数理解析研究所講究録
1098巻 1999年 138-146

楕円曲線暗号

Elliptic curve cryptosystems

宮地 充子

Atsuko Miyaji

北陸先端科学技術大学院大学
情報科学研究科

〒923-1292 石川県能美郡辰口町旭台 1-1

School of information science
Japan Advanced Institute of Science and Technology

1-1, Asahidai, tatsunokuchi, Nomi, Ishikawa, 923-1292, Japan
Email:miyaji@jaist.ac.jp

1 はじめに

1985年に楕円曲線に基づく公開鍵暗号が発表された ([8, 13]) . この公開鍵暗号は楕円曲線上の離散対数問題 (EDLP) の難しさを安全性の根拠にする暗号である. 一般に楕円曲線暗号とは, EDLP に基づく公開鍵暗号を指す. EDLP は有限体上の離散対数問題 (DLP) に対する強力な解法である「指数計算法 (Index Calculus) 」が直接適用できないことから, 有望な公開鍵暗号として盛んに研究されるようになった. なおこれとは別に, 1986年に環上の楕円曲線を素因数分解に用いる手法 ([10]) が発表されている. また1991年には, 楕円曲線を用いたRSA暗号及びRabin暗号が発表されている ([7]) . さらに, 種数2以上の代数曲線 (楕円曲線は種数1) を用いた暗号も検討されている ([9, 11]). このようにして整数論の長年の研究テーマの1つであった代数曲線が暗号分野に応用されるようになった.

本稿では, 楕円曲線暗号の基本原理について簡単に述べる. 楕円曲線暗号に関して, 詳しく知りたい読者は [19] を, また, 楕円曲線について興味を持たれた読者は, [29] を読まれることをお薦めする.

2 楕円曲線

まず楕円曲線について簡単に述べる. 楕円曲線とは, $a, b \in \boldsymbol{K}$ (体) に対して,

$$\boldsymbol{E} : y^2 = x^3 + ax + b \tag{1}$$

で定まる曲線である. ここで $4a^3 + 27b^2 \neq 0$ とし, $\boldsymbol{K}$ の標数は5以上とする. 標数が2または3の場合の楕円曲線の標準形については, [26] を参照されたい. 楕円曲線は (1) を満たす点の集合であるが, $x \to \infty$ のとき $y \to \infty$ と考えて, 無限遠点 $\mathcal{O} = (\infty, \infty)$ も $\boldsymbol{E}$ の点と考える. 特に, 楕円曲線の $\boldsymbol{K}$-有理点の集合を,

$$\boldsymbol{E}(\boldsymbol{K}) = \{(x, y) \in \boldsymbol{K}^2 | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

とする. 楕円曲線のパラメータ a, b を含む体 $\boldsymbol{K}$ を楕円曲線の定義体と呼ぶ. 楕円曲線には $\mathcal{O}$ が零元になるような加法が定義できる. 楕円曲線上の2点 $A = (x_1, y_1)$ と $B = (x_2, y_2)$ に対し, $A + B$ を, A と B を結ぶ直線と楕円曲線とのもう一つの交点の x 軸に対称な点と定義する. $\boldsymbol{K}$ として実数体を用いたとき. 加法は 図1 のように表され

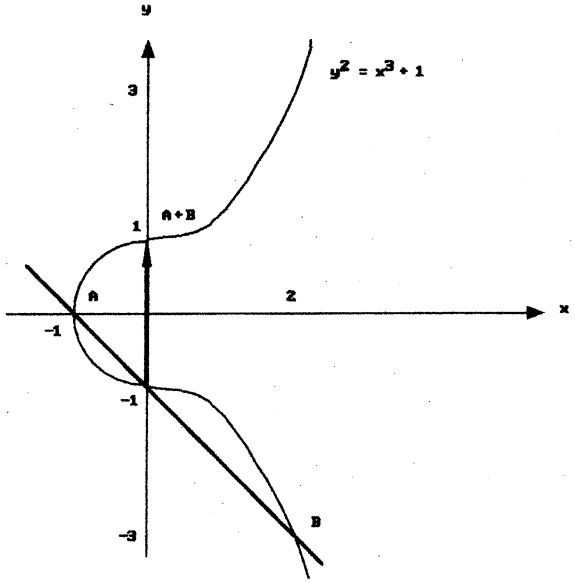

図 1: 楕円曲線上の加算

る．楕円曲線の加算の利点は，幾何学的に定義された加算が有理式で書き下せる点である．実際，$A \neq B$ に対して，$C = (x_3, y_3) = A + B$ は，以下の式で計算できる．

$$\begin{aligned} x_3 &= (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2 \\ y_3 &= \frac{y_2 - y_1}{x_2 - x_1}(x_1 - x_3) - y_1 \end{aligned} \tag{2}$$

$A = B$ のとき，$C = (x_3, y_3) = 2A$ は，以下の式で計算できる．

$$\begin{aligned} x_3 &= (\frac{3x_1^2 + a}{2y_1})^2 - 2x_1 \\ y_3 &= \frac{3x_1^2 + a}{2y_1}(x_1 - x_3) - y_1 \end{aligned} \tag{3}$$

3 楕円曲線暗号

楕円曲線暗号は，有限体 $\boldsymbol{K} = GF(q) = \mathbb{F}_q$ ($q = p^r, p$: 素数, r : 自然数) 上定義された楕円曲線を用いる．加算は，加算公式 (2), (3) を $\boldsymbol{K}$ 上計算するとよい．この加法により $\boldsymbol{E}(\boldsymbol{K})$ は有限可換群になり，暗号に重要な離散対数問題 (EDLP) が定義できる．ここで，EDLP の定義について述べる．

Definition 1 p を素数，r を自然数，$q = p^r$ とし，有限体 $\mathbb{F}_q$ 上の楕円曲線 $\boldsymbol{E}/\mathbb{F}_q$，$\boldsymbol{E}(\mathbb{F}_q) \ni G, Y$ に対して，

$$Y = xG = G + \cdots + G \ (G \text{ の } x \text{ 回の和})$$

なる x が存在するなら，その x を求めよ．

離散対数問題は，任意の有限群とその群演算を用いて定義できる．有限体とその乗法に対する離散対数問題が DLP であり，楕円曲線とその加法に対する離散対数問題が EDLP である．

次に具体的に楕円曲線を利用した暗号プロトコルとして鍵共有法を説明する．以下 $\boldsymbol{E}/\boldsymbol{K}$ を楕円曲線とし，$G \in \boldsymbol{E}(\boldsymbol{K})$ を位数 ($lG = \mathcal{O}$ となる最小の正整数 l) が大きな素数 l の元 (ベースポイント) とする．また $\boldsymbol{E}(\boldsymbol{K})$ 及び G はシステム内で公開する．

• **ユーザ A の鍵生成**

1. 乱数 $x_A \in \mathbb{Z}_l^*$ を選ぶ.
2. $P_A = x_A G$ を計算する.
3. x_A を秘密鍵, P_A を公開鍵として出力する.

ユーザ B も同様に鍵 (x_B, P_B) を生成する.

• **ECDH** (楕円 DH 鍵共有法)

A と B が通信なしに, それぞれの公開鍵 P_A, P_B を利用して, 鍵を共有する場合を考える.

1. A は公開ファイルから B の公開鍵 P_B を取ってきて $\boldsymbol{E}$ 上で

$$K_{A,B} = x_A P_B = x_A x_B G$$

を計算する.

2. B は公開ファイルから A の公開鍵 P_A を取ってきて $\boldsymbol{E}$ 上で

$$K_{B,A} = x_B P_A = x_B x_A G$$

を計算する.

3. A と B は $\boldsymbol{E}(\boldsymbol{K})$ の元 $K_{A,B} = K_{B,A}$ を鍵として共有する.

実際のシステムでは, 楕円曲線の定義体は 160 ビット程度の大きさに, 位数は 160 ビット程度の素数になるようにとる. 次章で述べるが, ある種の楕円曲線を除き, このような EDLP は, 現在最も効率のよい解読法で 10^{12} MIPS 年かかると考えられている. つまり, 1000MIPS の PC を 1 万台 用いても, 解法に 10^5 年かかることになる. また, 鍵共有の機能だけでなく, 署名生成／検証の機能も実現することができる. 詳しくは [19, 14] を参照されたい.

4 楕円曲線暗号の安全性について

この章では, 楕円曲線暗号の安全性の根拠である EDLP に対する攻撃法について述べる. これまで同様, 有限体を $\boldsymbol{K} = \mathbb{F}_q$, 楕円曲線を $\boldsymbol{E}/\boldsymbol{K}$, ベースポイントを $G \in \boldsymbol{E}(\boldsymbol{K})$, その位数を l と表す. EDLP に対する攻撃は, DLP も含め任意の群上の離散対数問題に対して有効な攻撃法と EDLP に固有な攻撃法の 2 つに分類できる. EDLP と DLP の攻撃の違いは, それぞれに固有な攻撃法の適用範囲の違いである. 本章では, 一般的な攻撃法について述べたあと, EDLP と DLP の攻撃の違い及び EDLP に固有な攻撃法について述べる.

4.1 離散対数問題に対する一般的な攻撃法

[20, 21, 28] は, 離散対数問題のベースとなる群に依らず, ベースポイントの位数 l に依存する攻撃である. 具体的に, 位数 l が $l = p_1^{r_1} \cdots p_n^{r_n} (p_1 > \cdots > p_n)$ と素因数分解されるとき, $O(\sum_{i=1}^{n} r_i \sqrt{p_1})$ の計算時間がかかる. この攻撃を効率的に回避するには, l が大きな素数であるようにとっておくとよい. この場合, 計算時間は $O(\sqrt{l})$ になる. 例えば, l が 160 bits の大きさの素数である場合, この攻撃にかかる時間のオーダは 2^{80} ということになり, 現実的な時間での解読は不可能になる. [28] の攻撃は, [20, 21] の方法をパラレルに実行する攻撃法で, m 個のプロセッサをパラレルに走らせた場合, 攻撃時間のオーダは, $O(\sqrt{l}/m)$ になる.

いずれにしてもこの攻撃は, 指数時間 (exponential time) の攻撃となり現実的な脅威にはならない.

4.2 DLP に対する攻撃との違い

EDLP と DLP に対する現状の攻撃の違いを簡単に述べる. DLP に対する攻撃は, 有限体 $\boldsymbol{K}$ の選択とは無関係に適用可能な攻撃である. 指数計算法 ([1]) やその改良は, 任意の有限体に対して準指数時間 (sub-exponential time) の攻撃を与える. このため, 10^{12} MIPS 年の安全性を確保するには 1,024 ビットの大きさの有限体が必要になる.

一方 EDLP には，前章で述べた指数時間攻撃を除くと，DLP のような汎用的な攻撃はまだ提案されていない．さらに楕円曲線は，一つの有限体上にたくさんの有限群を構成できるという性質をもつ．厳密に述べると，$\boldsymbol{K}$ 上定義された楕円曲線の元の個数は，以下の式を満たす (Hasse の定理 [26])

$$|q+1-\#\boldsymbol{E}(\boldsymbol{K})| \leq 2\sqrt{q}.$$

逆に，上記の範囲の元の個数を持つ楕円曲線が存在する．ここで，$t = q+1-\#\boldsymbol{E}(\boldsymbol{K})$ は楕円曲線のトレースと呼ばれる．つまり，$\boldsymbol{K}$ 上の楕円曲線は $|t| \leq 2\sqrt{q}$ 個の有限群を提供できる．楕円曲線に対する攻撃は，この t の値により異なる．

有限体 $\boldsymbol{K}$ が素体 $\mathbb{F}_p$ の場合，攻撃状況を図示しやすい．図 2 は，素体 $\mathbb{F}_p$ 上の楕円曲線に提案されている攻撃を表す．図は，$t=1$ のとき EDLP は $\mathbb{F}_p$ の加法群 $\mathbb{F}_p^+$ に，$t=0,2$ のとき $\mathbb{F}_p$ の拡大体の乗法群 $\mathbb{F}_{p^n}^*$ に帰着されることを意味する．$t \neq 0,1,2$ では楕円曲線 $\boldsymbol{E}/\mathbb{F}_p$ 上の EDLP に，このような帰着法は提案されていない．

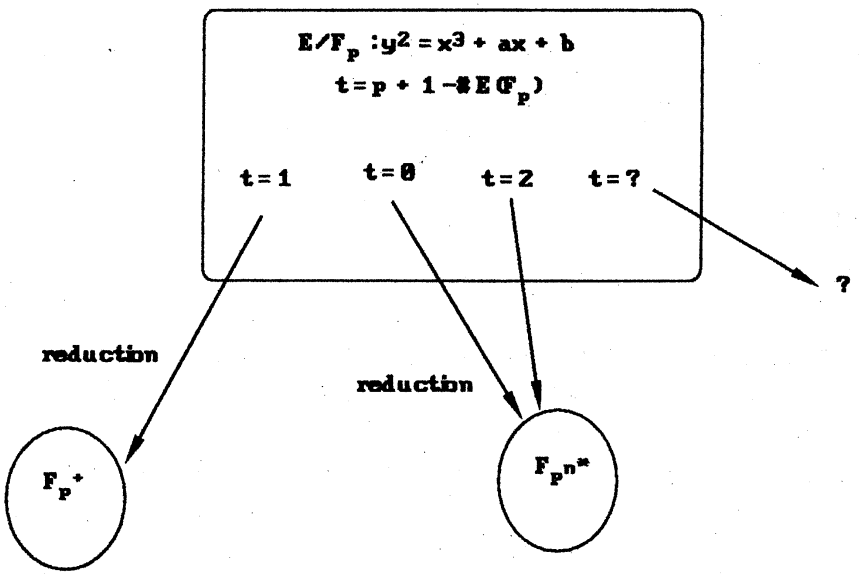

図 2: security hole

4.3 EDLP に固有な攻撃法

楕円曲線 $\boldsymbol{E}/\boldsymbol{K}$ に固有な攻撃について述べる．ここでベースポイントの位数 $l = p^t \cdot m\,(\gcd(m,p)=1)$ と表す．ここで p は定義体 $\boldsymbol{K}$ の標数であり，一般性を失うことなく m は素数としてよい．$<G>$ に関する EDLP は，chinese remainder theorem などを用いることにより，位数 p の p-群 $<mp^{t-1}G>$ に関する EDLP と位数が p と互いに素な群 $<p^tG>$ に関する EDLP を解くことに帰着する．ここで，$<G>=\{G,2G,\cdots,(l-1)G,\mathcal{O}\}$ とは G により生成される群を表す．

4.3.1 乗法群への帰着攻撃

まず乗法群への帰着攻撃について述べる．この攻撃は，1990 年に Menezes, Okamoto 及び Vanstone によって楕円曲線に対して提案され[1] (MOV-reduction [17])，Frey-Rück により任意の種数の代数曲線に対して拡張された (FR-reduction [4])．どちらの攻撃も，位数が p と互いに素な群 $<p^tG>$ に関する EDLP をもとめるアルゴリズムである．

[1] Semaev によっても独立に提案されていたことが後にわかった ([24]).

位数が m の集合を $\boldsymbol{E}[m]=\{T\in\boldsymbol{E}|mT=\mathcal{O}\}$ と表すと，$<p^tG>=\boldsymbol{E}[m]\cap\boldsymbol{E}(\boldsymbol{K})$ となる．$\boldsymbol{E}[m]\cap\boldsymbol{E}(\boldsymbol{K})$ に関する EDLP を Weil 対 ([26]) を利用して $\boldsymbol{K}$ の n 次拡大体 $\boldsymbol{L}$ の乗法群 $\boldsymbol{L}^*$ に帰着させるのが MOV-reduction であり Tate 対を利用するのが FR-reduction である．Weil 対, Tate 対共に非退化な双線形関数であり，確率的多項式時間で計算可能なので，$\boldsymbol{E}[m]$ に関する EDLP は，$\boldsymbol{L}^*$ に関する DLP に帰着する．4.2 章で述べたように，DLP には準指数時間の攻撃が存在する．よって $\boldsymbol{L}$ の拡大次数 $n<\log^2 q$ となる時，この帰着攻撃は準指数時間攻撃となる．実際，準指数時間攻撃になるのは，楕円曲線が supersingular([26]) である場合と $t=2$ の場合である．素体 $\mathbb{F}_p$ の場合，supersingular 楕円曲線は $t=0$ となるため，図 2 のように $t=0,2$ の場合が問題になる．

ここで，MOV-reduction と FR-reduction における拡大体 $\boldsymbol{L}$ の条件について述べる．MOV-reduction の場合，$\boldsymbol{L}\supset\boldsymbol{E}[m]$ を満たす最小の体であるのに対し，FR-reduction では $\boldsymbol{L}\supset\mu_m=\{1\text{ の }m\text{ 乗根}\}$ を満たす最小の体になる．一般に

$$\boldsymbol{L}\supset\boldsymbol{E}[m]\Rightarrow\boldsymbol{L}\supset\mu_m$$

であるが，その逆は成り立たない．この顕著な例が，$t=2$ の場合である．MOV-reduction は，$t=2$ の場合，準指数時間攻撃にならないが，FR-reduction は準指数時間攻撃になる．楕円曲線上においては，$t=2$ の場合を除き，MOV-reduction と FR-reduction は等価であることが，[2] より容易に導かれる．

4.3.2 加法群への帰着攻撃

次に加法群への帰着攻撃について述べる．これは，p-群に関する EDLP をターゲットにした攻撃である．この攻撃アルゴリズムには，2 つのアプローチがある．1 つは，1995 年に Semaev により提案され，Rück により任意の種数の代数曲線上の離散対数問題へ一般化された SR 攻撃である ([25, 22])．SR 攻撃は，代数幾何学的アプローチである．もう 1 つは，1997 年に Smart([27]), 佐藤, 荒木 ([23]) により独立に提案された SSA 攻撃である．SSA 攻撃は，数論的アプローチである[2]．後者については解説文献も多いので，ここでは，SR 攻撃について簡単に述べる．

楕円曲線 $\boldsymbol{E}$ は，次数 0 の divisor 群の principal divisor による商群，Divisor 類群 $Pic^0(\boldsymbol{E})$ と同型になる ([26])．このことから，$<mp^{t-1}G>\ni Q$ に対応する divisor，$D_Q=(Q)-(\mathcal{O})$ に対して，pD_Q は principal divisor となる．すなわち，ある関数 f_Q に対して，$pD_Q=(f_Q)$ となる．p-群の場合には，f_Q と $R(\neq\mathcal{O})\in<mp^{t-1}G>$ を用いて，

$$\phi:<mp^{t-1}G>\ni Q\longmapsto(f'_Q/f_Q)(R)\in\boldsymbol{K}$$

と定義すると，ϕ は $O(\log p)$ で計算可能な $\boldsymbol{K}$ の加法群への単射準同型となる．つまり，$<mp^{t-1}G>$ に関する離散対数問題は，$\boldsymbol{K}$ の加法群に関する離散対数問題に帰着する．有限体 $\boldsymbol{K}$ の加法群に関する離散対数問題は多項式時間で解読できるので，p-群の EDLP は，多項式時間で攻撃できることになる．この攻撃は，p-群にのみ有効なので容易に回避できる．

4.4 楕円曲線暗号の設計

前章までの EDLP に対する攻撃についてまとめる．楕円曲線 $\boldsymbol{E}/\boldsymbol{K}$ は，元の個数 $\#\boldsymbol{E}(\boldsymbol{K})$ が以下の 3 つの条件を満たすように構成すると，現時点では安全になる．

1. $\#\boldsymbol{E}(\boldsymbol{K})$ は，大きな素数 l と小さな正整数 t で，$\#\boldsymbol{E}(\boldsymbol{K})=l\cdot t$ と表される．このとき，$\#\boldsymbol{E}(\boldsymbol{K})$ は almost prime と呼ぶ．(4.1 章の攻撃)
2. $1<n<(\log q)^2$ の整数 k に対し，$l\not|(q^n-1)$ である．(4.3.1 章の攻撃)
3. l と p は互いに素である．(4.3.2 章の攻撃)

上記 3 つの条件を満たす楕円曲線 $\boldsymbol{E}/\boldsymbol{K}$ に対し，位数 l の点 G をベースポイントとしてとるとよい．現時点では，l は 160 ビット以上の大きさが必要と考えられている．

[2]加法群への帰着攻撃は，攻撃方法は異なるが，楕円曲線上の攻撃として SSSA 攻撃と呼ばれることもある．

5 楕円曲線の演算アルゴリズム

本章では，楕円曲線のべき演算アルゴリズムについて述べる．3章からわかるように，楕円曲線暗号の実行時間は楕円曲線のベキ演算アルゴリズムに支配される．

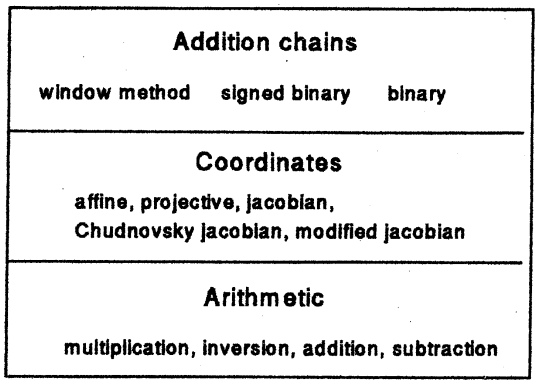

図 3: security hole

楕円曲線のべき演算アルゴリズムは，図3のように3つのレイヤ，定義体上の演算 (arithmetic)，座標系 (coordinates)，加算連鎖 (addition-chains) からなる．ここでは，第3レイヤの加算連鎖と第2レイヤの座標系について簡単に述べる．

5.1 加算連鎖

本章で述べる加算連鎖とは，楕円曲線 $E/\boldsymbol{K}$ のべき演算 $kP(P \in E(\boldsymbol{K}))$ の計算方法である．ベキ演算の手法は，G がベースポイントのような固定値の場合と公開鍵のような任意値の場合とで異なる．後者の任意値の場合，符号付2進法 (signed binary) と window 法を組み合わせるのが一般的である ([18, 6, 15, 16])．ここでは，この2手法について簡単に述べる．

符号付2進法

符号付2進法とは，k を $\{0, \pm 1\}$ の3情報で表すことにより，0 以外 (すなわち ± 1) の立つビット数を減らすというアイデアである．

Example 1 $k = (10\text{進})15 = (2\text{進})1111$ の符号付2進法を考える．通常の2進法では，$15G$ の計算に，$15G = 2(2(2G+G)+G)+G$ より3回の2倍算と3回の加算が必要である．k を符号付2進法で表すと，

$$k = (10\text{進})15 = 16 - 1 = (\text{符号付}2\text{進})1000\bar{1}$$

なる．このとき，$15G$ は

$$15G = 2^4G - G$$

より，4回の2倍算と1回の減算により求められる．このようにして，総計算回数を減らすことができる．

符号付2進法の表し方は一意的でないので，いくつかの方法が提案されている ([18, 6, 15])．

window 法 ([5])

window 法は window の幅を w とするとき，kP の計算を以下の2ステップで行なう．

(1) $P_l = lP(l \in \{1, 3, \cdots, 2^w - 1\})$ を計算する．(予備計算テーブル作成)

(2) kP を2倍算と (1) の予備計算テーブル $\{P_l\}$ との加算を繰り返すことにより求める．

Example 2 $k=$(2進)1011111, $w=4$ の場合を考える.
(1) $P_l = lP(l \in \{1,3,\cdots,15\})$ を求める.
(2) $kP = 1011\ \ 111\, P = 2^3 P_{11} + P_7$ として計算する. ここで, 1011 や 111 を *window* と呼ぶ.

window の幅は, 総計算量 (予備計算テーブル作成の計算量も含む) が最小になるように設定する.

楕円曲線のべき演算は, 符号付き 2 進法と window 法を組み合わせる. この組み合わせ方には, 以下の 2 つの案が提案されている.
(1) k を符号付 2 進法で表し, 次に window に分割する方法. ([6])
(2)window の幅 w により, 符号付 2 進法を決定する方法 ([16]).
総計算量は後者の方が少なくなる.

5.2 座標系

楕円曲線の表し方には, 大きくアファイン座標系 (1) と射影座標系がある. 2 章の座標系がアファイン座標系である. 2 章でみたように, アファイン座標系では加算及び2倍算が定義体上の除算を必要とする. 除算は乗算に比べ時間がかかるので, 除算演算が不要な射影座標系を利用する場合が多い.

射影座標系には, $(x,y)=(X/Z,Y/Z)$ の変換を行う座標系 (projective 座標系) と $(x,y)=(X/Z^2,Y/Z^3)$ の変換を行う座標系 (jacobian 座標系) がある ([3, 15]). 2つの座標系を比べると, 加算は projective 座標系が早く, 2倍算は jacobian 座標系が早い. 楕円曲線のべき演算は加算より 2 倍算を多く要求するので, jacobian 座標系がべき演算には適している. また jacobian 座標系は, 保持するパラメータを変えると, さらに2倍算の計算量を減らすことができる. ここでは jacobian 座標系及び2倍算の計算量を減らした modified jacobian 座標系について述べる..

jacobian 座標系の楕円曲線は, (1) を $(x,y)=(X/Z^2,Y/Z^3)$ とおくことにより与えられる.

$$E_J : Y^2 = X^3 + aXZ^4 + bZ^6. \tag{4}$$

加算公式は以下のようになる. $P=(X_1,Y_1,Z_1)$, $Q=(X_2,Y_2,Z_2)$, $P+Q=R=(X_3,Y_3,Z_3)$ とおく.
• **加算公式** $(P \neq \pm Q)$

$$X_3 = -H^3 - 2U_1H^2 + r^2, Y_3 = -S_1H^3 + r(U_1H^2 - X_3), Z_3 = Z_1Z_2H,$$

ここで $U_1 = X_1Z_2^2, U_2 = X_2Z_1^2, S_1 = Y_1Z_2^3, S_2 = Y_2Z_1^3, H = U_2 - U_1, r = S_2 - S_1$ である.
• **2 倍算公式** $(R=2P)$

$$X_3 = T, Y_3 = -8{Y_1}^4 + m(s-T), Z_3 = 2Y_1Z_1,$$

ここで $s = 4X_1Y_1^2, m = 3X_1^2 + aZ_1^4, T = -2s + m^2$ である.

加算及び2倍算の計算量 $t(\mathcal{J},\mathcal{J})$, $t(2\mathcal{J})$ は, $t(\mathcal{J},\mathcal{J}) = 12M + 4S$, $t(2\mathcal{J}) = 4M + 6S$ となる. ここで, M 及び S はそれぞれ定義体上の乗算と 2 乗算の計算量を表す.

jacobian 座標系を (X,Y,Z,aZ^4) とする modified jacobian 座標系では, 加算及び2倍算の計算量 $t(\mathcal{J}^m,\mathcal{J}^m)$, $t(2\mathcal{J}^m)$ は, $t(\mathcal{J}^m,\mathcal{J}^m) = 13M + 6S$, $t(2\mathcal{J}^m) = 4M + 4S$ となる. 加算では aZ_3^4 を求める余分な計算量が必要になるが, 2 倍算では

$$aZ_3^4 = 2^4(Y_1^4)(aZ_1^4)$$

となることから, aZ^4 をもつことで計算量が削減できる. 楕円曲線のベキ演算の総計算量は, 2 倍算の計算量が少ないので, modified jacobian 座標系を用いた方が jacobian 座標系より小さくなる. さらに, いくつかの座標系を組み合わせる混合座標系も提案されている ([16]).

このように座標系の取り方により, 楕円曲線演算の総計算量が変化するいうのも楕円曲線の一つの魅力といえる.

6 おわりに

整数論の長年の研究テーマであった楕円曲線が，暗号理論においても重要な位置を占めるようになった．楕円曲線暗号は提案から10年が過ぎ，実用化及び標準化という新たな局面を迎えた．今後より一層の活発な研究が，理論面においても実用面においてもなされることと思われる．

参考文献

[1] L. M. Adleman, C. Pomerance and R. S. Rumely, "On distinguishing prime numbers from composite numbers", *Annals of Mathematics*, **117**(1983) 173-206.

[2] R. Balasubramanian and N. Koblitz, "Improbability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone Algorithm", to appear in Journal of cryptology.

[3] D. V. Chudnovsky and G. V. Chudnovsky "Sequences of numbers generated by addition in formal group and new primality and factorization tests" *Advances in Applied Math.*, **7**(1986), 385-434.

[4] G. Frey and H. G. Rück, "A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves", *Mathematics of computation*, **62**(1994), 865-874.

[5] D. E. Knuth, *The art of computer programming, vol. 2, Seminumerical Algorithms*, 2nd ed., Addison-Wesley, Reading, Mass. 1981.

[6] K. Koyama and Y. Tsuruoka, "Speeding up elliptic cryptosystems by using a signed binarY window method", *Abstract of proceedings of CRYPTO'92*, 1992.

[7] K. Koyama, U. M. Maurer, T. Okamoto and S. A. Vanstone, "New public-key schemes based on elliptic curves over the ring Zn", *Advances in Cryptology-Proceedings of CRYPTO'91*, Lecture Notes in Computer Science, **576**(1992), Springer-Verlag, 252-266.

[8] N. Koblitz, "Elliptic curve cryptosystems", *Mathematics of Computation*, **48**(1987), pp.203-209.

[9] N. Koblitz, "Hyperelliptic Cryptosystems", *Journal of Cryptology*, vol.1, No.3 (1989), pp.139-150.

[10] H. W. Lenstra, Jr. "Factoring integers with elliptic curves", Report 86-18, Mathematisch Instituut, Universiteit van Amsterdam, 1986.

[11] N. Matsuda, J.Chao, and S. Tsujii "Efficient construction algorithms of secure hyperelliptic discrete logarithm problems", *IEICE Japan Tech. Rep.*, **ISEC96-18**(1996).

[12] A. J. Menezes, *Elliptic curve public key cryptosystems*, Kluwer academic publishers, 1993.

[13] V. S. Miller, "Use of elliptic curves in cryptography", *Advances in Cryptology-Proceedings of Crypto'85*, Lecture Notes in Computer Science, **218** (1986), Springer-Verlag, pp.417-426.

[14] A. Miyaji, "Another countermeasure to forgeries over message recovery signature", *IEICE Trans.*, Fundamentals. vol. E80-A, No.11(1997).

[15] A. Miyaji, T. Ono, and H. Cohen "Efficient elliptic curve exponentiation", *Advances in Cryptology-Proceedings of ICICS'97*, Lecture Notes in Computer Science, **1334**(1997), Springer-Verlag, 282-290.

[16] A. Miyaji, T. Ono, and H. Cohen "Efficient elliptic curve exponentiation using mixed coordinates", *Advances in Cryptology-Proceedings of ASIACRYPT'98*, Lecture Notes in Computer Science, **1514**(1998), Springer-Verlag, 51-65.

[17] A. Menezes, T. Okamoto and S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", *Proceedings of the 22nd Annual ACM Symposium on the Theory of Computing*, pp.80-89, 1991.

[18] F. Morain and J. Olivos, "Speeding up the computations on an elliptic curve using addition-subtraction chains", Theoretical Informatics and Applications Vol.24, No.6 (1990), 531-544.

[19] 岡本龍明, 太田和夫 **共編暗号・ゼロ知識証明・数論**, 共立出版, 1995.

[20] S. C. Pohlig and M. E. Hellman, "An improved algorithm for computing logarithm over $GF(p)$ and its cryptographic significance", *IEEE Trans. Inf. Theory*, IT-24(1978), pp.106-110.

[21] J. Pollard, "Monte Carlo methods for index computation(mod p)", *Mathematics of Computation*, 32 (1978), 918-924.

[22] H. G. Rück, "On the discrete logarithm in the divisor class group of curves", to appear in *Mathematics of computation*.

[23] T. Satoh and K. Araki "Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curve", to appear in Commentarii Math. Univ. St. Pauli.

[24] I. A. Semaev "On computing logarithms on elliptic curves", *Discrete Math. Appl.*, Vol. **67**(1996), 69-76.

[25] I. A. Semaev "Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curves in characteristic p", *Mathematics of computation*, **67**(1998), 353-356.

[26] J. H. Silverman, *The Arithmetic of Elliptic Curves*, GTM106, Springer-Verlag, New York, 1986.

[27] N. P. Smart "The discrete logarithm problem on elliptic curves of trace one", to appear in J. Cryptology.

[28] P. van Oorschot and M. Wiener, "Parallel collision search with cryptanalytic applications", *Proceedings of the 2nd ACM conference on Computer and Communications security*, ACM press(1994), 210-218.

[29] 山本 芳彦, **現代数学への入門 -数論入門** *2-*, 岩波書店, 1996.