Computer Security Symposium 2017
23 - 25 October 2017

各種楕円曲線におけるECDLPの強度に関する考察

小寺 健太[1]　宮地 充子[1,2]　鄭 振牟[1]

概要：楕円曲線暗号の安全性は楕円曲線状の離散対数問題（ECDLP）の難しさを根拠としている．現時点で最も強力な ECDLP の解読手法は，一般的な離散対数問題に対する解読手法として知られる Pollard の ρ 法であり，指数関数時間を要する．しかし近年，Semaev や Gaudly，Diem らにより ECDLP に対する指数計算法が提案され，ある条件下において ECDLP を準指数時間で解読できることを示した．本論文では，Weierstrass，Hessian，Montgomery，Edwards といった各種楕円曲線上の ECDLP に対する指数計算法に注目する．互いに同型写像を持つ各種曲線において ECDLP の解読時間の違いを実験的に確認し，その原因について検討する．

キーワード：楕円曲線暗号，ECDLP，指数計算法

Kenta Kodera[1]　Atsuko Miyaji[1,2]　Chen-Mou Cheng[1]

Abstract: The security of elliptic curve cryptography is closely related to the complexity of solving the elliptic curve discrete logarithm problem (ECDLP). Today, the best practical attacks against general ECDLP are generic discrete logarithm algorithms such as Pollard's rho method, which takes an exponential time. Recently, there is a line of research on index calculus algorithms for ECDLP started by Semaev, Gaudry, and Diem. Under certain heuristic assumptions, such algorithms could lead to subexponential attacks to ECDLP in some cases. In this paper, we investigate the complexity of solving ECDLP for elliptic curves in various forms—including Hessian, Montgomery, (twisted) Edwards, and Weierstrass using index calculus algorithms. We will provide some insights and empirical evidence showing an affirmative answer in this paper.

Keywords: ECDLP, index calculus, elliptic curves cryptography, security evaluation

1. 序論

楕円曲線暗号は公開鍵暗号の一つで，RSA 暗号などと比較して同程度の安全性の実現に必要な鍵長が非常に短いという特長をもつ．このことから，IoT 機器への応用などに関して大きな注目を浴びている．楕円曲線暗号の安全性は楕円曲線上の離散対数問題（ECDLP）の困難さを根拠とする．いま p を素数，E を 体 $\mathbb{F}_{p^n}$ 上で定義された非特異な楕円曲線とし，E 上で無限遠点 $\mathcal{O}$ とともに加法群をなす有理点集合を $E(\mathbb{F}_{p^n})$ と表す．ECDLP とは，素数位数の点 $P \in E(\mathbb{F}_{p^n})$ と $Q \in \langle P \rangle$ が与えられたとき，$Q = \alpha P$ を満たす整数 α を求める問題である．現在最も強力な解読手法は，一般的な離散対数問題の解読手法として知られる Pollard の ρ 法 [11] であり，これは指数関数時間を要する．一方で近年，Semaev，Gaudry， Diem らによって ECDLP に対して指数計算法を適用する研究が提案された [12]，[7]，[3]．この手法は特定の ECDLP を準指数関数時間で解読できるとされている [5]，[10]，[8]．

本論文では, Weierstrass, Hessian [13] , Montgomery [9], Edwards [2]，[1]，といった各種楕円曲線上の ECDLP に対して指数計算法を適用する．互いに同型である楕円曲線に限定し，それらの解読時間を実験的に比較する．この結果，曲線によって解読時間に明らかな違いがあることを示す．

本論文の構成は以下の通りである．第 2 章では ECDLP に対する指数計算法について詳細に説明する．第 3 章では各種楕円曲線について述べ，4 章では同型写像の構成方法について述べる．第 5 章では，数式処理ソフトウェア MAGMA を用いた実装実験の結果を記す．第 6 章では，実験結果を考察しその根拠を述べる．最後に第 7 章で本論文を総括する．

[1] 大阪大学大学院 工学研究科
Graduate School of Engineering, Osaka University
[2] 北陸先端科学技術大学院大学
Japan Advanced Institute of Science and Technology

2. Index calculus for ECDLP

E を $\mathbb{F}_{p^n}$ 上で定義された楕円曲線とする．素数位数の点 $P \in E(\mathbb{F}_{p^n})$ と $Q \in \langle P \rangle$ に関して指数計算法により ECDLP を解読する手順は以下の通りである．

(1) *factor base* $\mathcal{F} \subset E(\mathbb{F}_{p^n})$ を決定する．

(2) 乱数 $a_i, b_i \in \mathbb{F}_{p^n}$ を用いて楕円曲線上の点 $a_iP + b_iQ$ を作り $\mathcal{F}$ 内の点の加算で表した点の分解式の集合 $\mathcal{R}$ を得る．

$$\mathcal{R} = \left\{ a_iP + b_iQ = \sum_{j=1}^{m} P_{i,j} : P_{i,j} \in \mathcal{F} \right\}$$

(3) $|\mathcal{R}| \approx |\mathcal{F}|$ まで (2) を繰り返し，ガウスの消去法により $aP + bQ = \mathcal{O}$ となる a, b を得る．これより $\alpha = -a/b \bmod \mathrm{ord}(P)$ として α を求める．

2.1 Semaev's summation polynomials

ECDLP に対する指数計算法において，点の分解式を得る部分が最も重要となる．Semaev は summation polynomial と呼ばれる多変数多項式を解くことで点の分解式を得る手法を提案した [12]．Weierstrass 曲線 $y^2 = x^3 + ax + b$ において $P_1 + P_2 = \mathcal{O}$ を満たす 2 点は．その x 座標が等しいことは明らかである．次に $P_1 + P_2 + P_3 = \mathcal{O}$ となるような 3 点について考える．

$$Z = \left\{ \begin{array}{l} (x_1, y_1, x_2, y_2, x_3, y_3) \in \mathbb{F}_{p^n}^6 : \\ \quad (x_i, y_i) \in E(\mathbb{F}_{p^n}), i = 1, 2, 3; \\ \quad (x_1, y_1) + (x_2, y_2) + (x_3, y_3) = \mathcal{O} \end{array} \right\}.$$

ここで Z は明らかに以下の多項式から生成されるイデアル $I \subset \mathbb{F}_{p^n}[X_1, Y_1, X_2, Y_2, X_3, Y_3]$ の代数多様体と言える．

$$I = \left(\begin{array}{l} (X_3 - X_1)(Y_2 - Y_1) - (X_2 - X_1)(Y_3 - Y_1), \\ Y_i^2 - (X_i^3 + aX_i + b), i = 1, 2, 3 \end{array} \right).$$

いま，$J = I \cap \mathbb{F}_{p^n}[X_1, X_2, X_3]$ を MAGMA の `EliminationIdeal` 関数を用いて求めると，この J は次の多項式によって生成される単項イデアルとなる．

$$(X_2 - X_3)(X_1 - X_3)(X_1 - X_2)f_3$$

ここで f_3 は

$$\begin{aligned} f_3 =& X_1^2X_2^2 - 2X_1^2X_2X_3 + X_1^2X_3^2 \\ & - 2X_1X_2^2X_3 - 2X_1X_2X_3^2 - 2aX_1X_2 - 2aX_1X_3 \\ & - 4bX_1 + X_2^2X_3^2 - 2aX_2X_3 - 4bX_2 - 4bX_3 + a^2. \end{aligned}$$

$(X_2 - X_3)(X_1 - X_3)(X_1 - X_2)$ は 2 点の和が無限遠点となる $P_1 + (-P_1) + \mathcal{O} = \mathcal{O}$ のような自明な解に対応している．よって f_3 こそが加算により無限遠点となる 3 点を導く 3 変数多項式，summation polynomial であると言える．4 変数以上については以下のように 2，3 変数の summation polynomial による終結式から再帰的に求めることができる．

$$f_m = Res(f_{m-k}(X_1, \ldots, X_{m-k-1}, X), f_{k+2}(X_{m-k}, \ldots, X_m, X))$$

また Weierstrass 曲線の場合 *factor base* を以下とする．

$$\mathcal{F} = \left\{ (x, y) \in E(\mathbb{F}_{p^n}) : x \in V \subset \mathbb{F}_{p^n}) \right\}$$

ここで $V \subset \mathbb{F}_{p^n}$ とする．Weierstrass 曲線上の点はその逆元と x 座標が共通であるために factor base は x 座標について制約することで形成している．

2.2 Weil restriction

Weil restriction とは拡大体上の多項式システムをより解きやすくする手法である．3 変数の summation polynomial である f_3 を例に考えてみる．あるランダムな点 $aP + bQ$ をある 2 点の和に分解することは $aP + bQ$ との加算が無限遠点になる 2 点を探すことと等価である．よって実際には $aP + bQ$ の x 座標を f_3 の変数のうち 1 つに代入して解く．これは 2.1 章における J を $\mathbb{F}_{p^n}[X_1, X_2]$ へ写像していると考えられる．このイデアルの代数多様体の次元は 0 ではないので，この多項式システムをより解きやすくするためには X_1 と X_2 に関する式がさらに必要となる．

いま，$\mathbb{F}_{p^n}[X]$ 上の多項式において $\mathbb{F}_{p^n}$ 上の根を求めるとき，$\mathbb{F}_{p^n}[X]/(X^{p^n} - X) \cong \mathbb{F}_{p^n}[X_1, \ldots, X_n]/(X_1^p - X_1, \ldots, X_n^p - X_n)$ を考えることができる．これは $\mathbb{F}_{p^n}$ を $\mathbb{F}_p$ 上のベクトル空間と捉えたときの基底 $(\theta_1, \ldots, \theta_n)$ を用いて，不定元である X を $X_1\theta_1 + \cdots + X_n\theta_n$ とすることで実現できる．よって，多項式 $f = \sum a_iX^i \in \mathbb{F}_{p^n}[X]$ は $f_1, \ldots, f_n \in \mathbb{F}_p[X_1, \ldots, X_n]/(X_1^p - X_1, \ldots, X_n^p - X_n)$ を用いて $f_1\theta_1 + \cdots + f_n\theta_n$ と表現できる．以上より，$\mathbb{F}_{p^n}$ 上の方程式 $f = 0$ から $\mathbb{F}_p$ 上の n 本の方程式 $f_1 = \cdots = f_n = 0$ を得ることができる．この手法 Weil restriction は Gaudry や Diem らによって用いられ，その際は factor base を決定する部分空間 V として $\mathbb{F}_p$ が使用されている [3], [7].

2.3 対称性の利用

楕円曲線上の点集合は可換群であるから，点の分解式 $P_1 + \cdots + P_m$ は対称群 S_m の作用下で不変である．この性質に注目した Gaudry は，summation polynomial の変数 $x_1, \ldots, x_m \in \mathbb{F}_{p^n}$ を基本対称式 $e_1, \ldots, e_m$ によって書き換えることを提案した [7]．基本対称式は $e_1 = \sum x_i$, $e_2 = \sum_{i \neq j} x_ix_j$, $e_3 = \sum_{i \neq j, i \neq k, j \neq k} x_ix_jx_k$ のように表される．結果として summation polynomial の次数を下げ，点の分解式を得る計算を高速化できた [7].

さらに，factor base が小さい位数の点の加算作用の下で不変，つまり $^\forall P \in \mathcal{F}$ に対して位数 n の点 T_n を用いて

$P+T_n \in \mathcal{F}$ が成り立つとき，対称性に関する群構造を用いた高速化手法が提案されている [4].

例えば，ある点 R を加算により分解する関係式について位数 2 の点の加算作用を考える．

$$\begin{aligned} R &= P_1 + \cdots + P_n \\ &= (P_1 + u_1 T_2) + \cdots + (P_{n-1} + u_{n-1} T_2) \\ &\quad + \left(P_n + \left(\sum_{i=1}^{n-1} u_i \right) T_2 \right). \end{aligned}$$

これはどんな $u_1, \ldots, u_{n-1} \in \{0,1\}$ についても成立し，点 T_2 の加算作用下で factor base が不変であれば $P_i \in \mathcal{F}$ に対して常に $P_i + u_i T_2 \in \mathcal{F}$ となる．つまり R を n 点の和に分解する式が 1 つあれば，さらに 2^{n-1} 個の分解式を得ることができるのである．

3. 各種曲線について

3.1 Montgomery 曲線

$p \neq 2$ の $\mathbb{F}_{p^n}$ 上で定義された Montgomery 曲線 $M_{A,B}$ は以下の等式を満たす．

$$By^2 = x^3 + Ax^2 + x \tag{1}$$

ここで $A, B \in \mathbb{F}_{p^n}$ は $A \neq \pm 2$，$B \neq 0$，$B(A^2-4) \neq 0$ である [9]．曲線上の点 $P = (x, y) \in M_{A,B}$ に対し，逆元は $-P = (x, -y)$ で与えられ，これらの x 座標は同じである．また点の加法 $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ は以下の通りである．

- $(x_1, y_1) \neq (x_2, y_2)$ のとき:

$$\begin{aligned} x_3 &= B\left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - A - x_1 - x_2 = \frac{B(x_2 y_1 - x_1 y_2)^2}{x_1 x_2 (x_2 - x_1)^2} \\ y_3 &= \frac{(2x_1 + x_2 + A)(y_2 - y_1)}{x_2 - x_1} - \frac{B(y_2 - y_1)^3}{(x_2 - x_1)^3} - y_1 \end{aligned}$$

- $(x_1, y_1) = (x_2, y_2)$ のとき:

$$\begin{aligned} x_3 &= \frac{(x_1^2 - 1)^2}{4x_1(x_1^2 + Ax_1 + 1)} \\ y_3 &= \frac{(2x_1 + x_1 + A)(3x_1^2 + 2Ax_1 + 1)}{2By_1} \\ &\quad - \frac{B(3x_1^2 + 2Ax_1 + 1)^3}{(2By_1)^3} - y_1 \end{aligned}$$

3.2 Montgomery 曲線における summation polynomial

Semaev の手法 [12] に従い，Montgomery 曲線における summation polynomial を導出する．Weierstrass 曲線と同様に，Montgomery 曲線上の点とその逆元で x 座標が共通であることから，x 座標に関して構成する．$f_{M,2} = X_1 - X_2$ であることは明らかである．次に $f_{M,3}$ を考える．2 点 $P, Q \in M_{A,B}$ を $P = (x_1, y_1)$, $Q = (x_2, y_2)$ とおき $P + Q = (x_3, y_3)$，$P - Q = (x_4, y_4)$ とおく加法公式から，

$$x_3 = \frac{B(x_2 y_1 - x_1 y_2)^2}{x_1 x_2 (x_2 - x_1)^2}, x_4 = \frac{B(x_2 y_1 - x_1 y_2)^2}{x_1 x_2 (x_2 + x_1)^2}.$$

さらに，

$$\begin{aligned} x_3 + x_4 &= \frac{2\left((x_1 + x_2)(x_1 x_2 + 1) + 2Ax_1 x_2\right)}{(x_1 - x_2)^2}, \text{ and} \\ x_3 x_4 &= \frac{(1 - x_1 x_2)^2}{(x_1 - x_2)^2}. \end{aligned}$$

解と係数の関係から，x_3, x_4 を根にもつ 2 次多項式を以下のように構成できる．

$$(x_1 - x_2)^2 x^2 - 2\left((x_1 + x_2)(x_1 x_2 + 1) + 2Ax_1 x_2\right) x + (1 - x_1 x_2)^2.$$

よって $f_{M,3}$ は

$$\begin{aligned} f_{M,3}(X_1, X_2, X_3) = (X_1 - X_2)^2 X_3^2 \\ - 2((X_1 + X_2)(X_1 X_2 + 1) \\ + 2AX_1 X_2) X_3 + (1 - X_1 X_2)^2 \end{aligned}$$

4 変数以上の summation polynomial は，終結式によって計算できる．これはある点とその逆元を加算しても元の加算式を変えないことから，共通根を持つ 2 つの summation polynmoial に分解できるためである．

$$\begin{aligned} f_{M,m}(X_1, \ldots, X_m) = \mathrm{Res}_X(f_{M,m-k}(X_1, \ldots, X_{m-k-1}, X), \\ f_{M,k+2}(X_{m-k}, \ldots, X_m, X)). \end{aligned}$$

3.3 Montgomery 曲線における位数 2 の点の働き

Montgomery 曲線は常に位数 2 の点 T_2 をもつ．$T_2 + T_2 = 2T_2 = \mathcal{O}$ であるから $-T_2 = T_2$ を満たす．$T_2 = (x, y)$ とおくと，$-T_2 = (x, -y)$ であるから $y = 0$．これを曲線式 (1) に代入し $x^3 + Ax^2 + x = 0$ を得る．左辺は $x(x^2 + Ax + 1) = 0$ と因数分解できるので以下を得る．

$$x = 0, \frac{-A \pm \sqrt{A^2 - 4}}{2}.$$

従って，楕円曲線上の有理点集合には少なくとも $(0,0)$ で表される位数 2 の点が存在することが分かる．他の位数 2 の点は有理点でない場合があるため，本論文では Montgomery 曲線上の T_2 として $(0,0)$ に注目する．加算公式に $(x_2, y_2) = (0,0)$ を代入することで，任意の点 $P = (x, y) \in E(M_{A,B})$ に対し $P + (0,0) = (1/x, -y/x^2)$ を満たすことが分かる．

$T_2 = (0,0)$ の加算作用に関する対称性を利用するために，$\mathcal{F} = \{(x, y) \in E(\mathbb{F}_{p^n}) : x \in V \subset \mathbb{F}_{p^n}\}$ と定義される factor base を T_2 の加算下で不変であるように構成する必要がある．つまり部分空間 V が乗法逆元に関して閉じていなければならない．従って，V は曲線の定義体 $\mathbb{F}_{p^n}$ の部分体である必要があり，これを満たすのは n の約数 ℓ を用いて $V = \mathbb{F}_{p^\ell}$ と定義する場合である．

3.4 Hessian 曲線

$p^n = 2 \bmod 3$ を満たす $\mathbb{F}_{p^n}$ 上で定義された Hessian 曲線 H_d は 以下の等式を満たす.

$$x^3 + y^3 + 1 = 3dxy \tag{2}$$

ここで $d \in \mathbb{F}_{p^n}$ は $27d^3 \neq 1$ である [13]. 曲線上の点 $P = (x, y) \in H_d$ に対し，逆元は $-P = (y, x)$ で与えられ，これらの $x + y$ の値は等しい．さらに 2 点の加法 $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ を考えるとき以下の公式が存在する.

- $(x_1, y_1) \neq (x_2, y_2)$ のとき:

$$x_3 = \frac{y_1^2 x_2 - y_2^2 x_1}{x_2 y_2 - x_1 y_1}$$
$$y_3 = \frac{x_1^2 y_2 - x_2^2 y_1}{x_2 y_2 - x_1 y_1}$$

- $(x_1, y_1) = (x_2, y_2)$ のとき:

$$x_3 = \frac{y_1(1 - x_1^3)}{x_1^3 - y_1^3}$$
$$y_3 = \frac{x_1(y_1^3 - 1)}{x_1^3 - y_1^3}$$

3.5 Hessian 曲線における summation polynomial

Hessian 曲線における summation polynomial は Galbraith と Gebregiyorgis による手法 [6] を参考にして導出される．まず，曲線上の点からその逆元への写像において x 座標と y 座標の和は不変であることに注目し，$T = X + Y$ という新しい変数を考える．2 変数の場合は明らかに $f_{H,2} = T_1 - T_2$ となる.

$$Z = \left\{ \begin{array}{l} (x_1, y_1, t_1, x_2, y_2, t_2, x_3, y_3, t_3) \in \mathbb{F}_{p^n}^9 : \\ \quad (x_i, y_i) \in H_d(\mathbb{F}_{p^n}), i = 1, 2, 3; \\ \quad (x_1, y_1) + (x_2, y_2) + (x_3, y_3) = \mathcal{O}; \\ \quad x_i + y_i = t_i, i = 1, 2, 3 \end{array} \right\}.$$

ここで Z は以下によって生成されるイデアル $I \subset \mathbb{F}_{p^n}[X_1, Y_1, T_1, X_2, Y_2, T_2, X_3, Y_3, T_3]$ の代数多様体である.

$$I = \begin{pmatrix} (X_3 - X_1)(Y_2 - Y_1) - (X_2 - X_1)(Y_3 - Y_1), \\ X_i^3 + Y_i^3 + 1 - 3dX_iY_i, i = 1, 2, 3, \\ X_i + Y_i - T_i, i = 1, 2, 3 \end{pmatrix}.$$

2 章と同様にして $I \cap \mathbb{F}_{p^n}[T_1, T_2, T_3]$ を elimination ideal により計算する．整理すると以下のように $f_{H,3}$ が得られる.

$$\begin{aligned} f_{H,3}(T_1, T_2, T_3) = \\ & T_1^2 T_2^2 T_3 + dT_1^2 T_2^2 + T_1^2 T_2 T_3^2 + dT_1^2 T_2 T_3 + dT_1^2 T_3^2 \\ & - T_1^2 + T_1 T_2^2 T_3^2 + dT_1 T_2^2 T_3 + dT_1 T_2 T_3^2 + 3d^2 T_1 T_2 T_3 \\ & + 2T_1 T_2 + 2T_1 T_3 + 2dT_1 + dT_2^2 T_3^2 - T_2^2 \\ & + 2T_2 T_3 + 2dT_2 - T_3^2 + 2dT_3 + 3d^2 \end{aligned}$$

他の曲線と同様に 4 変数以上の場合は終結式によって求められる.

$$\begin{aligned} f_{H,m}(T_1, \ldots, T_m) = \mathrm{Res}(& f_{H,m-k}(T_1, \ldots, T_{m-k-1}, T), \\ & f_{H,k+2}(T_{m-k}, \ldots, T_m, T)) \end{aligned}$$

Hessian 曲線上の位数 2 の点を $T_2 = (x, y)$ とおく．同様にして $T_2 + T_2 = 2T_2 = \mathcal{O}$ より，$x = y$ を満たすので曲線式 (2) に代入し $2x^3 - 3dx^2 + 1 = 0$ を得る．よって，多項式 $2X^3 - 3dX^2 + 1$ が $\mathbb{F}_{p^n}$ 上に根 ζ を持つとき，Hessian 曲線は (ζ, ζ) という位数 2 の点を持つ．このとき $P = (x, y) \in H_d(\mathbb{F}_{p^n})$ に対して $P + T_2 = (x', y')$ とおけば

$$\left\{ \begin{array}{l} x' = \dfrac{\zeta y^2 - \zeta^2 x}{\zeta^2 - xy}, \\ y' = \dfrac{\zeta x^2 - \zeta^2 y}{\zeta^2 - xy}. \end{array} \right.$$

と書き表わすことができる．以上より明らかに Hessian 曲線上の factor base は T_2 の加算作用下で一般的に不変ではなく，対称性を利用することは難しい.

3.6 (twisted Edwards 曲線)

Faugère, Gaudry, Hout, Renault らによって twisted Edwards 曲線，twisted Jacobi intersection 曲線, Weierstrass 曲線の 3 曲線に関する手法の提案と比較が行われている [4]. 以下に (twisted) Edwards 曲線について基本的な事柄を記す．$p \neq 2$ の $\mathbb{F}_{p^n}$ 上で定義された Edwards 曲線は $d \in \mathbb{F}_{p^n}$ を用いた以下の式を満たす [2].

$$x^2 + y^2 = 1 + dx^2 y^2$$

さらに twisted Edwards 曲線は, Edwards 曲線の quadratic twist であり，$a', d' \in \mathbb{F}_{p^n}$ を用いた以下の等式を満たす [1].

$$a'x^2 + y^2 = 1 + d'x^2 y^2 \tag{3}$$

twisted Edwards 曲線上の点 $P = (x, y) \in tE_{a',d'}$ に対し，逆元は $-P = (-x, y)$ で与えられ，これらの y 座標は同じである．さらに $(x_3, y_3) = (x_1, y_1) + (x_2, y_2)$ に関する加法公式は以下で与えられる.

- $(x_1, y_1) \neq (x_2, y_2)$ のとき:

$$x_3 = \frac{x_1 y_2 + y_1 x_2}{1 + d'x_1 x_2 y_1 y_2}$$
$$y_3 = \frac{y_1 y_2 - a'x_1 x_2}{1 - d'x_1 x_2 y_1 y_2}$$

- $(x_1, y_1) = (x_2, y_2)$ のとき:

$$x_3 = \frac{2x_1 y_1}{1 + d'x_1^2 y_1^2}$$
$$y_3 = \frac{y_1^2 - a'x_1^2}{1 - d'x_1^2 y_1^2}$$

また，summation polynomial は以下の通りである.

$$f_{tE,2}(Y_1,Y_2) = Y_2 - Y_1$$
$$f_{tE,3}(Y_1,Y_2,Y_3) = \left(Y_1^2Y_2^2 - Y_1^2 - Y_2^2 + \frac{a}{d}\right)Y_3^2 + 2\frac{d-a}{d}Y_1Y_2Y_3 + \frac{a}{d}\left(Y_1^2 + Y_2^2 - 1\right) - Y_1^2Y_2^2$$

これまでと同様に，4 変数以上の summation polynomial は終結式によって計算される．

また，twisted Edwards 曲線は位数 2 の点 $T_2 = (0,-1)$ を持ち，$P = (x,y) \in E(tE_{a',d'})$ について $P + T_2 = (-x,-y)$ を満たす．

4. 各種曲線間の同型写像

本論文では Hessian(H), Weierstrass(W), Montgomery (M), twisted Edwards (tE) の 4 種類の曲線に注目する．それぞれの曲線における ECDLP の計算コストを比較する際，真に公平な比較となるように $H(\mathbb{F}_{p^n}) \cong M(\mathbb{F}_{p^n}) \cong tE(\mathbb{F}_{p^n}) \cong W(\mathbb{F}_{p^n})$ とお互いに $\mathbb{F}_{p^n}$ 上で同型写像を持つ曲線の組を使用する．この章ではどのようにしてこれらの同型写像を得るか，また factor base を決定する部分空間 V として $\mathbb{F}_p$ を使用するとき，各曲線の factor base が 位数 2 の点の加算の下で不変であるかを明らかにする．

まずは Hessian 曲線 H_d から考える．この曲線は $d \in \mathbb{F}_{p^n}$ を用いて $x^3 + y^3 + 1 = 3dxy$ を満たす．特筆すべき点として有理点の数 $\#H_d(\mathbb{F}_{p^n})$ が 12 で割れるものを選択する．3.4 章で述べた内容から，一般的な H_d において factor base は位数 2 の点の加算下で不変ではないことが分かる．

次に Hessian 曲線 H_d から $y^2 = x^3 + ax + b$ を満たす Weierstrass 曲線 $W_{a,b}$ を生成する．$a = -27d(d^3+8)$, $b = 54(d^6 - 20d^3 - 8)$ とすることで H_d と同型な $W_{a,b}$ を得ることができる [13]．同型写像 $\phi_{W,H} : W_{a,b}(\mathbb{F}_{p^n}) \to H_d(\mathbb{F}_{p^n})$ は $\mathbb{F}_{p^n}$ 上で定義されており，Weierstrass 曲線上の点 $(u,v) \in W_{a,b}$ を $(x,y) \in H_d$ に送る写像は以下で表せる．

$$\begin{cases} x = \dfrac{36(d^3-1) - v}{6(u + 9d^2)} - \dfrac{d}{2}, \\ y = \dfrac{36(d^3-1) + v}{6(u + 9d^2)} - \dfrac{d}{2}. \end{cases}$$

また逆写像は以下の通りである．

$$\begin{cases} u = \dfrac{12(d^3-1)}{d + x + y} - 9d^2, \\ v = \dfrac{36(d^3-1)(y-x)}{d + x + y}. \end{cases}$$

また Weierstrass 曲線上の factor base は位数 2 の点の加算下で不変ではない [4]．

さらに，以下の式に $W_{a,b}$ のパラメータを代入したものは高確率で解 A, B が存在する．これにより Weierstrass 曲線から $By^2 = x^3 + Ax^2 + x$ を満たす同型な Montgomery 曲線を生成できる．

$$\begin{cases} a = \dfrac{3 - A^2}{3B^2}, \\ b = \dfrac{2A^3 - 9A}{27B^3}. \end{cases}$$

同型写像 $\phi_{W,M}$ は $\mathbb{F}_{p^n}$ 上で定義されており，Weierstrass 曲線上の点 $(u,v) \in W_{a,b}$ は $x = Bu - 1/3A$, $y = Bv$ によって $(x,y) \in M_{A,B}$ に写像する．なお逆写像 $\phi_{M,W}$ は上記の等式を解くことで得られる． 3.1 章で述べたように，今回定義した factor base は $(0,0) \in M_{A,B}$ という位数 2 の点の加算下で不変である．

最後に，$a'x^2 + y^2 = 1 + d'x^2y^2$ を満たす twisted Edwards 曲線 $tE_{a',d'}$ を Montgomery 曲線 $M_{A,B}$ から得る．

$$\begin{cases} a' = \dfrac{A+2}{B}, \\ d' = \dfrac{A-2}{B}. \end{cases}$$

$a_0 = 1/(a' - d')$ に関して quadratic twist を計算する．同型写像 $\phi_{W,tE}$ は $\mathbb{F}_{p^n}$ 上で定義されており，$(u,v) \in W_{a,b}$ から $(x,y) \in tE_{a',d'}$ への写像は

$$\begin{cases} x = \dfrac{2a_0u}{v}, \\ y = \dfrac{u - a_0}{u + a_0}. \end{cases}$$

逆写像 $\phi_{tE,W}$ は

$$\begin{cases} u = \dfrac{a_0(1+y)}{1-y}, \\ v = \dfrac{2a_0^2(1+y)}{x(1-y)}. \end{cases}$$

となる．Faugère，Gaudry，Hout，Renault が述べたように位数 2 の点 $(0,-1) \in tE_{a',d'}$ の加算下で factor base は不変である [4]．

5. Experimental results

$\mathbb{F}_{q^n}$ 上の 4 つの曲線 Hessian, Weierstrass, Montgomery, twisted Edwards，それぞれの上で定義された ECDLP の解読の困難性を比較する実験を行った．真に公平な比較のために， 4 章で述べたようにして互いに同型である 4 つの曲線の組を用意した．同じ組のそれぞれの曲線は同じ j 不変量を持ち，ECDLP を構成する部分群の位数も大きさの等しい素数とした．

指数計算法においてボトルネックとなるのはランダムな点の分解式を得る部分である．従ってこの実験では summation polynomial から成る多項式システムを解く際に用いる F4 アルゴリズムのコストに注目した．なお 2 章で述べたように，多項式システムを構成する際には基本対称式による書き換えおよび Weil restriction を適用した．また全ての実験は数式処理ソフトウェアである MAGMA(version 2.23-1) を用いて実装し，2 GHz の Intel Xeon CPU E7-4830 v4

上でコア数を 1 として実行した．

解読の困難性の指標として，実行時間，Dreg，Matcost，以上の 3 つを用いた．“ Dreg ”とは，F4 アルゴリズムにおける step degree の最大値を指す．これは F4 アルゴリズムにおける Macaulay 行列の大きさの上界であり，“ Degree of regularity ”と呼ばれる [6]．また“ Matcost ”とは MAMGA の F4 アルゴリズムの出力値の 1 つであり，アルゴリズム中に実行される線形代数部分のコストを表すものである．

それらに加えて，多項式システムを 1 度解くにあたって得られる線型独立な関係式の個数を“ Rank ”とし，各種曲線をこの観点から比較した．指数計算法ではガウスの消去法を用いて解を求めるために $\mathcal{F}$ 本の線型独立な点の分解式が必要となる．よって Rank の値が大きいほど点の分解式を得る計算回数が減り，指数計算法全体にかかるコストは小さくなると言える．

さて，以下に $n = 5$ とし，factor base を決定する部分空間 V として楕円曲線の定義体 $\mathbb{F}_{p^n}$ の基礎体である $\mathbb{F}_p$ を用いた実験結果を示す．

表 1 $m = 3$

q	Curve	Time	Dreg	Matcost	Rank
251	Hessian	0	6	41420.4	1
	Weierstrass	0	6	42132.0	1
	Montgomery	0	6	61127.9	4
	tEdwards	0	6	6308.4	4
239	Hessian	0	6	42336.8	1
	Weierstrass	0	6	41259	1
	Montgomery	0	6	61239	4
	tEdwards	0	6	6308.36	4

表 2 $m = 4$

q	Curve	Time	Dreg	Matcost	Rank
251	Hessian	3.459	19	12069800000	1
	Weierstrass	3.659	19	12066400000	1
	Montgomery	3.280	18	11401700000	5
	tEdwards	0.119	18	54102900	5
239	Hessian	3.990	19	12066100000	1
	Weierstrass	3.680	19	12064700000	1
	Montgomery	3.489	18	11399100000	5
	tEdwards	0.150	18	54093000	5

表 1,2 より，異なる q や m について明らかに twisted Edwards 曲線が他の 3 つの曲線よりも実行時間が短いことが分かる．?章で述べたように, Dreg に注目すると特に $m = 4$ のとき Hessian, Weierstrass 曲線よりも Montgomery, twisted Edwards 曲線の方が小さい．また，Hessian, Weierstrass 曲線において Rank はどの場合も 1 であるのに対し Montgomery, twisted Edwards 曲線ではより大きな値になっている．

6. 考察

まず，twisted Edwards 曲線における実行時間が他の曲線に比べ明らかに短いことについて考察する．Faugère, Gaudry, Hout, and Renault らの論文 [5] の 4.1.1 章には，多項式システムの次数が小さくなることによって，twisted Edwards や twisted Jacobi intersection 曲線上の多項式システムは Weierstrass 曲線よりも高速に計算できると述べられている．しかしこれは，他の 2 曲線より Dreg が等しく小さい Montgomery，twisted Edwards 曲線の間で実行時間に大きな差があることを説明することができない．従って，twisted Edwards 曲線における高速化をもたらしたものは多項式システムに含まれる項数の違いであると考える．

表 3 number of terms (experimental/theoretical) in polynomial systems before Weil decent

m	Curve	before Weil decent		
		total	odd	even
2	Hessian	6/6	2/2	4/4
	Weierstrass	6/6	2/2	4/4
	Montgomery	6/6	2/2	4/4
	tEdwards	4/6	0/2	4/4
3	Hessian	35/35	16/16	19/19
	Weierstrass	35/35	16/16	19/19
	Montgomery	35/35	16/16	19/19
	tEdwards	25/35	6/16	19/19
4	Hessian	495/495	240/240	255/255
	Weierstrass	495/495	240/240	255/255
	Montgomery	495/495	240/240	255/255
	tEdwards	255/495	0/240	255/255

表 4 number of terms (experimental/theoretical) in polynomial systems after Weil decent

m	Curve	after Weil decent		
		total	odd	even
2	Hessian	5.2/6	2/2	3.2/4
	Weierstrass	5.2/6	2/2	3.2/4
	Montgomery	5.2/6	2/2	3.2/4
	tEdwards	3.2/6	0/2	3.2/4
3	Hessian	34.2/35	16/16	18.2/19
	Weierstrass	34.0/35	16/16	18.0/19
	Montgomery	33.4/35	16/16	17.4/19
	tEdwards	23.4/35	6/16	17.4/19
4	Hessian	493.2/495	239.4/240	253.8/255
	Weierstrass	492.0/495	238.4/240	253.6/255
	Montgomery	492.2/495	239.2/240	253.0/255
	tEdwards	253.0/495	0.0/240	253.0/255

表 4 に Weil restriction を適用する前後における各種曲線上の多項式システムの密度を $m = 2, 3, 4$ それぞれの場合についてまとめた．Weil restriction によって n 本の等

式が得られるため，数字は平均値とした．加えて表には m 変数 $2^{(m+1)-2}$ 次の多項式が持てる最大項数を記した．

全ての場合において，twisted Edwards 曲線は他の曲線よりも明らかに項数が少ない．このことから，F4 アルゴリズムにおいて使用される行列の大きさがより小さくなり高速な実行時間を実現したと推測できる．

さらに，曲線によってどのような単項式が存在しているのか明らかにするため，曲線それぞれの多項式システムに含まれる単項式を次数の偶奇によって分類した．なお多項式システムで使われている変数は基本対称式 $e_1, \ldots, e_m$ によって書き換えられているため，e_i^j について，i と j の両方が奇数である場合，その変数の次数は奇数であるとした．

$m = 2$ のとき，twisted Edwards 曲線には奇数次数の単項式は存在しないことが分かる．つまり例えば e_1 や e_1e_2 といった単項式が生成されることがない．これは summation polynomial を導出する際に使用する加算公式において全ての単項式が偶数次数であることに起因する．すなわち 3 変数の summation polynomial をある変数に関する 1 変数多項式として見た場合 1 次の項全体は奇数次数であるが，その変数に分解する点の y 座標を代入するため，結果として偶数次数になるのである．

$m = 3$ のとき，4 変数の summation polynomial を使用するが，これは 2 つの 3 変数 summation polynomial の終結式によって計算される．従って e_3 や $e_2^2e_3$ といったいくつかの奇数次数の単項式が存在する．$m = 4$ もまた偶数次数の単項式は存在しない．終結式を再帰的に計算する過程で共通因子とされる 2 つの変数が消去されるため全ての単項式が偶数次数になると考えられる．

次に，Rank の値について考察する．summation polynomial は足して無限遠点となる点の組でありさえすれば，その点に対応する x 座標や y 座標，または $x + y$ の値が解となる．そのため多項式システムには足して無限遠点になる点の組み合わせ全てに対応する個数の解が存在する．例えば楕円曲線上の点の加算は可換であるから，常に $m!$ の倍数個の解を持つ．また factor base が位数 2 の点の加算下で不変であれば，3 章で述べたように 2^{m-1} の倍数個の解を持つ．ただし，置換作用で生成された異なる $m!$ 個の関係式は線型従属であるため，Rank の値は factor base が位数 2 の点の加算下で不変であるかどうかに依存する．

4 章で述べたように，Montgomery 曲線と twisted Edwards 曲線における factor base は位数 2 の点の加算下で不変である．よって 1 つの分解式に対し，2^{m-1} 個の異なる分解式が存在する．$m = 3$ のとき，2 曲線の Rank は $2^{3-1} = 4$ であり上記を満たすが，$m = 4$ のときは Rank が $2^{4-1} = 8$ ではなく 5 であり仮定に反する．ここで $i = 1, 2, 3, 4$ について $Q_i = P_i + T_2$ とすると，存在する 8 本の関係式は以下のように書ける．

$$\begin{aligned} P_1 + P_2 + P_3 + P_4 &= Q_1 + Q_2 + P_3 + P_4 \\ = Q_1 + P_2 + Q_3 + P_4 &= Q_1 + P_2 + P_3 + Q_4 \\ = P_1 + Q_2 + Q_3 + P_4 &= P_1 + Q_2 + P_3 + Q_4 \\ = P_1 + P_2 + Q_3 + Q_4 &= Q_1 + Q_2 + Q_3 + Q_4. \end{aligned}$$

このうち，

$$\begin{aligned} &(P_1 + P_2 + P_3 + P_4) - (Q_1 + Q_2 + P_3 + P_4) \\ &\quad - (P_1 + P_2 + Q_3 + Q_4) + (Q_1 + Q_2 + Q_3 + Q_4) = \mathcal{O} \end{aligned}$$

という線形式が存在するため，8 本のうち線型独立な関係式は 5 本のみであることが分かる．

7. 結論

本論文では，$\mathbb{F}_{p^n}$ 上で互いに同型写像を持ちながら曲線式が異なる 4 つの曲線に関して ECDLP の解読の困難性を比較した．一見，等しい困難性を持つはずであるが，MAGMA による実装実験により twisted Edwards 曲線における ECDLP は異なる q, m に関して十分に高速に解読可能であることを示した．さらにそれは，多項式システム中の単項式数が他の 3 曲線に比べて常に少ないためであることを明らかにした．twisted Edwards 曲線はその加算公式が偶数次数の単項式のみで構成されているために，加算公式を元にして導出される summation polynomial においても生じる奇数次数の単項式が少ないことがその原因であった．

また，factor base を決定する部分空間 V を基礎体 $\mathbb{F}_p$ とした場合，Montgomery 曲線や twisted Edwards 曲線において位数 2 の点の加算作用下で不変であるため，指数計算法をより高速に実行可能であることを裏付けた．

8. おわりに

謝辞 本研究の一部は JSPS 科研費基盤 C (JP15K00183) と (JP15K00189) 及び科学技術振興機構（JST）の CREST(JPMJCR1404) と国際科学技術協力基盤整備事業 及び文部科学省の情報技術人材育成のための実践教育ネットワーク形成事業分野・地域を越えた実践的情報教育協働ネットワークの助成を受けています．

参考文献

[1] Daniel J. Bernstein, Peter Birkner, Marc Joye, Tanja Lange, and Christiane Peters. Twisted Edwards Curves. *IACR Cryptology ePrint Archive*, Vol. 2008, p. 13, 2008.

[2] Daniel J. Bernstein and Tanja Lange. Faster addition and doubling on elliptic curves. *IACR Cryptology ePrint Archive*, Vol. 2007, p. 286, 2007.

[3] Claus Diem. On the discrete logarithm problem in class groups of curves. *Math. Comput.*, Vol. 80, No. 273, pp. 443–475, 2011.

[4] Jean-Charles Faugère, Louise Huot, Antoine Joux, Gu'ena"el Renault, and Vanessa Vitse. Symmetrized Summation Polynomials: Using Small Order

Torsion Points to Speed Up Elliptic Curve Index Calculus. In *Advances in Cryptology - EUROCRYPT 2014 - 33rd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Copenhagen, Denmark, May 11-15, 2014. Proceedings*, pp. 40–57. Springer, 2014.

[5] Jean-Charles Faugère, Ludovic Perret, Christophe Petit, and Gu'ena"el Renault. Improving the Complexity of Index Calculus Algorithms in Elliptic Curves over Binary Fields. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, pp. 27–44. Springer, 2012.

[6] Steven D. Galbraith and Shishay W. Gebregiyorgis. Summation Polynomial Algorithms for Elliptic Curves in Characteristic Two. In *Progress in Cryptology - INDOCRYPT 2014 - 15th International Conference on Cryptology in India, New Delhi, India, December 14-17, 2014, Proceedings*, pp. 409–427. Springer, 2014.

[7] Pierrick Gaudry. Index calculus for abelian varieties of small dimension and the elliptic curve discrete logarithm problem. *J. Symb. Comput.*, Vol. 44, No. 12, pp. 1690–1702, 2009.

[8] Yun-Ju Huang, Christophe Petit, Naoyuki Shinohara, and Tsuyoshi Takagi. Improvement of Faugère et al.'s Method to Solve ECDLP. In *Advances in Information and Computer Security - 8th International Workshop on Security, IWSEC 2013, Okinawa, Japan, November 18-20, 2013, Proceedings*, pp. 115–132. Springer, 2013.

[9] Peter L. Montgomery. Speeding the Pollard and elliptic curve methods of factorization. *Mathematics of Computation*, Vol. 48, pp. 243–264, 1987. URL: http://links.jstor.org/sici?sici=0025-5718(198701)48:177<243:STPAEC>2.0.CO;2-3.

[10] Christophe Petit and Jean-Jacques Quisquater. On Polynomial Systems Arising from a Weil Descent. *IACR Cryptology ePrint Archive*, Vol. 2012, p. 146, 2012.

[11] John M. Pollard. Monte Carlo methods for index computation mod *p*. *Mathematics of Computation*, Vol. 32, pp. 918–924, 1978.

[12] Igor A. Semaev. Summation polynomials and the discrete logarithm problem on elliptic curves. *IACR Cryptology ePrint Archive*, Vol. 2004, p. 31, 2004.

[13] Nigel P. Smart. The Hessian Form of an Elliptic Curve. In *Cryptographic Hardware and Embedded Systems - CHES 2001, Third International Workshop, Paris, France, May 14-16, 2001, Proceedings*, No. Generators, pp. 118–125. Springer, 2001.