Computer Security Symposium 2012
30 October – 1 November 2012

Weierstrass 標準形の楕円曲線の加算公式について

白勢　政明 †

† 公立はこだて未来大学
041-8655 北海道函館市亀田中野町 116-2
shirase@fun.ac.jp

あらまし 本稿は，短 Weierstrass 標準形で与えられる楕円曲線上の点の新しい加算公式を提案する．詳細は以下のようになる．初めに，$P = (0, x_1), Q = (x_2, y_2)$ となるように座標変換を行い，楕円曲線の式を $y^2 = x^3 + ax^2 + bx + c$ に変換する．すると，$P + Q$ の x 座標は $(b - 2\lambda y_1)/x_2$ (λ は P を Q を通る直線の傾き) によって計算できる．この事実は，楕円曲線の点の加算 $P + Q$ の幾何学的定義から導出できる．提案公式を用いると，アフィン座標 + 射影座標 = 射影座標の mixed coordinate 系での加算公式の計算コストは約 20%削減される．但し，提案手法は 2 倍算の計算コストを増大させてしまうため，更なる研究が必要である．

An Addition formula on Ellipric Curves Given by Weierstrass Normal Form

Masaaki Shirase†

†Future University Hakodate
116-2 Kamedanakano-cho, Hakodate, Hokkaido 041-8655, JAPAN
shirase@fun.ac.jp

Abstract This paper proposes a new formula for adding points on an elliptic curve given by short Weierstrass form. In detail, we first make a coordinate conversion so that $P = (0, x_1), Q = (x_2, y_2)$, and change equation of the elliptic curve to $y^2 = x^3 + ax^2 + bx + c$. Then, the x coordinate of $P+Q$ is given by $(b-2\lambda y_1)/x_2$, where λ is slope of the line through P and Q. The fact can be derived due to the geometric definition of point addition. Applying the proposed formula reduces the cost of adding point of about 20% on the system of mixed coordinate of affine + projective = projective. However, it increases the cost of doubling point and then we need a further improvement in the future.

1　はじめに

1.1　楕円曲線

E を体 $\mathbb{F}$ 上楕円曲線 (つまり，E を定義する多項式 $f(x, y)$ の係数がすべて $\mathbb{F}$ の元) とする．このとき E の $\mathbb{F}$ 有理点の集合 $E(\mathbb{F})$ は

$$E(\mathbb{F}) = \{(x, y) \in \mathbb{F} \times \mathbb{F} : f(x, y) = 0\} \cup \{\mathcal{O}\}$$

と定義される．ここで $\mathcal{O}$ は無限遠点である．

楕円曲線の重要な性質に，$P, Q \in E(\mathbb{F})$ に対して第 3 の点 $P + Q \in E(\mathbb{F})$ が (幾何学的に) 定義でき，$\mathcal{O}$ を零元とする群をなすことである．

この加算の繰り返しにより，楕円曲線上の点 P と整数 n に対してスカラー倍

$$nP = \underbrace{P + P + \cdots + P}_{n\text{個の和}}$$

が定義される．

楕円曲線が Weierstrass 標準形

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

で与えられる[1]場合は，点 $P = (x_1, y_1)$，$Q = (x_2, y_2), P + Q = (x_3, y_3)$ に対して，x_3, y_3 を x_1, y_1, x_2, y_2, a, b から得る公式がよく知られている [12]．この公式は $x_1 \neq x_2$ の場合は加算公式，$P = Q$ の場合は 2 倍算公式と呼ばれる．この公式は $P+Q$ の**幾何的定義を数式化**したものである．

$\mathbb{F}$ が有限体 $\mathbb{F}_p$ の時，$E(\mathbb{F}_p)$ は有限群をなし，その位数を $\#E(\mathbb{F}_p)$ と表記する．

楕円曲線暗号は，楕円曲線の離散対数問題の困難性を利用している．楕円曲線暗号では，暗号化や復号の処理は，$\mathbb{F}_p$ 上楕円曲線のスカラー倍の計算コストが支配的となっている．従って，楕円曲線暗号の処理の高速化には，スカラー倍算の高速化が重要である．

多くの場合で楕円曲線は Wierstrass 標準形 (1) で与えられるが，スカラー倍算の高速化のために，Mongomery 型曲線 [10]

$$By^2 = x^3 + Ax^2 + x$$

や，Edwards 曲線 [6]

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

等の特殊な形式の楕円曲線の使用が提案されている．

1.2 ペアリング

l を素数，G_1, G_2 を位数 l の加群，G_3 を位数 l の乗法群とする．写像

$$e : G_1 \times G_2 \to G_3$$

が双線形性，

$$e(P_1 + P_2, Q) = e(P_1, Q)e(P_2, Q)$$
$$e(P, Q_1 + Q_2) = e(P, Q_1)e(P, Q_2)$$

を常に満たすとき，e をペアリングという．$G_1 = G_2$ のとき e を対称ペアリング，そうでないとき e を非対称ペアリングという．

ペアリングを利用した暗号プロトコル (ペアリング暗号) の研究が近年盛んになっており，そのような暗号プロトコルに ID ベース暗号 [11, 2]，タイムリリース暗号 [3]，属性ベース暗号 [8] 等がある．

暗号プロトコルの実装では，$\mathbb{F}_p$ 上楕円曲線 E に対して $(G_1, G_2, G_3) = (E(\mathbb{F}_p), E(\mathbb{F}_p), \mathbb{F}_{p^k})$，または $(G_1, G_2, G_3) = (E(\mathbb{F}_p), E'(\mathbb{F}_{p^d}), \mathbb{F}_{p^k})(E'$ は，$\#E'(\mathbb{F}_{p^d})$ の素因数 l を持つような E のツイスト) とするペアリングがよく用いられる．ここで，$E(\mathbb{F}_p)$ の位数 $\#E(\mathbb{F}_p)$ の最大素因数 l に対して k は $l|(p^k - 1)$ 満たす最小正整数であり，E の l に関する埋め込み次数と呼ばれる．d は k の正の約数のどれかである．

ペアリング暗号の実装に適した $\mathbb{F}_p$ 上の楕円曲線 E は pairing-friendly 曲線と呼ばれる．E が pairing-friendly であるための条件は

1. $\#E(\mathbb{F}_p)$ の最大素因数 l が十分に大きい，
2. 埋め込み次数 k が適切な値[2]，
3. $\log p / \log r$ が 1 に近い，

を満たすことである．従って，ペアリング暗号を実装するには，これらの条件を満たす楕円曲線を構成する必要がある．そして，ペアリングの値 $e(P, Q)$ を計算は，Miller のアルゴリズム (あるいはその改良版) によってなされる [9]．

文献 [7] は pairing-friendly 曲線の構成法を総括的に扱っているが，そこで与えられる pairing-friendly 曲線は，すべて Weierstrass 標準形で与えられている．また，ペアリング暗号は一般にペアリング $e(P, Q)$ の計算だけでなくスカラー倍の計算も必要である．従って，ペアリング暗号処理の高速化には，Weierstrass 標準形で与えられる楕円曲線のスカラー倍算の高速化が重要である．

本稿は，楕円曲線 $E_0 : y^2 = x^3 + a_0x^2 + b_0x + c_0$ で与えられる $\mathbb{F}_p$ 上楕円曲線に対して，$P = (0, y_1), Q = (x_2, y_2) \in E_0(\mathbb{F}_p)$ に対する

[1] この形式は短 Weierstrass 標準形と呼ぶ方がより正確かも知れないが，本稿では Weierstrass 標準形を呼ぶ．

[2] 128 ビットセキュリティに最適な k の値は 12 である．ランダムに p と E の係数を選ぶとほとんどの場合で $k \approx p$ となる．

$P+Q=(x_3,y_3)$ を計算する新しい**加算公式を幾何的定義から導く**．(楕円曲線 E の x^2 の係数が 0 でないことと，点 P の x 座標が 0 であることに注意．) それから，この公式を使用して，mixed coordinate 系 (アフィン座標の点 + 射影座標の点 → 射影座標の点) における加算公式を与える[3]．なお，このような楕円曲線と点を考えることは**特殊な場合でない**ことを強調したい．一般的な場合のように，Weierstrass 標準形 (1) で与えられる $\mathbb{F}_p$ 上楕円曲線 E に対して，$P=(x_1,y_1)\in E(\mathbb{F}_p)$ とする．すると，座標変換 $x\to x+x_1$ を施せば，楕円曲線 E の式は $E_0: y^2=x^3+a_0x^2+b_0x+c_0$ の形式に，P の座標は $(0,y_1)$ に変換される．これは本稿が扱う場合と一致する．

2 準備

2.1 楕円曲線の加算公式

E を Weierstrass 標準形 (1) で与えられる楕円曲線とすると，E の点には幾何学的に加算 + を定義でき，その加法 + において，$\mathcal{O}$ を零元とする群をなす．この幾何学的操作は，

1. P と Q を通る直線 L を引く，($P=Q$ の場合は，P での E の接線を L とする，)
2. E と L の第 3 の交点を $P*Q$ とする，
3. $P*Q$ の x 軸に対称な点を $P+Q$ とする，

である (図 1).

楕円曲線の点 $P=(x_1,y_1), Q=(x_2,y_2)$ の座標から $P+Q=(x_3,y_3)$ の座標を求める公式を加算公式 ($x_1\neq x_2$ の場合)，または 2 倍算公式 ($P=Q$ の場合) という．加算公式/2 倍算公式が点加算の幾何学的定義から導く過程は文献 [12] 等に記述されているが，本稿ではそれは重要なので以下に説明する．

E を Weierstrass 標準形 (1) で与えられる楕円曲線とする．$P=(x_1,y_1), Q=(x_2,y_2)\in E$ に対して，$P+Q=(x_3,y_3), P*Q=(x_3,y_3')$ とする．($P+Q$ と $P*Q$ は x 軸に対して対称

[3]他の座標系での新しい加算公式の導出は今後の課題としたい.

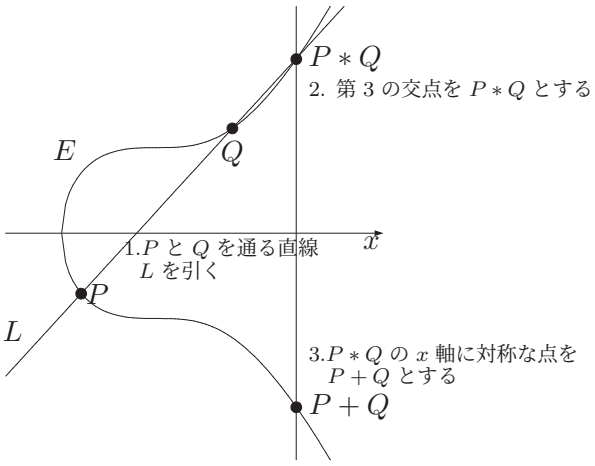


図 1: 点の加算 $P+Q$ の幾何学的定義

なのでこれらの x 座標は同じであり，$y_3'=-y_3$ である．) P と Q を通る直線を

$$L: y=\lambda x+\nu$$

とする．ここで，L の傾き λ は $x_1\neq x_2$ の場合は

$$\lambda=\frac{y_2-y_1}{x_2-x_1}, \tag{2}$$

$P=Q$ の場合は

$$\lambda=\left.\frac{\frac{d}{dx}(x^3+ax+b)}{\frac{d}{dy}\,y^2}\right|_{\substack{x=x_1\\ y=y_1}}=\frac{3x_1^2+a}{2y_1} \tag{3}$$

となる．なお，(2) の λ によって得られる公式が加算公式，(3) の λ によって得られる公式が 2 倍算公式となる．L の式を E の式 (1) に代入して y を消去すると，$\lambda^2x^2+2\lambda\nu x+\nu^2=x^3+ax+b$ となり，これを整理すると，

$$x^3-\lambda^2x^2+(a-2\lambda\nu)x+b-\nu^2=0 \tag{4}$$

が得られる．すると，

3 次方程式 (4) の根は x_1,x_2,x_3

であり，**2 次の項に関する解と係数の関係**から $x_1+x_2+x_3=\lambda^2$，つまり

$$x_3=\lambda^2-x_1-x_2 \tag{5}$$

が得られる．また，$P*Q=(x_3,y_3')$ は L 上の点なので，$y_3'-y_1=\lambda(x_3-x_1)$ が成り立ち，これを計算すると $y_3'=\lambda(x_3-x_1)+y_1$ となる．最後に $y_3'=-y_3$ であることから，

$$y_3=\lambda(x_1-x_3)-y_1 \tag{6}$$

アルゴリズム 1 (バイナリ法)

入力: $P \in E(\mathbb{F}_p), n = (n_{t-1}...n_0)_2$
出力: nP

1. $Q \leftarrow \mathcal{O}$ and $i \leftarrow t-1$
2. **while** $i \geq 0$
3. $\quad Q \leftarrow 2Q$
4. $\quad$ **if** $n_i = 1$ **then** $Q \leftarrow P + Q$
5. $\quad i \leftarrow i - 1$
6. **return** Q

アルゴリズム 2 (耐 SPA 攻撃)

入力: $P \in E(\mathbb{F}_p), n = (n_{t-1}...n_0)_2$
出力: nP

1. $Q[0] \leftarrow P$
2. **for** $i = t-2$ **down to** 0 **do**
3. $\quad Q[0] \leftarrow 2Q[0]$
4. $\quad Q[1] \leftarrow Q[0] + P$
5. $\quad Q[0] \leftarrow Q[n_i]$
6. **return** $Q[0]$

が得られる．このようにして，幾何学的定義から，よく知られている公式 (5)，(6) が導き出される．

2.2 スカラー倍算

楕円曲線暗号やペアリング暗号では，$\mathbb{F}_p$ 上楕円曲線 E に対して $P \in E(\mathbb{F}_p)$ と整数 n からスカラー倍 nP を計算する必要がある．この節は，基本的なスカラー倍算のためのアルゴリズムを紹介し，その計算コストの評価を点の加算と 2 倍算の回数により与える．今後，次の記号を使用する．

$\mathcal{ADD}$: 加算公式の計算コスト
$\mathcal{DBL}$: 2 倍算公式の計算コスト
$\mathcal{M}$: $\mathbb{F}_p$での乗算の計算コスト
$\mathcal{S}$: $\mathbb{F}_p$での 2 乗算の計算コスト
$\mathcal{I}$: $\mathbb{F}_p$での除算の計算コスト

なお，[5] や [4] と同様に，本稿は $\mathbb{F}_p$ での加算の計算コストは無視する．また，整数 n は t ビットとし，その 2 進展開を $(n_{t-1}...n_0)_2$ とする．$HW(\cdot)$ はハミング重みを表す．

2.2.1 スカラー倍算アルゴリズム

加算公式と 2 倍算公式を使って，スカラー倍を計算するための基本的なアルゴリズムにバイナリ法 (アルゴリズム 1) がある．アルゴリズム 1 の計算コストは

$$HW(n) \cdot \mathcal{ADD} + (t-1) \cdot \mathcal{DBL} \qquad (7)$$

となる．アルゴリズム 1 は，ステップ 4 で n_i が 0 か 1 で処理が異なるため，消費電力やタイミングなどの観測により n の値を見つけようとする SPA 攻撃に対して脆弱性を持つ．

SPA 攻撃への対策として，以下のようなアルゴリズム 2 が提案されている．このアルゴリズムでは n_i の値に関係なく各ループでの処理が一定となる．アルゴリズム 2 の計算コストは

$$(t-1) \cdot \mathcal{ADD} + (t-1) \cdot \mathcal{DBL} \qquad (8)$$

である．

2.2.2 座標系

座標系の選び方によって，スカラー倍算の計算コストは変動する．[5] や [4] では，各座標系の $\mathcal{ADD}$ や $\mathcal{DBL}$ の計算コストが $\mathcal{M}, \mathcal{S}, \mathcal{I}$ を使って評価されている．3 節の $\mathcal{ADD}$ や $\mathcal{DBL}$ の計算コストに関する表 1 では，提案公式以外の値はこれらの文献を参考にしている．また，各座標系でのアルゴリズム 1 と 2 の計算コストは表 2, 3 を参照．なお，出力が射影座標や Jacobian 座標となる場合は，出力をアフィン座標に変換するためのコストを考慮している．miixed coordinate 系については以下のような略記を使用する．

$MC(A + P = P)$:
アフィン座標 + 射影座標 = 射影座標の mixed coordinate

$MC(A + J = J)$:
アフィン座標 +Jacobian 座標 =Jacobian 座標の mixed coordinate

3 本稿の成果

楕円曲線の点の加算 $P + Q$ の幾何学的定義から，$P + Q$ の座標を求める新しい公式を導出する．

3.1 提案加算公式の導出過程

E を Weierstrass 標準形 (1) で与えられる楕円曲線とする．任意の点 $P = (x_1, y_1) \in E$ のスカラー倍を考える．アルゴリズム 1 や 2 では点加算の一方の点 P は定点なので，P の x 座標を 0 になるように座標変換して良い．座標変換 $x \to x + x_1$ を施すと，E の式は

$$E_0 : y^2 = x^3 + a_0^2 + b_0 x + c_0 \qquad (9)$$

の形になり，P の座標は $(0, y_1)$ となる．ここで，

$$\begin{aligned} a_0 &= 3x_1, \\ b_0 &= 3x_1^2 + a, \\ c_0 &= y_1^2, \end{aligned}$$

である．

図 2 から分かるように，このような座標変換を行っても，**楕円曲線加算の幾何学的定義には影響しない**．そこで，式 (9) で与えられる楕円曲線 E_0 に対する $P = (0, y_1), Q = (x_2, y_2) \in E(\mathbb{F}_p)$ から $P + Q = (x_3, y_3)$ を計算する加算公式を考える．P と Q を通る直線 L は $(0, y_1)$ を通るため $y = \lambda x + y_1$ と書け，直線 L の傾き λ は

$$\lambda = \frac{y_2 - y_1}{x_2}$$

となる．L の式を E_0 の式 (9) に代入して y を消去すると

$$\lambda^2 x^2 + 2\lambda y_1 x + y_1^2 = x^3 + a_0 x^2 + b_0 x + c_0$$

となり，これを整理すると，

$$x^3 + (a_0 - \lambda^2)x^2 + (b_0 - 2\lambda\nu)x + c_0 - y_1^2 = 0 \quad (10)$$

が得られる．従って，

3 次方程式 (10) の根は $0, x_2, x_3$

となる．ここで従来とは異なり，3 次方程式 (10) の **1 次の項に関する解と係数の関係**を考える．すると，$0 \cdot x_2 + 0 \cdot x_3 + x_2 x_3 = b_0 - 2\lambda y_1$，つまり

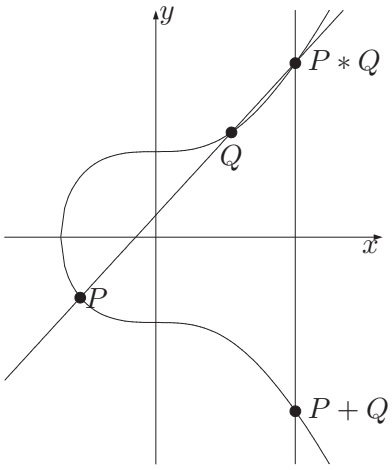
$$x_3 = \frac{b_0 - 2\lambda y_1}{x_2} \qquad (11)$$

が得られる．

ちなみに，従来のように 3 次方程式 (10) の **2 次の項に関する解と係数の関係**を考えると，$0 + x_2 + x_3 = \lambda$，つまり

$$x_3 = a_0 - \lambda^2 - x_2 \qquad (12)$$

が得られる．この x_3 の公式は従来の公式とほぼ同じである．



⇓ P の x 座標が 0 となるように座標変換

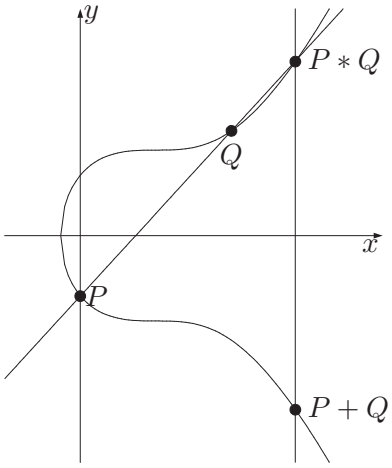


図 2: 座標変換を行っても，点の加算の幾何学的定義に影響しない

式 (11) と式 (12) を見比べると，射影座標系などを用いる場合，式 (12) より式 (11) が計算コストが低くなりそうである．y_3 は

$$y_3 = -\lambda x_3 - y_1 \qquad (13)$$

により得られる．

なお，3 次方程式 (10) の定数項の解と係数の関係からも別の加算公式が得られる．付録 A を参照．

表 1: 加算公式 ($\mathcal{ADD}$) と 2 倍算公式 ($\mathcal{DBL}$) の計算コスト

		$\mathcal{ADD}$ のコスト	$S=0.8\mathcal{M}$ の場合	$S=\mathcal{M}$ の場合	$\mathcal{DBL}$ のコスト	$S=0.8\mathcal{M}$ の場合	$S=\mathcal{M}$ の場合
従来公式	アフィン座標系	$2\mathcal{M}+\mathcal{S}+\mathcal{I}$	$2.8\mathcal{M}+\mathcal{I}$	$3\mathcal{M}+\mathcal{I}$	$2\mathcal{M}+2\mathcal{S}+\mathcal{I}$	$3.6\mathcal{M}+\mathcal{I}$	$4\mathcal{M}+\mathcal{I}$
	射影座標系	$12\mathcal{M}+2\mathcal{S}$	$13.6\mathcal{M}$ (1.55)	$14\mathcal{M}$ (1.56)	$7\mathcal{M}+5\mathcal{S}$	$11\mathcal{M}$ (0.89)	$12\mathcal{M}$ (0.92)
	Jacobian 座標系	$12\mathcal{M}+4\mathcal{S}$	$15.2\mathcal{M}$ (1.73)	$16\mathcal{M}$ (1.78)	$4\mathcal{M}+6\mathcal{S}$	$8.8\mathcal{M}$ (0.71)	$10\mathcal{M}$ (0.77)
	$MC(A+P\to P)$	$9\mathcal{M}+2\mathcal{S}$	$10.6\mathcal{M}$ (1.20)	$11\mathcal{M}$ (1.22)	–	–	–
	$MC(A+J\to J)$	$8\mathcal{M}+3\mathcal{S}$	$10.4\mathcal{M}$ (1.18)	$11\mathcal{M}$ (1.22)	–	–	–
提案公式 $(A+P\to P)$		$8\mathcal{M}+\mathcal{S}$	$8.8\mathcal{M}$	$9\mathcal{M}$	–	–	–

( ) の値は提案公式との比を表している.

注意 1

Weierstrass 標準形 (1) で与えられる楕円曲線 E に関する 3 次方程式 (4) に対して，1 次の項に関する解と係数の関係からは

$$x_3 = \frac{a - 2\lambda\nu - x_1x_2}{x_1 + x_2} \tag{14}$$

が得られ，定数項に関する解と係数の関係からは

$$x_3 = \frac{\nu^2 - b}{x_1x_2} \tag{15}$$

が得られる．式 (14) と (15) は，従来の x_3 に関する公式 (5) と比較して，計算コストの削減に貢献しなさそうである.

注意 2　2 倍算公式について

楕円曲線の 2 倍算にとって，x^2 の項の有無が計算コストに大きく影響する．そのため，E_1 の点の 2 倍算は，座標変換 $x \to x - x_1$ により Weierstrass 標準形 (1) で与えられる楕円曲線 E 上の点に写し，E で 2 倍算を行うことが最良と，著者は現時点では考えている．なお，この座標変換 $x \to x - x_1$ は，射影座標の点 $[X, Y, Z] \in E_0$ を $[X + x_1Z, Y, Z] \in E$ に写す．従って，射影座標の場合，座標変換の計算コストは $\mathcal{M}$ である.

3.2　提案加算公式

3.1 節からアフィン座標系における加算公式は，次のように与えられる.

アルゴリズム 3: (提案加算公式)

入力 $P = (0, y_1)$(アフィン座標)
　　$Q = [X_2, Y_2, Z_2]$(射影座標)
出力 $P + Q = (X_3, Y_3, Z_3)$(射影座標)

1. $A \leftarrow b_0X_2$
2. $B \leftarrow Y_2 - y_1Z_2$
3. $C \leftarrow y_1B$
4. $D \leftarrow A - 2C$
5. $E \leftarrow Z_2D$
6. $F \leftarrow BE$
7. $G \leftarrow X_2^2$
8. $Z_3 \leftarrow X_2G$
9. $H \leftarrow y_1Z_3$
10. $Y_3 \leftarrow F - H$
11. $X_3 \leftarrow X_2E$
12. **return** $[X_3, Y_3, Z_3]$

アフィン座標における提案加算公式:

楕円曲線 $E_0 : y^2 = x^3 + a_0x + b_0x + c_0$ に対して，$P = (0, y_1), Q = (x_2, y_2), P + Q = (x_3, y_3) \in E_0$ とする.

$$\lambda = \frac{y_2 - y_1}{x_2},$$

$$x_3 = \frac{b - 2\lambda y_1}{x_2},$$

$$y_3 = -\lambda x_3 - y_1.$$

上記のアフィン座標系での加算公式を，$MC(A+P=P)$ 系での公式にしアルゴリズム化すると，アルゴリズム 3 が得られる．アルゴリズム 3 の計算コストは $8\mathcal{M} + \mathcal{S}$ である.

表 2: アルゴリズム 1(バイナリ法) の計算コスト

使用公式と座標系		アルゴリズム 1 の計算コスト	$HW(n)=0.5t$, $\mathcal{S}=0.8\mathcal{M}$ の場合	$HW(n)=0.5t$, $\mathcal{S}=\mathcal{M}$ の場合
従来公式	射影座標系	$(12HW(n)+7t-5)\mathcal{M}+(2HW(n)+5t-5)\mathcal{S}+\mathcal{I}$	$(17.8t-9)\mathcal{M}+\mathcal{I}$	$(19t-10)\mathcal{M}+\mathcal{I}$
	Jacobian 座標系	$(12HW(n)+4t-1)\mathcal{M}+(4HW(n)+6t-5)\mathcal{S}+\mathcal{I}$	$(16.4t-5)\mathcal{M}+\mathcal{I}$	$(18t-6)\mathcal{M}+\mathcal{I}$
	$MC(A+P=P)$	$(9HW(n)+7t-5)\mathcal{M}+(2HW(n)+5t-5)\mathcal{S}+\mathcal{I}$	$(16.3t-9)\mathcal{M}+\mathcal{I}$	$(17.5t-10)\mathcal{M}+\mathcal{I}$
	$MC(A+J=J)$	$(8HW(n)+4t-1)\mathcal{M}+(3HW(n)+6t-5)\mathcal{S}+\mathcal{I}$	$(14t-5)\mathcal{M}+\mathcal{I}$	$(15.5t-6)\mathcal{M}+\mathcal{I}$
提案公式 $(A+P=P)$		$(10HW(n)+7t-5)\mathcal{M}+(HW(n)+5t-5)\mathcal{S}+\mathcal{I}$	$(16.4t-9)\mathcal{M}+\mathcal{I}$	$(17.5t-10)\mathcal{M}+\mathcal{I}$

表 3: アルゴリズム 2(SPA 攻撃対策) の計算コスト

使用公式と座標系		アルゴリズム 2 の計算コスト	$\mathcal{S}=0.8\mathcal{M}$ の場合	$\mathcal{S}=\mathcal{M}$ の場合
従来公式	射影座標系	$(19t-17)\mathcal{M}+(7t-7)\mathcal{S}+\mathcal{I}$	$(24.6t-22.6)\mathcal{M}+\mathcal{I}$	$(26t-24)\mathcal{M}+\mathcal{I}$
	Jacobian 座標系	$(16t-13)\mathcal{M}+(10t-9)\mathcal{S}+\mathcal{I}$	$(24t-20.2)\mathcal{M}+\mathcal{I}$	$(26t-22)\mathcal{M}+\mathcal{I}$
	$MC(A+P=P)$	$(16t-14)\mathcal{M}+(7t-7)\mathcal{S}+\mathcal{I}$	$(21.6t-19.6)\mathcal{M}+\mathcal{I}$	$(23t-21)\mathcal{M}+\mathcal{I}$
	$MC(A+J=J)$	$(12t-9)\mathcal{M}+(9t-8)\mathcal{S}+\mathcal{I}$	$(19.2t-15.4)\mathcal{M}+\mathcal{I}$	$(21t-17)\mathcal{M}+\mathcal{I}$
提案公式 $(A+P=P)$		$(17t-15)\mathcal{M}+(6t-6)\mathcal{S}+\mathcal{I}$	$(21.8t-19.8)\mathcal{M}+\mathcal{I}$	$(23t-21)\mathcal{M}+\mathcal{I}$

3.3 計算コストの比較

表 1 は各座標系における従来加算/2 倍算公式の計算コストと $MC(A+P=P)$ 系における提案加算公式の計算コストをまとめている．加算公式のみに注目すると，表 1 の中では提案公式が計算コストに関して最良である．しかしながら注意 2 で述べたように，E_0 上の点の 2 倍算は，座標変換により E 上の点に写してから，行う必要がある．

次にスカラー倍算 nP の計算コストを考える．2.2 節と同様に，$n=(n_{t-1}\ldots n_0)_2$，$HW(n)=n$ のハミング重み，とする．

提案手法を使ってアルゴリズム 1 を実装する場合，E_0 から E への変換が $HW(n)$ 回 (計算コスト $HW(n)\mathcal{M}$)，E から E_0 への変換が $HW(n)$ 回 (計算コスト $HW(n)\mathcal{M}$) が必要となる．従って，提案手法を使うときのアルゴリズム 1 の計算コストは

$$\begin{aligned} &HW(n)\cdot\mathcal{ADD}+(t-1)\cdot\mathcal{DBL} && ((7)\text{ より})\\ &\quad +2HW(n)\cdot\mathcal{M} && (\text{座標変換})\\ &\quad +2\mathcal{M}+\mathcal{I} && (\text{アフィン座標に戻す})\\ &=(10HW(n)+7t-5)\mathcal{M}\\ &\qquad +(HW(n)+5t-5)\mathcal{S}+\mathcal{I} \end{aligned}$$

となる．

提案手法を使ってアルゴリズム 2 を実装する場合，E_0 から E への変換が $t-1$ 回 (計算コスト $(t-1)\mathcal{M}$)，E から E_0 への変換が $t-1$ 回 (計算コスト $(t-1)\mathcal{M}$) が必要となる．従って，提案手法を使うときのアルゴリズム 2 の計算コストは

$$\begin{aligned} &(t-1)\cdot\mathcal{ADD}+(t-1)\cdot\mathcal{DBL} && ((8)\text{ より})\\ &\quad +(t-1)\cdot\mathcal{M} && (\text{座標変換})\\ &\quad +2\mathcal{M}+\mathcal{I} && (\text{アフィン座標に戻す})\\ &=(17t-15)\mathcal{M}+(6t-6)\mathcal{S}+\mathcal{I} \end{aligned}$$

となる．

以上のように，2 倍算の計算コストが増大するため，提案手法を使ってのスカラー倍の計算コストは，加算の計算コストは削減されるにも関わらず 2 倍算の計算コストが増大するため，従来の $MC(A+P=P)$ 系での計算コストとほぼ同じとなる．

表 2 は従来公式と提案公式によるアルゴリズム 1 の計算コストを，表 3 は従来公式と提案公式によるアルゴリズム 2 の計算コストを，それぞれまとめている．また，両表とも $\mathcal{S}=0.8\mathcal{M}$ を仮定する場合と，$\mathcal{S}=\mathcal{M}$ を仮定する場合の計算コストを評価している．

4 まとめと今後の課題

本稿は，Weierstrass 標準形 $y^2=x^3+ax+b$ で与えられる楕円曲線に対して，点の加算の幾

何学的定義から，新たな加算公式を導出した．提案公式では，座標変換を施すことで，楕円曲線は $E_0 : y^2 = x^3 + ax^2 + bx + c$ で与えられ，点 $P \in E_0$ の座標は $(0, y_1)$ であることを仮定する．従って，提案公式を使ってスカラー倍を計算する場合は，点加算の一方の点が定点であるようなスカラー倍算アルゴリズムを使う必要がある．

提案公式を使ってのスカラー倍算の計算コストは，表 2,3 から分かるようにまだ最良とは言えない．しかしながら，提案公式に適した座標系を見つけることで，提案公式を使ってのスカラー倍算の計算コストの削減が達成できることを著者は期待しており，今後そのような座標系を探索したい．

提案公式に適した座標系の探索以外にも，既存の様々な座標系での提案公式の計算コストの評価，提案公式の実装評価，pairing-friendly である BN 曲線 [1] : $y^2 = x^3 + b$ のような特殊な形式の楕円曲線に対しての新加算公式の導出，2 倍算公式の考察，を今後の課題としたい．

参考文献

[1] P. Barreto and M. Naehrig, “Pairing-friendly elliptic curves of prime order,” *SAC 2005*, LNCS 3897, pp.319-331, 2006.

[2] D. Boneh and M. Franklin, “Identity based encryption from the Weil pairing,” *SIAM Journal of Computing*, Vol. 32, No. 3, pp. 586-615, 2003.

[3] K. Chalkias and G. Stephanides, “Timed release cryptography from bilinear pairings using hash chains,” *CMS 2006*, LNCS 4237, pp. 130-140, 2006.

[4] H. Cohen, G. Frey, R. Avanzi, C. Doche, and T. Lange, *Handbook of Elliptic and hyperelliptic curve cryptography, 2nd edition*, Chapman and Hall/CRC, 2011.

[5] H, Cohen, A, Miyaji, and T. Ono, “Effcient Elliptic Curve Exponentiation Using Mixed Coordinates,” it ASIACRYPT’98, LNCS 1514, pp.51-65, 1998.

[6] H. Edwards, “A normal form for elliptic curves,” *Bull. Amer. Math. Soc.*. Vol.44, No.3, pp.393-422, 2007.

[7] D. Freeman, M. Scott, and E. Teske, “A taxonomy of pairing-friendly elliptic curves,” Journal of Cryptology 23, pp.224-280, 2010.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-based Encryption for Fine-grained Access Control of Encrypted Data,” CCS 2010, pp.89-98, 2006.

[9] V. Miller, “The Weil Pairing, and Its Efficient Calculation,” Journal of Cryptology, Vol.17, No.4, pp.235-261, 2004.

[10] P. L. Montgomery, “Speeding the Pollard and elliptic curve method of factorization,” *Math. Comp.* Vol.48, No.177, pp.243-264, 1987.

[11] R. Sakai, K. Ohgishi, and M. Kasahara, “Cryptosystems based on pairing,” *SCIS 2000*, pp. (2000)

[12] J. Silverman, *The arithmetic of elliptic curves*, Springer–Verlag, 1986.

A もう一つの新加算公式

3.1 節では，式 (9) で与えられる楕円曲線 E_0 に対して，$P = (0, y_1), Q = (x_2, y_2)$ から $P + Q$ の座標を求める加算公式を，3 次方程式 (10) の 1 次の項に関する解と係数の関係から導出した．ここでは，定数項に関する解と係数の関係を用いても別の加算公式を導出できることを示す．3 次方程式 (10) の根を x_1, x_2, x_3 とする．本稿では $x_1 = 0$ を仮定しているが，まずはこの仮定を設定しないと，3 次方程式 (10) の定数項に関する解と係数の関係から，

$$\begin{aligned} x_1x_2x_3 &= b_0 - \nu^2 \\ &= b_0 - \frac{(x_2y_1 - x_1y_2)^2}{(x_2 - x_1)^2} \end{aligned}$$

が得られる．ここで上式の分子を，$y_i^2 = x_i^3 + a_0x_i^2 + b_0x_i + c_0$ $(i = 1, 2)$ を使って整理すると

分子$= x_1x_2(-x_1^2x_2 - x_1x_2^2 - a_0x_1 - a_0x_2 + 2y_1y_2 - 2b_0)$

となる．従って，

$$x_3 = \frac{-x_1^2x_2 - x_1x_2^2 - a_0x_1 - a_0x_2 + 2y_1y_2 - 2b_0)}{(x_2 - x_1)^2}$$

となる．ここで $x_1 = 0$ を代入すると，

$$x_3 = \frac{-a_0x_2 + 2y_1y_2 - 2b_0}{x_2^2}$$

が得られる．