修 士 学 位 論 文

題 名

Montgomery 曲線を用いた KMOV 暗号について

指導教員　内田 幸寛　准教授

2021 年 1 月 8 日 提出

東京都立大学大学院

理学研究科 数理科学専攻

学修番号 19843402

氏名 市川 幸司

学位論文要旨 (修士 (理学))

数理科学専攻 19843402
論文著者名 市川 幸司

論文題名：Montgomery 曲線を用いた KMOV 暗号について

1978 年に Rivest, Shamir, Adleman によって RSA 暗号が提案された．これは現在でも普及している公開鍵暗号方式である．RSA 暗号は $n = pq$ となる RSA モジュラスと $ed \equiv 1 \pmod{(p-1)(q-1)}$ となる, 公開鍵 e と秘密鍵 d を用いて構成されたものである．その安全性は素因数分解の困難性に根拠をおいている．一方 KMOV 暗号は 1992 年, 小山, Maurer, 岡本, Vanstone [1] によって楕円曲線を用いて開発された公開鍵暗号方式である．この方式は素数 p, q を用いた $n = pq$ となる剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上での楕円曲線を基にしている．その安全性は素因数分解の困難性に根拠を置いている．KMOV 暗号は様々な形で一般化されている．Demytko [2] は楕円曲線上の x 座標のみ使用する方式を提案した．そして Boudabra と Nitaj [3] は $n = p^r q^s$ となる素数べき乗 RSA モジュラスを用いた KMOV 暗号の提案をした．さらに楕円曲線暗号に通常用いられる Weierstrass 型の楕円曲線 $y^2 = x^3 + ax + b$ の代わりに, twisted Edwards 曲線 $ax^2 + y^2 = 1 + dx^2y^2$ を用いた方式も構築されている [4]．一方 Montgomery 曲線と呼ばれる別の標準型の楕円曲線 $By^2 = x^3 + Ax^2 + x$ が知られている．Montgomery 曲線は x 座標のみで加算やスカラー倍が行えるので, Weierstrass 型の楕円曲線に比べ高速に計算できることが知られている [5]．そのことから楕円曲線暗号については Montgomery 曲線の利用が提案されている．しかし Montgomery 曲線を利用した KMOV 暗号に関しては考察はされていなかった．

そこで本論文では, 素数べき乗 RSA モジュラス $n = p^r q^s$ となる剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上の Montgomery 曲線 $By^2 = x^3 + x$ を用いてスカラー倍された x 座標から同じ座標成分である y 座標を復元する方法 [6] を組み合わせた新しい KMOV 暗号の方式を提案した．さらにこの方式の安全性や Weierstrass 型の楕円曲線と twisted Edwards 曲線と Montgomery 曲線の KMOV 暗号を比較して効率性の評価を行った．

参考文献

[1] K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone, *New public-key schemes based on elliptic curves over the ring* $\mathbf{Z}_n$, Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991), Lecture Notes in Comput. Sci., vol. 576, Springer, Berlin, 1992, pp. 252–266.

[2] N. Demytko, *A new elliptic curve based analogue of RSA*, Advances in cryptology—EUROCRYPT '93 (Lofthus, 1993), Lecture Notes in Comput. Sci., vol. 765, Springer, Berlin, 1994, pp. 40–49.

[3] M. Boudabra and A. Nitaj, *A new generalization of the KMOV cryptosystem*, J. Appl. Math. Comput. **57** (2018), no. 1-2, 229–245.

[4] M. Boudabra and A. Nitaj, *A new public key cryptosystem based on Edwards curves*, J. Appl. Math. Comput. **61** (2019), no. 1-2, 431–450.

[5] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), no. 177, 243–264.

[6] K. Okeya and K. Sakurai, *Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve*, Cryptographic hardware and embedded systems—CHES 2001 (Paris), Lecture Notes in Comput. Sci., vol. 2162, Springer, Berlin, 2001, pp. 126–141.

Montgomery 曲線を用いた KMOV 暗号について

東京都立大学大学院 理学研究科 数理科学専攻
19843402 市川幸司

2021 年 1 月 8 日

目次

1 はじめに

1978 年に Rivest, Shamir, Adleman によって RSA 暗号が提案された．これは現在でも普及している公開鍵暗号方式である．RSA 暗号は $n = pq$ となる RSA モジュラスと $ed \equiv 1 \pmod{(p-1)(q-1)}$ となる, 公開鍵 e と秘密鍵 d を用いて構成されたものである．その安全性は素因数分解の困難性に根拠をおいている．一方 KMOV 暗号は 1992 年, 小山, Maurer, 岡本, Vanstone [1] によって楕円曲線を用いて開発された公開鍵暗号方式である．この方式は素数 p, q を用いた $n = pq$ となる剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上での楕円曲線を基にしている．その安全性は素因数分解の困難性に根拠を置いている．KMOV 暗号は様々な形で一般化されている．Demytko [2] は楕円曲線上の x 座標のみ使用する方式を提案した．そして Boudabra と Nitaj [3] は $n = p^r q^s$ となる素数べき乗 RSA モジュラスを用いた KMOV 暗号の提案をした．さらに楕円曲線暗号に通常用いられる Weierstrass 型の楕円曲線 $y^2 = x^3 + ax + b$ の代わりに, twisted Edwards 曲線 $ax^2 + y^2 = 1 + dx^2y^2$ を用いた方式も構築されている [4]．一方 Montgomery 曲線と呼ばれる別の標準型の楕円曲線 $By^2 = x^3 + Ax^2 + x$ が知られている．Montgomery 曲線は x 座標のみで加算やスカラー倍が行えるので, Weierstrass 型の楕円曲線に比べ高速に計算できることが知られている [5]．そのことから楕円曲線暗号については Montgomery 曲線の利用が提案されている．しかし Montgomery 曲線を利用した KMOV 暗号に関しては考察はされていなかった．

そこで本論文では, 素数べき乗 RSA モジュラス $n = p^r q^s$ となる剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上の Montgomery 曲線 $By^2 = x^3 + x$ を用いてスカラー倍された x 座標から同じ座標成分である y 座標を復元する方法 [6] を組み合わせた新しい KMOV 暗号の方式を提案した．さらにこの方式の安全性や Weierstrass 型の楕円曲線と twisted Edwards 曲線と Montgomery 曲線の KMOV 暗号を比較して効率性の評価を行った．

2 準備

本章では, 本論文に必要な予備知識についてまとめる．

2.1 記号の定義

本論文では, 以下の記号を用いることにする．

- $\mathbb{Z}$: 整数全体の集合
- p, q: 互いに異なる 2, 3 を除く素数
- $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$: 元の要素が p 個の有限体
- $\mathbb{Z}/n\mathbb{Z}$: 元の個数が n 個の剰余環

2.2 有限体上の楕円曲線

本節では, 有限体上の Weierstrass 型の楕円曲線の定義と性質について述べる．

定義 2.1 (有限体上の Weierstrass 型の楕円曲線) $a, b \in \mathbb{F}_p$, $4a^3 + 27b^2 \neq 0$ とする．$\mathbb{F}_p$ 上の楕円曲線 $E^W_{p,a,b}$ を

$$E^W_{p,a,b} = \{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

と定義する．ここで $\mathcal{O}$ は無限遠点と呼ばれる点である．

定理 2.1 (Weierstrass 型の楕円曲線の位数) 楕円曲線 $E^W_{p,a,b}$ の有理点の個数を $\#E^W_{p,a,b}$ と表記し，その位数は

$$\#E^W_{p,a,b} = p + 1 + \sum_{x=0}^{p-1} \left(\frac{x^3 + ax + b}{p} \right)$$

で与えられる．ここで $\left(\frac{\cdot}{p}\right)$ はルジャンドル記号であり，

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a \equiv 0 \pmod{p} \\ 1, & a \text{ が } p \text{ を法として平方剰余である場合} \\ -1, & a \text{ が } p \text{ を法として平方非剰余である場合} \end{cases}$$

と定義される．

定義 2.2 (Weierstrass 型の楕円曲線の演算) $P = (x_1, y_1)$, $Q = (x_2, y_2) \in E^W_{p,a,b}$ に対し，

- $P = \mathcal{O}$ のとき $P + Q = Q + P = Q$
- $-P = (x_1, -y_1)$
- $P + (-P) = \mathcal{O}$
- 上記以外では，$P + Q = (x_3, y_3)$ を

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

ただし，

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & (P \neq Q \text{ のとき}) \\ \frac{3x^2 + a}{2y_1} & (P = Q \text{ のとき}) \end{cases}$$

と定義する．

定義 2.2 より $E^W_{p,a,b}$ はアーベル群を成す ($\mathcal{O}$ が単位元, $-P$ が P の逆元).
そして整数 k に対して, k 回演算を施した点 P を

$$kP = P + P + \ldots + P$$

と定義する．また, 有限体上の任意の楕円曲線の有理点の個数をある範囲で定められる Hasse の定理について述べる．

定理 2.2 (Hasse の定理) 楕円曲線 $E^W_{p,a,b}$ の有理点の個数 $\#E^W_{p,a,b}$ は

$$|\#E^W_{p,a,b} - (p+1)| \leqq 2\sqrt{p}$$

を満たす．

以下の定理によって, ある特別な場合においての Weierstrass 型の楕円曲線は容易に位数を決定することができる．

定理 2.3

$$\#E^W_{p,a,b} = \begin{cases} p+1 & a=0, b\neq 0, p\equiv 2 \pmod 3 \\ p+1 & a\neq 0, b=0, p\equiv 3 \pmod 4 \end{cases}$$

が成り立つ.

証明は [1] を参照されたい. また以下の補題が成り立つ.

補題 2.1 整数 k, 楕円曲線 $E^W_{p,a,b}$ 上の点 P に対し,

$$\{1+k(p+1)\}P = \begin{cases} P & a=0, b\neq 0, p\equiv 2 \pmod 3 \\ P & a\neq 0, b=0, p\equiv 3 \pmod 4 \end{cases}$$

が成り立つ.

2.3 剰余環上の楕円曲線

本節では, 素数 p, q を用いて $n = pq$ となる剰余環上の Weierstrass 型の楕円曲線の性質について述べる.

定義 2.3 (剰余環上の Weierstrass 型の楕円曲線) 素数 p, q を用いて, $n = pq$ とする. そして, $a, b \in \mathbb{Z}/n\mathbb{Z}$, $\gcd(4a^3 + 27b^2, n) = 1$ とする. このとき $\mathbb{Z}/n\mathbb{Z}$ 上の楕円曲線 $E^W_{n,a,b}$ を

$$E^W_{n,a,b} = \{(x, y) \in (\mathbb{Z}/n\mathbb{Z})^2 \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

と定義する. ここで $\mathcal{O}$ は無限遠点と呼ばれる点である.

加法演算においても有限体と同様に定義することができる. しかし $P = (x_1, y_1), Q = (x_2, y_2) \in E^W_{n,a,b}$ に対して, 以下の条件の時に定義することは不可能である.

- $P \neq Q$ のときに, $\gcd(x_2 - x_1, n) \neq 1$
- $P = Q$ のときに, $\gcd(2y_1, n) \neq 1$

この場合は中国剰余定理を用いることによって回避することが可能である. 即ち, $\mathcal{O}_p \in E^W_{p,a,b}, \mathcal{O}_q \in E^W_{q,a,b}$ に対して, $\mathcal{O}$ を $(\mathcal{O}_p, \mathcal{O}_q)$ と表し, $P_p = (x_p, y_p) \in E^W_{p,a,b}, P_q = (x_q, y_q) \in E^W_{q,a,b}$ に対して $P = (x, y) \in E^W_{n,a,b} \setminus \{\mathcal{O}\}$ は $(P_p, P_q) = [(x_p, y_p), (x_q, y_q)]$ として表記できる. 写像 $E^W_{n,a,b} \to E^W_{p,a,b} \times E^W_{q,a,b}$ によって, $E^W_{p,a,b} \times E^W_{q,a,b}$ の全ての元は P_p と P_q のうち 1 つが無限遠点となるような点 $(\mathcal{O}, P_q), (P_p, \mathcal{O})$ を除いて $E^W_{n,a,b}$ の元で表される. 仮に $E^W_{n,a,b}$ 上の 2 点の加法が点 $(\mathcal{O}, P_q), (P_p, \mathcal{O})$ になったとき, $\gcd(x_2 - x_1, n)$ または $\gcd(2y_1, n)$ が p または q となる. このときに n の因数が明らかになる. この場合は巨大な素数 p, q を選ぶことで高確率で回避することが出来る. この表記を用いてさらに前節の定理 2.3 と中国剰余定理を適用すると以下の補題が成立する.

補題 2.2 整数 k, $N_n = \mathrm{lcm}(p+1, q+1)$, 楕円曲線 $E^W_{n,a,b}$ 上の点 P に対し,

$$(1+kN_n)P = \begin{cases} P & a=0, b\neq 0, p\equiv 2 \pmod 3 \\ P & a\neq 0, b=0, p\equiv 3 \pmod 4 \end{cases}$$

が成り立つ.

詳しくは [1] を参照されたい.

3 KMOV 暗号

KMOV 暗号は 1992 年に小山, Maurer, 岡本, Vanstone によって素数 p, q を用いて $n = pq$ となる剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上の楕円曲線 $y^2 \equiv x^3 + b \pmod{n}$ を用いて提案された公開鍵暗号方式である [1]. 本章では, [1] の Type 1 における [鍵生成], [暗号化], [復号] のそれぞれについて紹介する.

3.1 鍵生成

1. 素数 p, q を $p \equiv q \equiv 2 \pmod{3}$ となるように選ぶ.
2. $n = pq, N_n = \mathrm{lcm}(\#E^W_{p,0,b}, \#E^W_{q,0,b}) = \mathrm{lcm}(p+1, q+1)$ を計算する.
3. 整数 e を $\gcd(e, N_n) = 1$ となるように選ぶ.
4. 整数 d を $d \equiv e^{-1} \pmod{N_n}$ となるように選ぶ.

ここで n, e を公開鍵, d を秘密鍵とする.

3.2 暗号化

1. メッセージを $M = (x_M, y_M) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ として変換する.
2. $b \equiv y_M^2 - x_M^3 \pmod{n}$ を計算する. ここで楕円曲線は $y^2 \equiv x^3 + b \pmod{n}$ として定義される.
3. 楕円曲線上で $C = (x_C, y_C) = e(x_M, y_M)$ を計算する.

点 (x_C, y_C) が暗号文となる.

3.3 復号

1. $b \equiv y_C^2 - x_C^3 \pmod{n}$ を計算する. ここで楕円曲線は $y^2 \equiv x^3 + b \pmod{n}$ として定義される.
2. 楕円曲線上で $M = (x_M, y_M) = d(x_C, y_C)$ を計算する.

点 (x_M, y_M) が元のメッセージとなる.

3.4 正当性

この方式での正当性について紹介する.
秘密鍵 d を $d \equiv e^{-1} \pmod{N_n}$ として選ぶことにより, $ed - kN_n = 1$ となるようなある整数 k が存在する. また, $b \equiv y_M^2 - x_M^3 \equiv y_C^2 - x_C^3 \pmod{n}$ が成り立つ. さらに補題 2.2 より

$$d(x_C, y_C) = deM = (1 + kN_n)M = M$$

となるので, この方式は正しいことがわかる.

4 Twisted Edwards 曲線

2007 年に Edwards は楕円曲線の新しい標準型を提案した [7]. 2008 年に Bernstein らによって twisted Edwards 曲線という楕円曲線が提案された [8]. 本章では, twisted Edwards 曲線と呼ばれる楕円曲線について述べ, さらに定義や演算について述べる.

4.1 定義

本節では, twisted Edwards 曲線, Edwards 曲線の定義と twisted Edwards 曲線の点の加法公式を与える.

定義 4.1 (Twisted Edwards 曲線) $\mathbb{F}_p$ を標数が 2 ではない体, $a, d \in \mathbb{F}_p$, $ad(a-d) \neq 0$ とする. $\mathbb{F}_p$ 上の twisted Edwards 曲線を

$$E^E_{a,d} : ax^2 + y^2 = 1 + dx^2y^2$$

と定義する. また, $\#E^E_{a,d}$ の表記で有理点の個数も表すものとする.

定義 4.2 (Edwards 曲線) $a = 1$ のとき, $E^E_{1,d} : x^2 + y^2 = 1 + dx^2y^2$ を Edwards 曲線という.

定義 4.3 (加法公式) $E^E_{a,d}$ 上の 2 点 $P = (x_1, y_1), Q = (x_2, y_2)$ に対し,

$$P + Q = \left(\frac{x_1y_2 + y_1x_2}{1 + dx_1x_2y_1y_2}, \frac{y_1y_2 - ax_1x_2}{1 - dx_1x_2y_1y_2} \right) \tag{1}$$

と定義する. 単位元 $\mathcal{O}$ は $(0, 1)$, 点 P の逆元 $-P$ は $(-x_1, y_1)$.

定義 4.3 より, $E^E_{a,d}$ はアーベル群をなす. また (1) の式は $P = Q$ でも成り立つ. 特に,

$$2P = \left(\frac{2x_1y_1}{ax_1^2 + y_1^2}, \frac{y_1^2 - ax_1^2}{2 - ax_1^2 - y_1^2} \right)$$

となる.

5 Montgomery 曲線

1987 年に Montgomery は Montgomery 曲線と呼ばれる楕円曲線の別の標準形 $By^2 = x^3 + Ax^2 + x$ を提案した [5]. これは Weierstrass 型の楕円曲線と比べて高速にスカラー乗算が行えることが知られている. 本章では, Montgomery 曲線と呼ばれる楕円曲線について述べ, その定義や性質を与える.

5.1 定義

本節では, Montgomery 曲線の定義と点の加法公式を与える.

定義 5.1 (Montgomery 曲線) $A \in \mathbb{F}_p \setminus \{-2, 2\}$, $B \in \mathbb{F}_p \setminus \{0\}$ とする.

$$E^M_{p,A,B} = \{(x, y) \in \mathbb{F}_p^2 \mid By^2 = x^3 + Ax^2 + x\} \cup \{\mathcal{O}\}$$

を $\mathbb{F}_p$ 上の Montgomery 曲線という.

Weierstrass 型の楕円曲線と同じように加法を定められる. 特に射影座標の点で計算することで逆元計算を避けることが出来る.
点 $(x, y) \in E^M_{p,A,B}$ を $(X/Z, Y/Z)$ と変換し, 点 $P = (X : Y : Z)$ の n 倍点を $nP = (X_n : Y_n : Z_n)$ と表記したとき $(m + n)P = mP + nP$ は Y を用いずに以下のようになる.

定義 5.2 (加法公式 ($m \neq n$))

$$X_{m+n} = Z_{m-n}\{(X_m - Z_m)(X_n + Z_n) + (X_m + Z_m)(X_n - Z_n)\}^2$$
$$Z_{m+n} = X_{m-n}\{(X_m - Z_m)(X_n + Z_n) - (X_m + Z_m)(X_n - Z_n)\}^2$$

定義 5.3 (2 倍公式 ($m = n$))

$$4X_nZ_n = (X_n + Z_n)^2 - (X_n - Z_n)^2$$
$$X_{2n} = (X_n + Z_n)^2(X_n - Z_n)^2$$
$$Z_{2n} = (4X_nZ_n)\left\{(X_n - Z_n)^2 + ((A+2)/4)\,(4X_nZ_n)\right\}$$

加法公式は $\mathbb{F}_p$ 上で 4 回の乗算と 2 回の平方計算が必要であり, 2 倍公式は $\mathbb{F}_p$ 上で 3 回の乗算と 2 回の平方計算が必要. (差分点 $Z_{m-n} = 1$ と仮定出来れば加法公式は 3 回の乗算と 2 回の平方計算で出来る.)

5.2 Montgomery 曲線と Weierstrass 型の楕円曲線の関係

本節では, Weierstrass 型の楕円曲線と Montgomery 曲線との関係ついて述べる. 詳しくは [5] を参照されたい.

定理 5.1 (Weierstrass 型の楕円曲線と Montgomery 曲線との関係) Weierstrass 型の楕円曲線 $y^2 = x^3 + ax + b$ が Montgomery 曲線 $By^2 = x^3 + Ax^2 + x$ に変形可能であることと以下の 2 つの条件は同値である.

1. $x^3 + ax + b$ は $\mathbb{F}_p$ 上で少なくとも 1 つの解を持つ.
2. α が $\mathbb{F}_p$ 上の $x^3 + ax + b$ の解とすると $3\alpha^2 + a$ は $\mathbb{F}_p$ 上で平方剰余となる.

定理 5.1 の証明から以下の補題が導ける.

補題 5.1 $A \in \mathbb{F}_p \setminus \{-2, 2\}$, $B \in \mathbb{F}_p \setminus \{0\}$, Montgomery 曲線を $By^2 = x^3 + Ax^2 + x$ とおく. 以下のように定めると Montgomery 曲線は $\mathbb{F}_p$ の変換における Weierstrass 型の楕円曲線 $v^2 = u^3 + (1/B^2)(1 - A^2/3)u + A(2A^2 - 9)/(27B^3)$ への $\mathbb{F}_p$-同型

$$(x, y) \to (u, v) = \begin{cases} \mathcal{O} & ((x, y) = \mathcal{O} \text{ のとき}) \\ ((3x + A)/(3B), y/B) & ((x, y) \neq \mathcal{O} \text{ のとき}) \end{cases}$$

が成り立つ.

補題 5.2 $A \in \mathbb{F}_p \setminus \{-2, 2\}$, $B \in \mathbb{F}_p \setminus \{0\}$, Weierstrass 型の楕円曲線を $v^2 = u^3 + (1/B^2)(1 - A^2/3)u + A(2A^2 - 9)/(27B^3)$ とおく. 以下のように定めると Weierstrass 型の楕円曲線は $\mathbb{F}_p$ の変換における Montgomery 曲線 $By^2 = x^3 + Ax^2 + x$ への $\mathbb{F}_p$-同型

$$(u, v) \to (x, y) = \begin{cases} \mathcal{O} & ((u, v) = \mathcal{O} \text{ のとき}) \\ (Bu - A/3, Bv) & ((u, v) \neq \mathcal{O} \text{ のとき}) \end{cases}$$

が成り立つ.

今回考える KMOV 暗号において, Montgomery 曲線の位数を明らかにすることは重要である. そこで $p \equiv 3 \pmod 4$ のとき定理 2.3 と補題 5.2 を組み合わせると Weierstrass 型の楕円曲線から $\#E^M_{p,0,B} = p + 1$ となる Montgomery 曲線が生成できる.

補題 5.3 $p \equiv 3 \pmod 4, B \in \mathbb{F}_p \setminus \{0\}$ のとき Weierstrass 型の楕円曲線を $v^2 = u^3 + (1/B^2)u$ とおく. 以下のように定めると Weierstrass 型の楕円曲線は $\mathbb{F}_p$ の変換における Montgomery 曲線 $By^2 = x^3 + x$ への $\mathbb{F}_p$-同型

$$(u, v) \to (x, y) = \begin{cases} \mathcal{O} & ((u, v) = \mathcal{O} \text{ のとき}) \\ (Bu, Bv) & ((u, v) \neq \mathcal{O} \text{ のとき}) \end{cases}$$

が成り立つ. さらに $\#E^M_{p,0,B} = p + 1$ を満たす.

今後, Montgomery 曲線を $By^2 = x^3 + x$ として考えこの曲線を用いて KMOV 暗号を考察する.

6 $\mathbb{Z}/p^r\mathbb{Z}$ 上の Montgomery 曲線

本章では, 整数 r, 素数 p を用いた $\mathbb{Z}/p^r\mathbb{Z}$ 上の Montgomery 曲線について述べる. 前節と同様に射影平面上の Montgomery 曲線における加算は定義できるが, その射影点 $(x : y : z)$ は $\gcd(p, x, y, z) = 1$ となることに留意する. 最初に特異点と正則点について述べる.

定義 6.1 (特異点と正則点の定義) 整数 r を用いた素数のべき乗を p^r とおき, 多項式 $f(x_1, x_2, \cdots, x_k) \in \mathbb{Z}[x_1, x_2, \cdots, x_k]$ に対して, $f(x_1, x_2, \cdots, x_k) \equiv 0 \pmod{p^r}$ を満たす点 $(x_1, x_2, \cdots, x_k) \in (\mathbb{Z}/p^r\mathbb{Z})^k$ はすべての $i = 1, 2, \cdots, k$ において

$$\frac{\partial f}{\partial x_i}(x_1, x_2, \cdots, x_k) \equiv 0 \pmod p$$

を満たすとき特異点と呼ぶ. 一方, 特異点ではない点を正則点と呼ぶ.

定義 6.2 整数 r を用いた素数のべき乗を p^r とおき, $f(x_1, x_2, \cdots, x_k) \in \mathbb{Z}[x_1, x_2, \cdots, x_k]$ に対して $f(x_1, x_2, \cdots, x_k) \equiv 0 \pmod{p^r}$ を満たす点の個数 c_{p^r} を

$$c_{p^r} = \#\{(x_1, x_2, \cdots, x_k) \in (\mathbb{Z}/p^r\mathbb{Z})^k \mid f(x_1, x_2, \cdots, x_k) \equiv 0 \pmod{p^r}\}$$

また特異点の個数 s_{p^r} を

$$\begin{aligned} s_{p^r} = \#\{(x_1, x_2, \cdots, x_k) \in (\mathbb{Z}/p^r\mathbb{Z})^k \mid & f(x_1, x_2, \cdots, x_k) \equiv 0 \pmod{p^r}, \\ & \frac{\partial f}{\partial x_i}(x_1, x_2, \cdots, x_k) \equiv 0 \pmod p,\ i = 1, \cdots, k\} \end{aligned}$$

p^r 上の正則点の個数 R_{p^r} を

$$R_{p^r} = c_{p^r} - s_{p^r}$$

とそれぞれ表記する.

次に R_{p^r} と R_p の関係式を表す定理について述べる. 証明は [2] を参照されたい.

定理 6.1 R_{p^r} を $f(x_1, x_2, \cdots, x_k) \equiv 0 \pmod{p^r}$ の正則点の個数とおく. このとき

$$R_{p^r} = p^{(k-1)(r-1)} R_p$$

が成り立つ.

ここで $\gcd(p, B) = 1$ とする. 定理 6.1 を用いると多項式 $By^2 \equiv x^3 + x \pmod{p^r}$ の点の個数は $By^2 \equiv x^3 + x \pmod p$ の点の個数で求められる.

系 6.1 $\gcd(p, B) = 1$, 整数 r に対して

$$\begin{aligned}&\#\left\{(x, y) \in \left(\mathbb{Z}/p^r\mathbb{Z}\right)^2 \mid By^2 \equiv x^3 + x \pmod{p^r}\right\}\\&= p^{r-1}\#\left\{(x, y) \in \left(\mathbb{Z}/p\mathbb{Z}\right)^2 \mid By^2 \equiv x^3 + x \pmod{p}\right\}\end{aligned}$$

が成り立つ.

証明 方程式を $f(x, y) = x^3 + x - By^2$ とおき, $f(x, y)$ の導関数を考えると

$$\partial f(x, y) = \left(\frac{\partial f}{\partial x}(x, y), \frac{\partial f}{\partial y}(x, y)\right) = (3x^2 + 1, -2By)$$

ここで, $f(x, y)$ 上の特異点 (x, y) は 3 つの方程式

$$\left\{\begin{array}{lll} 3x^2 + 1 & \equiv & 0 \pmod{p} \\ -2By & \equiv & 0 \pmod{p} \\ x^3 + x - By^2 & \equiv & 0 \pmod{p} \end{array}\right. \tag{2}$$

を満たす点である. 仮定より $B \not\equiv 0 \pmod{p}$ であるから 2 番目の方程式は $y \equiv 0 \pmod{p}$ となる. これを 3 番目の方程式に代入すると $x^3 + x \equiv 0 \pmod{p}$ を得られこの式を満たす値は $x \equiv 0 \pmod{p}$ であるが, これらは 1 番目の方程式を満たさない. よって $f(x, y)$ は特異点を持たない. ここで定理 6.1 を用いると題意は示せる. □

方程式を $By^2z \equiv x^3 + xz^2 \pmod{p}$ と変形する. 素数を $p \equiv 3 \pmod{4}$ と仮定すると, 以下の結果を得られる.

系 6.2 $p \equiv 3 \pmod{4}$, $\gcd(p, B) = 1$ と仮定する. このとき

$$\#\left\{(x, y, z) \in \left(\mathbb{Z}/p\mathbb{Z}\right)^3 \mid By^2z \equiv x^3 + xz^2 \pmod{p}\right\} = p^2$$

が成り立つ.

証明 $z \not\equiv 0 \pmod{p}$ のとき, 方程式 $By^2z \equiv x^3 + xz^2 \pmod{p}$ は $By^2 \equiv x^3 + x \pmod{p}$ と変形できる. ここで補題 5.3 よりこの方程式の解の個数は無限遠点 $\mathcal{O}$ を除くので, p となる. $z \equiv 0 \pmod{p}$ のとき, $x = 0$, $y = 0, 1, \cdots, p-1$ が満たす解である. 従って方程式 $By^2z \equiv x^3 + xz^2 \pmod{p}$ の解の個数は $(p-1)p + p = p^2$ である. □

下記の射影点の性質を用いると今までの結果は $By^2z \equiv x^3 + xz^2 \pmod{p^r}$ に拡張することが可能である. ここで射影点とは

$$(x : y : z) = \left\{(\lambda x, \lambda y, \lambda z) \in \left(\mathbb{Z}/p^r\mathbb{Z}\right)^3 \mid \lambda \in \mathbb{Z}/p^r\mathbb{Z},\ \gcd(p, \lambda) = 1\right\}$$

を満たし, さらに $\gcd(p, x, y, z) = 1$ を満たす点のことである. さらに射影点全体の集合を $\mathbb{P}^2_{p^r}$ と表記する.

定理 6.2 整数 r, $p \equiv 3 \pmod{4}$, $\gcd(p, B) = 1$ と仮定する. このとき $By^2z \equiv x^3 + xz^2 \pmod{p^r}$ の点の個数は

$$\#\left\{(x, y, z) \in \mathbb{P}^2_{p^r} \mid By^2z \equiv x^3 + xz^2 \pmod{p^r}\right\} = p^{r-1}(p+1)$$

となる.

証明　方程式 $By^2z \equiv x^3 + xz^2 \pmod{p^r}$ の満たす点 $(0,0,0)$ のみが射影点として表記できないので, 特異点となる. 定理 6.1 と系 6.2 を組み合わせるとこの方程式の正則点 (x,y,z) の個数は

$$c_{p^r} - 1 = p^{2(r-1)}(c_p - 1) = p^{2(r-1)}(p^2 - 1)$$

となる. そして各一組の射影点 $(x:y:z)$ は $\phi(p^r) = p^{r-1}(p-1)$ 組の点 $(u,v,w) \in \mathbb{Z}/p^r\mathbb{Z}$ として表せる. 従って方程式 $By^2z \equiv x^3 + xz^2 \pmod{p^r}$ の射影点の個数は

$$\frac{p^{2(r-1)}(p^2-1)}{p^{r-1}(p-1)} = p^{r-1}(p+1)$$

となる. □

さらに定理 6.2 と Montgomery 曲線の射影点による群の性質を組み合わせると以下の結果を得られる.

補題 6.1 点 P は方程式 $By^2z \equiv x^3 + xz^2 \pmod{p^r}$ を満たす点とし, $p \equiv 3 \pmod 4$, $\gcd(p,B) = 1$, 整数 k に対して

$$\{1 + kp^{r-1}(p+1)\}P = P$$

が成り立つ.

7　$\mathbb{Z}/n\mathbb{Z}$ 上の Montgomery 曲線

本章では, 整数 r,s と素数 p,q を用いて $n = p^rq^s$ となる剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上の Montgomery 曲線について述べる. 前節と同様に射影平面上の Montgomery 曲線における加算は定義できるが, その射影点 $(x:y:z)$ は $\gcd(n,x,y,z) = 1$ となることに留意する. 定理 6.2 と中国剰余定理を組み合わせると方程式 $By^2z \equiv x^3 + xz^2 \pmod n$ 上の点の個数が求められる.

定理 7.1 整数 r,s, $\gcd(p,q) = 1$ となるような p^r, q^s を素数のべき乗とする. そして $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$, $n = p^rq^s$, $\gcd(n,B) = 1$ を満たすとする. このとき方程式 $By^2z \equiv x^3 + xz^2 \pmod n$ の点の個数は

$$\#\{(x,y,z) \in \mathbb{P}_n^2 \mid By^2z \equiv x^3 + xz^2 \pmod n\} = p^{r-1}q^{s-1}(p+1)(q+1)$$

となる

証明　仮定より $\gcd(p,q) = 1$ であるから, 中国剰余定理を用いると方程式 $By^2z \equiv x^3 + xz^2 \pmod n$ を満たす点はそれぞれの方程式 $By^2z \equiv x^3 + xz^2 \pmod{p^r}, By^2z \equiv x^3 + xz^2 \pmod{q^s}$ を満たす点と一対一対応している. 従って方程式 $By^2z \equiv x^3 + xz^2 \pmod n$ の点の個数は

$$\begin{aligned}
&\#\{(x,y,z) \in \mathbb{P}_n^2 \mid By^2z \equiv x^3 + xz^2 \pmod n\} \\
&= \#\{(x,y,z) \in \mathbb{P}_{p^r}^2 \mid By^2z \equiv x^3 + xz^2 \pmod{p^r}\} \\
&\quad \times \#\{(x,y,z) \in \mathbb{P}_{q^s}^2 \mid By^2z \equiv x^3 + xz^2 \pmod{q^s}\} \\
&= p^{r-1}q^{s-1}(p+1)(q+1)
\end{aligned}$$

となる. □

さらに定理 7.1 と Montgomery 曲線の射影点による群の性質を組み合わせると以下の結果を得られる.

補題 7.1 整数 r, s, $\gcd(p, q) = 1$ となるような p^r, q^s を素数のべき乗とする．そして $p \equiv 3 \pmod 4$, $q \equiv 3 \pmod 4$, $n = p^r q^s$, $\gcd(n, B) = 1$ を満たし，点 P は方程式 $By^2 z \equiv x^3 + xz^2 \pmod n$ を満たす点とする．このとき整数 k に対して

$$\{1 + kp^{r-1}q^{s-1}(p+1)(q+1)\}P = P$$

が成り立つ．

7.1 Montgomery 曲線における y 座標復元法

今回考える KMOV において鍵交換を施すときに y 座標が必要不可欠である．そのため本節では，Montgomery 曲線による y 座標復元法について述べる．詳しくは [6] を参照されたい．

定理 7.2 (Montgomery 曲線による y 座標復元法) Montgomery 曲線上の点を $P = (x, y)$, $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ とする．$P_2 = P_1 + P$, $\gcd(y, n) = 1$ と仮定すると

$$y_1 = \frac{(x_1 x + 1)(x_1 + x) - (x_1 - x)^2 x_2}{2By}$$

が成り立つ．

定理 7.2 では $2By$ の除算があるので，それを避けるために点 P_1, P_2 を射影平面上の点として考える．

系 7.1 点 P, P_1, P_2 は定理 7.1 と同様にする．$P_1 = (X_1/Z_1, Y_1/Z_1), P_2 = (X_2/Z_2, Y_2/Z_2)$ とおき $X_1^{sim}, Y_1^{sim}, Z_1^{sim}$ を以下のように定義する．

$$\begin{aligned} X_1^{sim} &= 2ByZ_1Z_2X_1 \\ Y_1^{sim} &= Z_2\{(X_1 + xZ_1)(X_1 x + Z_1)\} - (X_1 - xZ_1)^2 X_2 \\ Z_1^{sim} &= 2ByZ_1Z_2Z_1 \end{aligned}$$

このとき $(X_1^{sim}, Y_1^{sim}, Z_1^{sim})$ は $x = X_1^{sim}/Z_1^{sim} = X_1/Z_1$, $y = Y_1^{sim}/Z_1^{sim} = Y_1/Z_1$ と表記でき射影座標となる．

y 座標を復元する方法は 10 回の乗算と 1 回の平方計算が必要となる．系 7.2 を用いたアルゴリズムを *Recover* に示す．

Algorithm 1 *Recover*(y 座標復元法)

Input: $P = (x, y)$, $P_1 = (X_1, Z_1)$, $P_2 = (X_2, Z_2)$

Output: $(X_1^{sim} : Y_1^{sim} : Z_1^{sim})$

1: $T_1 \leftarrow x \times Z_1$
2: $T_2 \leftarrow X_1 + T_1$
3: $T_3 \leftarrow X_1 - T_1$
4: $T_3 \leftarrow T_3 \times T_3$
5: $T_3 \leftarrow T_3 \times X_2$
6: $T_4 \leftarrow x \times X_1$
7: $T_4 \leftarrow T_4 + Z_1$
8: $T_2 \leftarrow T_2 \times T_4$
9: $T_2 \leftarrow T_2 \times Z_2$
10: $Y_1^{sim} \leftarrow T_2 - T_3$
11: $T_5 \leftarrow 2B \times y$
12: $T_5 \leftarrow T_5 \times Z_1$
13: $T_5 \leftarrow T_5 \times Z_2$
14: $X_1^{sim} \leftarrow T_5 \times X_1$
15: $Z_1^{sim} \leftarrow T_5 \times Z_1$
16: **return** $(X_1^{sim} : Y_1^{sim} : Z_1^{sim})$

本研究において Montgomery 曲線上で効率的に加算が行えるアルゴリズム Montgomery ladder の結果に点 $P = (X : Y : Z)$ の m 倍点 $mP = (X_m : Z_m)$ と $(m+1)$ 倍点 $(m+1)P = (X_{m+1} : Z_{m+1})$ を出力させ本節で述べた y 座標復元法のアルゴリズムを組み合わせると完全な点 P の m 倍点 $mP = (X_m : Y_m : Z_m)$ を得られる. 詳しくは次章で述べる.

8 提案手法

本章では, 整数 r, s と素数 p, q を用いて $n = p^r q^s$ となる剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上の Montgomery 曲線 $E_{0,B}^M : By^2 = x^3 + x$ (B は $\gcd(pq, B) = 1$ となる整数) を用いて KMOV 暗号を考える. 最初に前章で述べた Montgomery ladder のアルゴリズムを *Ladder* に示す. 表記については [9] を参考にした.

Algorithm 2 *Ladder*(Montgomery 曲線上の演算アルゴリズム)

Input: $m = \sum_{i=0}^{l-1} k_i 2^i$, 但し, $k_{l-1} = 1, P = (X : Z)$

Output: $(X_m : Z_m), (X_{m+1} : Z_{m+1})$

1: $(V_0, V_1) \leftarrow (P, 2P)$
2: **for** $i = l - 2$ to 0 **do**
3: **if** $k_i = 0$ **then**
4: $(V_0, V_1) \leftarrow (2V_0, V_0 + V_1)$
5: **else**
6: $(V_0, V_1) \leftarrow (V_0 + V_1, 2V_1)$
7: **end if**
8: **end for**
9: **return** V_0, V_1

Recover と *Ladder* を組み合わせることにより完全な $mP = (X_m : Y_m : Z_m)$ を得られる.

Algorithm 3 nP の演算アルゴリズム

Input: 整数 m, 点 $P = (X : Z)$ は $E^M_{n,0,B}$ 上の点とする. 但し P は位数 2 の点ではない

Output: $mP = (X_m : Y_m : Z_m)$

1: $(V_0, V_1) \leftarrow Ladder(m, (X : Z))$
2: $mP \leftarrow Recover(P, V_0, V_1)$
3: **return** mP

以上の議論を用いて Montgomery 曲線を用いて KMOV 暗号を考察する.

8.1 鍵生成

1. 2 つの大きな素数 p, q を以下のように選択.
   - $p \equiv 3 \pmod 4$
   - $p + 1 = 4u \quad (u$: 素数)
   - $q \equiv 3 \pmod 4$
   - $q + 1 = 4v \quad (v$: 素数)
2. $n = p^r q^s$ を計算する.
3. 整数 e を $\gcd(e, p^{r-1}q^{s-1}(p+1)(q+1)) = 1$ となるように選ぶ.
4. 整数 d を $d \equiv e^{-1} \pmod{p^{r-1}q^{s-1}(p+1)(q+1)}$ となるように選ぶ.

ここで n, e を公開鍵, d を秘密鍵とする.

8.2 暗号化

1. $\gcd(x_M, n) = 1, \gcd(y_M, n) = 1$ となるようにメッセージを $M = (x_M, y_M) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ として変換する.
2. $$B \equiv \frac{x_M(x_M^2 + 1)}{y_M^2} \pmod n$$

を計算する. ここで楕円曲線は $By^2 \equiv x^3 + x \pmod{n}$ として定義される.

3. 楕円曲線上で Algorithm 3 を用いて $C = (x_C, y_C) = e(x_M, y_M)$ を計算する.

点 (x_C, y_C) が暗号文となる.

8.3 復号

1. $$B \equiv \frac{x_C(x_C^2 + 1)}{y_C^2} \pmod{n}$$

   を計算する.

2. 楕円曲線 $By^2 \equiv x^3 + x \pmod{n}$ 上で Algorithm 3 を用いて $M = (x_M, y_M) = d(x_C, y_C)$ を計算する.

点 (x_M, y_M) が元のメッセージとなる.

8.4 正当性

この方式での正当性について紹介する.

$ed \equiv 1 \pmod{p^{r-1}q^{s-1}(p+1)(q+1)}$ であるから, $ed = 1 + kp^{r-1}q^{s-1}(p+1)(q+1)$ となるようなある整数 k が存在する. 従って, 系 7.1 を用いると

$$\begin{aligned} d(x_C, y_C) &= de(x_M, y_M) \\ &= (x_M, y_M) \end{aligned}$$

となるので, この方式は正しいことがわかる.

9 安全性

本章では, 提案した方式の安全性について述べる.

9.1 RSA モジュラスによる因数分解の困難性

本節では, 提案した RSA モジュラス $n = p^r q^s$ の因数分解の困難性について考察する. 以下の表 1 に当てはまるような素数 p, q と指数 r, s を選ぶと, 因数分解の方法として知られる楕円曲線法や数体ふるい法によって因数が求まるのが困難になる [10]. ここで楕円曲線法は, スカラー乗算によって n の非自

表 1　最適な素因子の選び方

ビットによるモジュラスの大きさ	モジュラスの形
2048	pq, p^2q
3072	pq, p^2q
3584	pq, p^2q
4096	pq, p^2q, p^3q
8192	pq, p^2q, p^3q, p^3q^2

明な因数を求めている．これは, 楕円曲線の位数が小さい素数の積になった場合に成功するので, 今回用いる楕円曲線に対しては, $p+1=4u$ $(u:$素数$)$, $q+1=4v$ $(v:$素数$)$ とした場合に因数分解を失敗する確率が高くなる．

9.2 Montgomery 曲線の位数と因数分解の関係

本節では, Montgomery 曲線の位数と因数分解の関係について考察する．提案した方式は, 素数 p, q が $p \equiv q \equiv 3 \pmod 4$, $p+1=4u$ $(u:$素数$)$, $q+1=4v$ $(v:$素数$)$ を満たす RSA モジュラス $n=p^rq^s$ を用いている．定理 7.1 によって, Montgomery 曲線の位数は $p^{r-1}q^{s-1}(p+1)(q+1)$ となる．Montgomery 曲線の位数が求められれば, n が因数分解できる．実際,

$$g=\gcd(n,p^{r-1}q^{s-1}(p+1)(q+1))=p^{r-1}q^{s-1}$$

かつ

$$h=\frac{p^{r-1}q^{s-1}(p+1)(q+1)}{p^{r-1}q^{s-1}}=(p+1)(q+1)$$

を計算する．そして $h=(p+1)(q+1)$ と $n/g=pq$ を組み合わせることによって素数 p, q を求められる．一方で, n が因数分解できれば, Montgomery 曲線の位数が求められる．結果として, Montgomery 曲線の位数を求めることと n を因数分解することは計算量的に等価である．

10 計算量まとめ

本章では, 整数 r,s と素数 p,q を用いて $n=p^rq^s$ となる剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上の Weierstrass, twisted Edwards, Montgomery 曲線それぞれのスカラー乗算の計算量をまとめる．
楕円曲線上の点 $P=(x_1,y_1)$, $Q=(x_2,y_2)$ に対して射影座標系による加法公式は, それぞれの曲線を $(x_i,y_i)=(X_i/Z_i,Y_i/Z_i)$ $(i=1,2,3)$ と変換することにより, $P=(X_1:Y_1:Z_1)$, $Q=(X_2:Y_2:Z_2)$ を用いて $P+Q=(X_3:Y_3:Z_3)$ として表記する．また, 射影平面上の加法公式の表記については [8], [11] を参考にした．

10.1 Weierstrass 型の射影座標系での楕円曲線

Weierstrass 型の射影座標系の楕円曲線は

$$Y^2Z=X^3+aXZ^2+bZ^3 \quad (a,b\in\mathbb{Z}/n\mathbb{Z}, 4a^3+27b^2\neq 0)$$

であり, 射影座標系の加法公式は下記で与えられる．
射影座標系の加法公式
$P\neq Q$ のとき

$$\begin{cases} X_3=vA \\ Y_3=u(v^2X_1Z_2-A)-v^3Y_1Z_2 \\ Z_3=v^3Z_1Z_2 \end{cases} \tag{3}$$

ここで $u=Y_2Z_1-Y_1Z_2, v=X_2Z_1-X_1Z_2, A=u^2Z_1Z_2-v^3-2v^2X_1Z_2$ である。
$P=Q$ のとき

$$\begin{cases} X_3=2hs \\ Y_3=w(4B-h)-8Y_1^2s^2 \\ Z_3=8s^3 \end{cases} \tag{4}$$

ここで $w = aZ_1^2 + 3X_1^2, s = Y_1Z_1, B = X_1Y_1s, h = w^2 - 8B$ である。

10.2 Twisted Edwards 曲線の射影座標系の楕円曲線

Twisted Edwards 曲線の射影座標系の楕円曲線は

$$(aX^2 + Y^2)Z^2 = Z^4 + dX^2Y^2$$

であり, 射影座標系の加法公式は下記で与えられる.

射影座標系の加法公式

$P \neq Q$ のとき

$$\begin{cases} X_3 = AF\{(X_1 + Y_1)(X_2 + Y_2) - C - D\} \\ Y_3 = AG(D - aC) \\ Z_3 = FG \end{cases} \tag{5}$$

ここで $A = Z_1Z_2, B = A^2, C = X_1X_2, D = Y_1Y_2, E = dCD, F = B - E, G = B + E$ である.

$P = Q$ のとき

$$\begin{cases} X_3 = (B - C - D)J \\ Y_3 = F(E - D) \\ Z_3 = FJ \end{cases} \tag{6}$$

ここで $B = (X_1 + Y_1)^2, C = X_1^2, D = Y_1^2, E = aC, F = E + D, H = Z_1^2, J = F - 2H$ である.

10.3 各曲線上における計算量まとめ

以上より Weierstrass, twisted Edwards, Montgomery 曲線のそれぞれの曲線上のスカラー乗算における計算量をまとめる. $\mathbb{Z}/n\mathbb{Z}$ 上の 1 回の乗算, 平方算を $\mathbf{M}$, $\mathbf{S}$ で表記すると以下のような表となる. (比較する 3 つのタイプの曲線の位数と公開鍵 e と秘密鍵 d はそれぞれ同じビット長であると仮定する.)

表 2　各曲線上の計算量

曲線の種類 / 演算の種類	Weierstrass	twisted Edwards	Montgomery
射影座標系の加算	$12\mathbf{M} + 2\mathbf{S}$	$12\mathbf{M} + \mathbf{S}$	$4\mathbf{M} + 2\mathbf{S}$
射影座標系の 2 倍算	$7\mathbf{M} + 5\mathbf{S}$	$4\mathbf{M} + 4\mathbf{S}$	$3\mathbf{M} + 2\mathbf{S}$

ここでスカラー値のビット長を l として表記する. Algorithm 2 を用いた Montgomery 曲線の計算量は

$$(l-1)(3\mathbf{M} + 2\mathbf{S}) + l(3\mathbf{M} + 2\mathbf{S}) = (6l - 3)\mathbf{M} + (4l - 2)\mathbf{S}$$

となる. (加法公式において差分点 $Z_{m-n} = 1$ を仮定している.) さらに, Algorithm 3 の計算量は $10\mathbf{M} + \mathbf{S}$ である. 従って, Montgomery 曲線上で点 $nP = (X_{nP} : Y_{nP} : Z_{nP})$ を得るための計算量は,

$$(6l + 7)\mathbf{M} + (4l - 1)\mathbf{S}$$

である. さらに Weierstrass と twisted Edwards 曲線のスカラー乗算の計算量を [11] のバイナリ法 1 を用いて評価する. ここで 2 進表記における 1 の数を h とする. $Z_1 = 1$ であることを考慮すると, Weierstrass 型の楕円曲線の計算量は

$$(h-1)(8\mathbf{M} + 2\mathbf{S}) + (l-2)(6\mathbf{M} + 4\mathbf{S}) + (5\mathbf{M} + 4\mathbf{S}) = (8h + 6l - 15)\mathbf{M} + (2h + 4l - 6)\mathbf{S}$$

となる. ([2] の方式では $a = 0$ として計算しているのでその分も考慮した.) そして twisted Edwards 曲線の計算量は

$$(h-1)(11\mathbf{M}+\mathbf{S})+(l-2)(4\mathbf{M}+4\mathbf{S})+(4\mathbf{M}+3\mathbf{S}) = (11h+4l-15)\mathbf{M}+(h+4l-6)\mathbf{S}$$

として評価できる. l が十分大きな値として考え, h を $l/2$ としておくと, Weierstrass, twisted Edwards, Montgomery 曲線のスカラー乗算の計算量は $10l\mathbf{M}+5l\mathbf{S}$, $(19l/2)\mathbf{M}+(9l/2)\mathbf{S}$, $6l\mathbf{M}+4l\mathbf{S}$ としてそれぞれ表記できる. 従って, Montgomery 曲線が最も少ない計算量で演算が成されることがわかる.

11 まとめ

本研究では, 素数べき乗 RSA モジュラス $n = p^r q^s$ となる剰余環 $\mathbb{Z}/n\mathbb{Z}$ 上の Montgomery 曲線を用いてさらに y 座標を復元してそこから KMOV を導入することを考えた. 結果としては, KMOV 暗号として機能することが確かめられ, Weierstrass 型の楕円曲線と twisted Edwards 曲線と比べて Montgomery 曲線を用いた方が効率的に計算できることが分かった. 今回は理論としての KMOV 暗号を考えたが, RSA 暗号や KMOV 暗号に対して知られている攻撃法に対しての安全性評価を行い, そこから安全な n のサイズを決定し, そのサイズでの実装が今後の発展課題として考えられる.

12 謝辞

本研究は, 著者が東京都立大学大学院理学研究科数理科学専攻博士前期課程在学中に, 同大学院理学研究科数理科学専攻の内田幸寛准教授の指導の下行ったものである. 本年の先行きが不透明の中, 慣れない環境においても常に親身に, 熱心に指導してくださった内田幸寛准教授に深くお礼申し上げます. そしてご多忙の中, 本論文の副査を快諾していただいた内山成憲教授と横山俊一准教授に深く感謝いたします. また, 今まで支えてくださった家族にも感謝いたします. 最後に学生時代の 6 年間, 関わってくださった全ての方にお礼申し上げます.

参考文献

[1] K. Koyama, U. M. Maurer, T. Okamoto, and S. A. Vanstone, *New public-key schemes based on elliptic curves over the ring* $\mathbf{Z}_n$, Advances in cryptology—CRYPTO '91 (Santa Barbara, CA, 1991), Lecture Notes in Comput. Sci., vol. 576, Springer, Berlin, 1992, pp. 252–266.

[2] M. Boudabra and A. Nitaj, *A new generalization of the KMOV cryptosystem*, J. Appl. Math. Comput. **57** (2018), no. 1-2, 229–245.

[3] M. Boudabra and A. Nitaj, *A new public key cryptosystem based on Edwards curves*, J. Appl. Math. Comput. **61** (2019), no. 1-2, 431–450.

[4] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), no. 177, 243–264.

[5] K. Okeya, H. Kurumatani, and K. Sakurai, *Elliptic curves with the Montgomery-form and their cryptographic applications*, Public key cryptography (Melbourne, 2000), Lecture Notes in Comput. Sci., vol. 1751, Springer, Berlin, 2000, pp. 238–257.

[6] K. Okeya and K. Sakurai, *Efficient elliptic curve cryptosystems from a scalar multiplication algorithm with recovery of the y-coordinate on a Montgomery-form elliptic curve*, Cryptographic hardware and embedded systems—CHES 2001 (Paris), Lecture Notes in Comput. Sci., vol. 2162, Springer, Berlin, 2001, pp. 126–141.

[7] H. M. Edwards, *A normal form for elliptic curves*, Bull. Amer. Math. Soc. (N. S.) **44** (2007), no. 3, 393–422.

[8] D. J. Bernstein, P. Birkner, M. Joye, T. Lange, and C. Peters, *Twisted Edwards curves*, Progress in cryptology—AFRICACRYPT 2008, Lecture Notes in Comput. Sci., vol. 5023, Springer, Berlin, 2008, pp. 389–405.

[9] C. Costello and B. Smith, *Montgomery curves and their arithmetic*: *The case of large characteristic fields*, Cryptographic Engineering **8** (2017), 227–240.

[10] Compaq Computer Corporation, *Cryptography Using Compaq MultiPrime Technology in a Parallel Processing Environment* (2000).
[11] 宮地充子, 代数学から学ぶ暗号理論 : 整数論の基礎から楕円曲線暗号の実装まで, 日本評論社 (2012).