathrm{GCD}(n, m)$

図1．提案手法により高速化した楕円曲線法のアルゴリズム

5. 評価

C++ により提案アルゴリズムを実装し，動作を評価した．入力 n が 4096 ビットの場合でも，10 秒未満の短い時間で素因数を見つけることができた．

6. むすび

本研究では，ECM の虚数乗法を用いた高速化を検討し，有理点の探索に対して平易な新規手法を提案した．また，提案手法を実装し，$4p = 1 + Dv^2$ を満たす素因数を持つ合成数の脆弱性を確認した．

今後の課題として，$H_D(\mathrm{x})$ が線型でない場合への一般化などが挙げられる．

参考文献

[1] Y. Aikawa, et al., Elliptic Curve Method Using Complex Multiplication Method, IEICE Trans. Fundamentals , Vol. E102.A, No. 1, pp. 74-80, 2019.

[2] I. F. Blake, et al., 楕円曲線暗号, ピアソン・エデュケーション, 2001.