Memoirs of the Faculty of Science
Kochi University (Information Science)
Vol. 26 (2005), No. 4

楕円曲線上のトレース写像を用いた暗号方式

佐伯忠典、塩田研一
高知大学大学院理学研究科数理情報科学専攻

概 要

近年、IC カードや組み込み機器のような制限された処理能力環境下での暗号技術の導入が必要不可欠である。小さな鍵サイズ、高速な暗号化・復号化を可能にする暗号方式として楕円曲線暗号に注目が集まっている。しかしながら、楕円曲線暗号には、暗号化したい情報に冗長ビットを付加しなければ、暗号化することが不可能といった短所がある。本研究では、楕円曲線とそのツイストをペアにすることで冗長ビットを不要にとする新たな暗号方式を提唱する。

1 まえがき

2003 年 K.Rubin 氏と A.Silverberg 氏は torus-based cryptography という新たな暗号方式を提唱した [1]。それは、有限体のノルム写像の核を用いることで従来の有限体の乗法群上の離散対数型暗号に比べ、2 倍以上のセキュリティレベルをもつ暗号方式である。本論文では、楕円曲線暗号と torus-based cryptography を組み合わせる方法について報告する。

2 有限体上の楕円曲線

2.1 楕円曲線

$E : y^2 = x^3 + ax + b$ を、標数 5 以上の有限体 $\mathbf{F}_q$ 上定義された楕円曲線とし、$\mathbf{F}_q$ の拡大体 k に対し、E の k - 有理点の成す有限群を $E(k)$ と表す。

2.2 加法公式

E 上の 2 点 $P = (x_1, y_1), Q = (x_2, y_2)$ について、群演算は以下のように定義されていた。

$$\begin{aligned} -P &= (x_1, -y_1) \\ P + Q &= (x_3, y_3) \\ &= (\lambda^2 - x_1 - x_2, (x_1 - x_3)\lambda - y_1) \end{aligned}$$

ただし、

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & (x_1 \neq x_2 \text{ のとき}) \\ \dfrac{3x_1^2 + a}{2y_1} & (x_1 = x_2, y_1 \neq 0 \text{ のとき}) \end{cases}$$

2.3 楕円曲線の twist

E の twist とは

$$E' : y^2 = x^3 + v^2 ax + v^3 b, \quad v \in \mathbf{F}_q : \text{非平方数}$$

により表される $\mathbf{F}_q$ 上の楕円曲線である。2 つの曲線 E と E' は群位数において

$$\#E(\mathbf{F}_q) + \#E'(\mathbf{F}_q) = 2q + 2$$

という関係にあることが知られている。

2.4 トレース写像

$\mathbf{F}_q$ 上の楕円曲線 $E : y^2 = x^3 + ax + b$ に対して、トレース写像 $Tr = Tr_{\mathbf{F}_{q^f}/\mathbf{F}_q}$ を

$$\begin{aligned} Tr : E(\mathbf{F}_{q^f}) &\to E(\mathbf{F}_q) \\ Tr(P) &= P + P^q + P^{q^2} + \cdots + P^{q^{f-1}} \end{aligned}$$

として定義することができる。このトレース写像は準同型写像である。ただし、P^q は $\mathbf{F}_q$ 上の Frobenius 写像 $x \mapsto x^q$ による像を表す。

2.5 トレース写像の核

集合 KT_f を $\mathbf{F}_{q^f}$ の自分自身を除くすべての部分体 M に対するトレース写像 $Tr_{\mathbf{F}_{q^f}/M}$ の核（ker）の共通部分として定義する。

$$KT_f := \cap_{M \neq \mathbf{F}_{q^f}} ker(Tr_{\mathbf{F}_{q^f}/M} : E(\mathbf{F}_{q^f}) \to E(M))$$
$$i.e., KT_f := \cap_{M \neq \mathbf{F}_{q^f}} \{Tr_{\mathbf{F}_{q^f}/M}(P) = \mathcal{O}\}$$

KT_f は $E(F_{q^f})$ の部分群となる。

3 KT_f 暗号方式の概要

3.1 KT_f 上の離散対数問題

KT_f 上の離散対数問題とは「$P, Q \in KT_f$ に対して、$xP = Q$ となるような $x \in \mathbf{Z}$ を求める問題」である。KT_f は $E(\mathbf{F}_{q^f})$ の部分群であるから、楕円曲線上の離散対数問題と同程度に難しいと思われる。

3.2 KT_f 暗号方式

KT_f 上の離散対数問題の困難性に基づいた公開鍵暗号方式を提案する。鍵生成、暗号化、復号化の 3 段階に分けて説明する。

3.2.1 鍵生成

KT_f 暗号方式における鍵は「共通鍵」、「復号化鍵」、「暗号化鍵」の 3 つに分けられる。

共通鍵 楕円曲線の定義方程式 $E : y^2 = x^3 + ax + b$、群 KT_f、有限体 $\mathbf{F}_{q^f}$、ベース点 P で構成される。

復号化鍵 $s \in \mathbf{Z}$

暗号化鍵 点 $Q = sP$

共通鍵と暗号化鍵は公開し、復号化鍵は秘密にしておく。

3.2.2 暗号化

メッセージ $m \in KT_f$ を送るために、送信者は乱数 k を生成し、点 $(kP, m + kQ)$ を計算して送る。この点がメッセージ m に対する暗号文である。

3.2.3 復号化

受信者は復号化鍵 s を用いて、

$$m + kQ - s(kP) = m + k(sP) - s(kP) = m$$

を計算することでメッセージ m を復号化することができる。

4 KT_2 暗号方式

4.1 群 KT_2

KT_f の定義において、$f = 2$ の場合であるから、

$$Tr : E(\mathbf{F}_{q^2}) \to E(\mathbf{F}_q)$$
$$Tr(P) = P + P^q$$
$$KT_2 = \{P | P = -P^q\}$$

である。$P = (x, y)$ とすると、

$$-P^q = -(x, y)^q = -(x^q, y^q) = (x^q, -y^q)$$

ゆえ、

$$\begin{aligned} & P = -P^q \\ \Leftrightarrow \quad & (x, y) = (x^q, -y^q) \\ \Leftrightarrow \quad & x = x^q, y = -y^q \end{aligned}$$

$x = x^q$ より $x \in \mathbf{F}_q$、$y = -y^q$ より $y = 0$ または $y \notin \mathbf{F}_q$ であることがわかる。すなわち、

$$\begin{aligned} KT_2 \quad = \quad & \{\mathcal{O}\} \cup \{(x, 0) | x^3 + ax + b = 0, x \in \mathbf{F}_q\} \\ & \cup \{(x, y) | y^2 = x^3 + ax + b, x \in \mathbf{F}_q, \\ & \qquad y^2 \text{は非平方数}\} \end{aligned}$$

ここで $E(\mathbf{F}_q)$ の $\mathcal{O}$ 以外の点 (x, y) については $x^3 + ax + b$ が $\mathbf{F}_q$ の平方数または 0 であることを思い出そう。

一方、KT_2 は、$x^3 + ax + b$ が非平方数もしくは 0 となっている。すなわち、各 x について。$x^3 + ax + b$ が平方数であれば $E(\mathbf{F}_q)$ の点として、非平方数であれば KT_2 の点として 2 回ずつカウントされる。$x^3 + ax + b = 0$ である場合には、$E(\mathbf{F}_q)$、KT_2 のどちらにも 1 点ずつ存在する。さらにどちらにも無限遠点を 1 つずつカウントして、

$$\#E(\mathbf{F}_q) + \#KT_2 = 2(q - 1) + 2 + 2 = 2q + 2$$

である、KT_2 は曲線の twist と同じ位数をもつことがわかる。

4.2 KT_2 と twist

KT_2 と曲線の twist の関係をさらに調べるために次のような写像を考える。v を $\mathbf{F}_q$ の非平方数、$E' : y^2 = x^3 + v^2ax + v^3b$ として、

$$\begin{aligned}\varphi \quad &: KT_2 \to E'(\mathbf{F}_q) \\ &(x, y) \mapsto (vx, v\sqrt{v}y)\end{aligned}$$

この写像 φ は群同型写像である。つまり、$KT_2 \cong E'(\mathbf{F}_q)$ である。前節で KT_f 暗号方式は群 KT_f 上の離散対数問題に基づいていると紹介したが、KT_2 においてはこれは正しくない。なぜなら、$KT_2 \cong E'(\mathbf{F}_q)$ であるため、KT_2 上の離散対数型暗号は E'（曲線の twist）上での離散対数型暗号と同じ、すなわち従来の楕円曲線暗号と同じである（より詳しく言えば楕円曲線の定義方程式のパラメータを変えたに過ぎない）。KT_f 暗号方式の目的は「セキュリティレベルの向上」、「鍵サイズの縮小」にあるのだが、KT_2 においてはそのどちらも達成することはできず、さらに計算処理時間の増加という欠点だけが残ることになる。

そこで、我々は KT_2 と曲線の twist が同型であるという事実を利用した新たな暗号方式を提案する。

4.3 KT_2 暗号方式

4.3.1 鍵生成

共通鍵 楕円曲線の定義方程式 $E : y^2 = x^3 + ax + b$、有限体 $\mathbf{F}_q$、非平方数 $\lambda \in \mathbf{F}_q$、ベース点 $P_1 \in E(\mathbf{F}_q)$、$P_2 \in E'(\mathbf{F}_q)$（E の twist）

復号化鍵 $s_1, s_2 \in \mathbf{Z}$

暗号化鍵 点 $Q_1 = s_1P_1, Q_2 = s_2P_2$

4.3.2 暗号化

メッセージ m を送るために、$x^3 + ax + b$ が平方数であれば $P = P_1, Q = Q_1$、非平方数であれば $P = P_2, Q = Q_2, m = \lambda m$ とし、送信者は乱数 k を生成して、点の組 $(kP, M + kQ)$ を計算し、$x^3 + ax + b$ が平方数であれば、$(kP, M + kQ, 0)$ を、非平方数であれば、$(kP, M + kQ, 1)$ を送る。（ただし、M は m を x 座標に持つような点）

4.3.3 復号化

受信者は暗号文の第 3 要素が 0 であれば $s = s_1$、1 であれば $s = s_2$ として、$M + kQ - skP = M + ksP - skP = M$ を計算することでメッセージを受け取れる。ただし、暗号文の第 3 要素が 1 であった場合には最後に $m = m\lambda^{-1}$ を計算する。従来の楕円曲線暗号と比べ、平文の x 座標が $E(\mathbf{F}_q)$ の x 座標となっていなくとも E の twist の x 座標になっている（正確には KT_2 の x 座標だが、λ 倍（同型写像）することで twist の点へと移す）。残念ながら、当初の目標であったセキュリティレベルの向上の達成はならなかったが、従来の楕円曲線暗号における平文選択の際の手間を省くことに成功した。

4.4 KT_2 暗号方式への攻撃

KT_2 暗号方式は楕円曲線 E とその twist E' を利用したものであるから、E, E' 各々に対して従来の楕円曲線暗号への攻撃方法が有効である。楕円曲線暗号に対する攻撃方法として代表的な 3 つをあげる。

MOV 攻撃 super-singular な曲線（$\#E(\mathbf{F}_q) = q + 1$ であるもの）に対して、楕円曲線上の離散対数問題を有限体上の離散対数問題へと還元する方法

anomalous 攻撃 anomalous な曲線（$\#E(\mathbf{F}_q) = q$ であるもの）に対して、離散対数問題を線形オーダーで解く方法

Pohlig-Hellman 攻撃 $\#E(\mathbf{F}_q)$ が小さな素因数のみの積になる場合、高速に離散対数問題を解く方法

4.5 安全なパラメータ生成

上記の 3 つの攻撃方法を回避したパラメータを生成するには、選んだ曲線が「super-singular でない」、

「anomalous でない」、「位数が少なくとも 1 つ大きな (160 ビット以上推奨) 素因数をもつ」を満たす必要がある。安全なパラメータを生成するためのアルゴリズムを紹介する。

1. ランダムに曲線 $E : y^2 = x^3 + ax + b$ を生成する。
2. $\#E(\mathbf{F}_q)$ を計算する。
3. $\#E(\mathbf{F}_q) \neq q$ かつ $\#E(\mathbf{F}_q) \neq q+1$ であることを確認する。成り立たないときは 1. へ戻る
4. $\#E(\mathbf{F}_q)$ が大きな素因数をもっているか確認する。小さな素因数のみの積になっている場合は 1. へ戻る。
5. 非平方数 $\lambda \in \mathbf{F}_q$ を選び、$E' : y^2 = x^3 + \lambda^2 ax + \lambda^3 b$ を生成する。
6. $\#E'(\mathbf{F}_q) = 2q + 2 - \#E(\mathbf{F}_q)$ を計算する。
7. $\#E'(\mathbf{F}_q) \neq q$ かつ $\#E'(\mathbf{F}_q) \neq q+1$ であることを確認する。成り立たないときは 1. へ戻る
8. $\#E'(\mathbf{F}_q)$ が大きな素因数をもっているか確認する。小さな素因数のみの積になっている場合は 1. へ戻る。

実験により、ランダムに選ばれた E と E' の位数がどちらも大きな素因数をもつ確率は約 50 % であることが確かめた。

5 KT_6 暗号方式

5.1 群 KT_6

KT_6 の定義は M を $\mathbf{F}_{q^6}$ の部分体として、

$$KT_6 := \cap_{M \neq \mathbf{F}_{q^6}} ker(Tr_{\mathbf{F}_{q^6}/M} : E(\mathbf{F}_{q^6}) \to E(M))$$

$\mathbf{F}_{q^6}$ の部分体は $\mathbf{F}_q, \mathbf{F}_{q^2}, \mathbf{F}_{q^3}$ の 3 つであるが、$ker(Tr_{\mathbf{F}_{q^6}/\mathbf{F}_q} : E(\mathbf{F}_{q^6}) \to E(\mathbf{F}_q))$ は $ker(Tr_{\mathbf{F}_{q^6}/\mathbf{F}_{q^3}} : E(\mathbf{F}_{q^6}) \to E(\mathbf{F}_{q^3}))$ の部分集合であるため

$$\begin{aligned} KT_6 &= ker(Tr_{\mathbf{F}_{q^6}/\mathbf{F}_{q^2}} : E(\mathbf{F}_{q^6}) \to E(\mathbf{F}_{q^2})) \\ &\cap \quad ker(Tr_{\mathbf{F}_{q^6}/\mathbf{F}_{q^3}} : E(\mathbf{F}_{q^6}) \to E(\mathbf{F}_{q^3})) \end{aligned}$$

である。$ker(Tr_{\mathbf{F}_{q^6}/\mathbf{F}_{q^2}} : E(\mathbf{F}_{q^6}) \to E(\mathbf{F}_{q^2}))$ に属する点 P は次の条件を満たす。

$$\begin{aligned} & P \in ker(Tr_{\mathbf{F}_{q^6}/\mathbf{F}_{q^2}} : E(\mathbf{F}_{q^6}) \to E(\mathbf{F}_{q^2})) \\ \Leftrightarrow \quad & Tr_{\mathbf{F}_{q^6}/\mathbf{F}_{q^2}}(P) = \mathcal{O} \\ \Leftrightarrow \quad & P + P^{q^2} + P^{q^4} = \mathcal{O} \end{aligned}$$

さらに、$ker(Tr_{\mathbf{F}_{q^6}/\mathbf{F}_{q^3}} : E(\mathbf{F}_{q^6}) \to E(\mathbf{F}_{q^3}))$ に属する点 P は次の条件を満たす。

$$\begin{aligned} & P \in ker(Tr_{\mathbf{F}_{q^6}/\mathbf{F}_{q^3}} : E(\mathbf{F}_{q^6}) \to E(\mathbf{F}_{q^3})) \\ \Leftrightarrow \quad & Tr_{\mathbf{F}_{q^6}/\mathbf{F}_{q^3}}(P) = \mathcal{O} \\ \Leftrightarrow \quad & P + P^{q^3} = \mathcal{O} \\ \Leftrightarrow \quad & x = x^{q^3}, y = -y^{q^3} \\ \Leftrightarrow \quad & x \in \mathbf{F}_{q^3} \text{かつ } y = 0 \text{ または } y \in \mathbf{F}_{q^6} - \mathbf{F}_{q^3} \end{aligned}$$

5.2 KT_6 定義方程式の求め方

$\mathbf{F}_{q^6} = \mathbf{F}_q[\sqrt{m}][x]/(x^3 + x + k)$ の元を $u_0 + u_1 x + u_2 x^2 + \sqrt{m}(u_3 + u_4 x + u_5 x^2)$ の形で表す ($\mathbf{F}_q$ 上の 3 次既約多項式は $x^3 + x + k$ の形で取れる)。$P = (X, Y) \in KT_6$ は $X = u_0 + u_1 x + u_2 x^2, Y = \sqrt{m}(v_3 + v_4 x + v_5 x^2)$ の形式で表すとする。

まず、点 P が曲線 E 上にあるためには、$Y^2 = X^3 + aX + b$ を満たさなければならないので、代入し、x について各係数を抜き出し 3 つの関係式を得る (順に定数項、1 次の項、2 次の項)

1 $mv_3^2 - 2kmv_4v_5 = b + au_0 + u_0^3 - ku_1^3 - 6ku_0u_1u_2 + 3ku_1u_2^2 + k^2u_2^3$

2 $2mv_3v_4 - 2mv_4v_5 - kmv_5^2 = au_1 + 3u_0^2u_1 - u_1^3 - 6u_0u_1u_2 - 3ku_1^2u_2 - 3ku_0u_2^2 + 3u_1u_2^2 + 2ku_2^3$

3 $mv_4^2 + 2mv_3v_5 - mv_5^2 = 3u_0u_1^2 + au_2 + 3u_0^2u_2 - 3u_1^2u_2 - 3u_0u_2^2 - 3ku_1u_2^2 + u_2^3$

また、点 P が $ker(Tr_{\mathbf{F}_{q^6}}/\mathbf{F}_{q^2} : E(\mathbf{F}_{q^6}) \to E(\mathbf{F}_{q^2}))$ に属する、すなわち、P, P^{q^2}, P^{q^4} が同一直線上にある条件は

4 $u_1v_5 = u_2v_4$

$u_1 \neq 0$ のとき、4 を用いて 1 から 3 の v_5 を消去すると

$1'$ $mv_3^2 - \frac{2kmu_2v_4^2}{u_1} = b + au_0 + u_0^3 - ku_1^3 - 6ku_0u_1u_2 + 3ku_1u_2^2 + k^2u_2^3$

$2'$ $2mv_3v_4 - \frac{2mu_2v_4^2}{u_1} - \frac{kmu_2^2v_4^2}{u_1^2} = au_1 + 3u_0^2u_1 - u_1^3 - 6u_0u_1u_2 - 3ku_1^2u_2 - 3ku_0u_2^2 + 3u_1u_2^2 + 2ku_2^3$

$3'$ $mv_4^2 + \frac{2mu_2v_3v_4}{u_1} - \frac{mu_2^2v_4^2}{u_1^2} = 3u_0u_1^2 + au_2 + 3u_0^2u_2 - 3u_1^2u_2 - 3u_0u_2^2 - 3ku_1u_2^2 + u_2^3$

$2'$、$3'$ から v_3、v_4 を消去すると

5 $(-\frac{mu_1}{u_2} - \frac{mu_2}{u_1} - \frac{kmu_2^2}{u_1^2})v_4^2 = 2u_1^3 - \frac{3u_0u_1^3}{u2} - 3u_0u_1u_2 - 3ku_0u_2^2 + 2u_1u_2^2 + 2ku_2^3$

v_4^2 の係数 $\neq 0$ のときにはこれより

$5'$ $mv_4^2 = -u_1^2(-3u_0 + 2u_2)$

$1'$ と $5'$ より v_3^2 の式を作ると

6 $mv_3^2 = b + au_0 + u_0^3 - ku_1^3 - ku_1u_2^2 + k^2u_2^3$

また $2'$ と $5'$ より v_3v_4 の式を作ると

7 $2mv_3v_4 = au_1 + 3u_0^2u_1 - u_1^3 - 3ku_1^2u_2 - u_1u_2^2$

最後に u_0, u_1, u_2 の関係式を得るために 4、$5'$、6、7 式を用いると

8 $-a^2 + 12bu_0 + 6au_0^2 + 3u_0^4 + 2au_1^2 + 6u_0^2u_1^2 - 12ku_0u_1^3 - u_1^4 - 8bu_2 - 8au_0u_2 - 8u_0^3u_2 + 6aku_1u_2 + 18ku_0^2u_1u_2 + 2ku_1^3u_2 + 2au_2^2 + 6u_0^2u_2^2 - 12ku_0u_1u_2^2 - 2u_1^2u_2^2 - 9k^2u_1^2u_2^2 + 12k^2u_0u_2^3 + 2ku_1u_2^3 - u_2^4 - 8k^2u_2^4 = 0$

したがって、KT_6 定義方程式は若干の例外点を除いて $5'$,6,7,8 式の４つの方程式からなる。

5.3 KT_6 暗号方式

5.3.1 鍵生成

共通鍵 楕円曲線の定義方程式 $E : y^2 = x^3 + ax + b$、有限体 F_{q^6} ベース点 $P \in KT_6$

復号化鍵 $s \in \mathbf{Z}$

暗号化鍵 点 $Q = sP$

5.3.2 暗号化

メッセージ m を送るために、送信者は乱数 k を生成して、点の組 $(kP, M + kQ)$ を計算し送る（M は m を x 座標に持つような点)。

5.3.3 復号化

受信者は $M + kQ - skP = M + ksP - skP = M$ を計算することでメッセージを受け取れる。

5.4 平文選択のアルゴリズム

KT_6 暗号方式において平文は KT_6 の点として符号化されなければならない。KT_6 の点として扱えるようにするためのアルゴリズムを紹介する。

$P = (X, Y) = (u_0 + u_1x + u_2x^2, \sqrt{m}(v_3 + v_4x + v_5x^2))$ とする。楕円曲線暗号のとき同様平文 (m_1, m_2) に乱数ビット（ビット幅を k とする）を付加する。

$$a_1 = m_1 \ll k + \text{乱数ビット}$$
$$a_2 = m_2 \ll k + \text{乱数ビット}$$

$a_1 = 0$ または $a_2 = 0$ の場合には乱数ビットを取り替える。次に KT_6 定義方程式の 8 式において $u_0 = t, u_1 = a_1, u_2 = a_2$ を代入して、t に関する解を求める。その解の 1 つを a_0 とする。次に q_1 に定義方程式の $5'$ 式の右辺、q_2 に 6 式の右辺、q_3 に 7 式の右辺にそれぞれ $u_0 = a_0, u_1 = a_1, u_2 = a_2$ を代入した式に m^{-1} を掛けた式。すなわち、

$$\begin{aligned} q_1 &= m^{-1}(-a_1^2(-3a_0 + 2a_2)) \\ q_2 &= m^{-1}(b + au_0 + u_0^3 - ku_1^3 - ku_1u_2^2 + k^2u_2^3) \\ q_3 &= m^{-1}(au_1 + 3u_0^2u_1 - u_1^3 - 3ku_1^2u_2 - u_1u_2^2) \end{aligned}$$

q_1 は v_4^2 の式、q_2 は v_3^2 の式、q_3 は $2v_3v_4$ の式を表すことになる。そして、q_1, q_2 どちらも非平方数でなければ $r_1 = \sqrt{q_1}, r_2 = \sqrt{q_2}$ を求める（i.e.,$r_1 = v_4, r_2 = v_3$)。またこの r_1, r_2 が 7 式を満たすかどうかを $2r_2r_1 = q_3$ が成り立つかどうかによって確かめる。成り立たない場合は $r_2 = -r_2$ に取り替えて同様に行う。7 式を満たすことが確認できたならば、次は

$$r_3 = \frac{a_2r_1}{a_1}$$

を計算し、$u = a_0 + a_1 x + a_2 x^2, v = r_2 + r_1 x + r_3 x^2$ を求める。このとき、$(X, Y) = (u, \sqrt{m}v)$ が暗号化したい情報 (m_1, m_2) に対する平文である。q_1, q_2 のどちらかが平方数であった場合もしくは $2r_2 r_1 \neq q_3$ であった場合は乱数を取り替えて同様に行う。

6 今後の課題

KT_6 では定義方程式は与えたもののかなり複雑である。KT_6 暗号方式に高速性を求めるならば、定義方程式を簡略化するのが有効であると考えられる。なぜならば、KT_6 暗号方式における平文埋め込みアルゴリズムにおいて、4 つの定義方程式のうちもっとも複雑な方程式を解くという作業をしなければならないためである（残り 3 つはこの方程式に比べれば単純）。今後、暗号技術の発展により楕円曲線暗号の鍵サイズが大きくなったとき（楕円曲線暗号の鍵サイズが小さいのは楕円曲線上の離散対数問題を解く効果的なアルゴリズムが未発見であるため）、$KT_{30}(30 = 2 \times 3 \times 5)$、$KT_{210}(210 = 2 \times 3 \times 5 \times 7)$ 暗号方式の出現によって小さな鍵サイズを維持したまま高いセキュリティレベルを提供することが可能になると期待できる。

7 おわりに

本研究における最大の成果は KT_f という新たな有限アーベル群の発見、および KT_2 と楕円曲線の twist が同型であるという事実も発見したことである。KT_2 暗号方式ではセキュリティレベルの向上はならなかったものの従来の楕円曲線暗号における平文の選択の煩わしさを解消することに成功した。しかし、2 つの曲線を同時使用していることを利用した攻撃方法が存在しないという保証はない。今回提案した暗号方式が実用的なものとなるためには、少なくとも既存の攻撃方法に対抗し、また新たに登場する攻撃方法に耐えなければならない。

8 参考文献

[1] Karl Rubin and Alice Silverberg,Torus-Based Cryptography,Springer LNCS 2729, pp.349-365,2003.

[2] Neal Koblitz,A Course In Number Theory and Cryptography,GTM114 ,Springer-Verlag,1997.

[3] I.Blake and G.Seroussi and N.Smart,Elliptic Curves in Cryptography,London Mathematical Society LN265,Cambridge Univ. Press,1999.