ツイスト曲線上の有理点に対する有理点ノルムの性質とRho法への応用

有井 智紀† 根角 健太† 野上 保之†

†岡山大学大学院自然科学研究科
700–8530 岡山県岡山市北区津島中 3–1–1
{arii,nekado,nogami}@trans.cne.okayama-u.ac.jp

あらまし 近年，公開鍵暗号の１つであるペアリング暗号が注目されている．ペアリング暗号は楕円曲線暗号を応用した暗号であり，その安全性は楕円曲線上の離散対数問題 (ECDLP) にも依存している．そのため，様々な攻撃法を用いて ECDLP を解く試みがペアリング暗号の安全性の検証に繋がる．本稿では，ペアリングに使用される BN 曲線上の特殊な巡回群 $\mathbb{G}'_2$ を攻撃の対象とし，攻撃法として Rho 法を応用する． 具体的には，グルーピングや省メモリ化を行った Rho 法を基に，有理点の座標のノルムを衝突判定に用いたものを提案し，性能を評価する．また，提案手法およびその基となった Rho 法では偽衝突と呼ばれる現象が発生する．そこで，それぞれの手法において有理点の座標とそのノルムの値を求め，偽衝突を起こす点の個数を調査する．実験結果では，それらの点は有理点の座標のノルムに比べて有理点の座標に多く含まれていることを報告する．

A Property of Norm Pairs of Rational Point on A Twisted Elliptic Curve and Adapting Pollard's Rho Method

Tomonori Arii † Kenta Nekado † Yasuyuki Nogami †

†Graduate School of Natural Science and Technology, Okayama University
3–1–1 Tsushima-naka, Kita-ward, Okayama–city, Okayama, 700–8530, JAPAN
{arii,nekado,nogami}@trans.cne.okayama-u.ac.jp

Abstract Recently, pairing–based cryptography which is the public key cryptography has received much attention. Since the security of pairing–based cryptography is based on Elliptic Curve Discrete Logarithm Problem (ECDLP), solving ECDLP leads to a lack of the security. As an approach for solving ECDLP, this paper considers the Pollard's rho method which adapts the memory–saved technique, which uses the *norm* of a coordinate in each rational point on a certain torsion group of $\mathbb{G}'_2$ over Barreto–Naehrig pairing–friendly curve. This paper implemets both of the proposed rho method and the conventional rho method and compares them.

1 序論

近年，ID–base 暗号 [1] やグループ署名 [2] などのペアリングに基づいた暗号技術が注目を集めている．これらの技術を実用化するために，Ate[3], R–ate[4], twisted–Ate[5], Optimal Ate[6], Cross–twisted Xate ペアリング [7] などの様々なペアリングが提案されている．このペアリング暗号技術は楕円曲線暗号技術を応用した技術である． 現在，ペアリング暗号技術および楕円曲線暗号技術の研究が盛んに行われており，ペアリング計算の高速化，効率化だけでなく暗号技術の安全性の検証といった研究も注目

されている．

本研究では，楕円曲線暗号の安全性を検証するために， ペアリングに用いられる楕円曲線上のねじれ群上に存在する $\mathbb{G}_2'$ を攻撃する． 具体的には，Barreto–Naehrig (BN) 曲線 [8] 上の $\mathbb{G}_2'$ に対して，攻撃法として有名な Pollard の Rho 法 [9] を適用することを考える．本稿では，グルーピングや省メモリ化を行った Rho 法を基に，その衝突判定に座標のノルムを用いたものを提案，実装する．そして，基となった Rho 法と提案法との性能比較を行う．この提案法では，特徴点のみ保持する省メモリ化手法を用いてノルム計算処理の発生回数を抑え，基となる Rho 法と同等の実行速度を維持している．

また，基となる Rho 法では衝突判定に座標の一部の要素の値を用いているが，提案法では座標のノルム値を用いている．今回，どちらの値を用いた実装でも偽衝突と呼ばれる現象が発生することがある．そこで，座標の一部の値を用いた場合とノルム値を用いた場合では，どちらが偽衝突を起こしやすいのかを調査する．低い位数の $\mathbb{G}_2'$ 上の有理点を調査した結果では，座標のノルム値の方が偽衝突を引き起こす点が少なかったことを報告する．

2 数学的準備

本章では，楕円曲線と Ate ペアリング，ツイスト写像および Frobenius 写像，そして本稿で重要となる拡大体の元に対するノルム計算，共役有理点と Pollard の Rho 法について復習する．

2.1 楕円曲線と BN 曲線

標数 $p > 3$ として素体 $\mathbb{F}_p$ 上で定義される楕円曲線 E を考える．一般的な楕円曲線の式は以下のように表される．

$$E : y^2 = x^3 + ax + b, \qquad a, b \in \mathbb{F}_p \tag{1}$$

無限遠点 $\mathcal{O}$ を含む E 上の有理点の集合は，有理点に関する加算を定義することで可換群を成し，これを $E(\mathbb{F}_p)$ と表す．ここで $E(\mathbb{F}_p)$ の位数を $\#E(\mathbb{F}_p)$，Frobenius のトレースを t とすると，$\#E(\mathbb{F}_p)$ は t を用いて次式で与えられる．

$$\#E(\mathbb{F}_p) = p + 1 - t \tag{2}$$

また，r を $\#E(\mathbb{F}_p)$ を割り切る大きな素数とし，$r|(p^k - 1)$ を満たす最小の正整数 k を埋め込み次数とする．このとき，$\mathbb{F}_p$ の k 次拡大体 $\mathbb{F}_{p^k}$ 上で定義される楕円曲線上の有理点群がねじれ群の構造をもつ．このねじれ群の構造によってペアリングを行うことが可能となる．

ペアリングに用いられる楕円曲線の中でも，Barreto–Naehrig (BN) 曲線 [8] は以下のように整数変数 ℓ を用いて，曲線のパラメータを組織的に決定できる特徴があるためによく使用される．

$$p(\ell) = 36\ell^4 - 36\ell^3 + 24\ell^2 - 6\ell + 1 \tag{3a}$$
$$r(\ell) = 36\ell^4 - 36\ell^3 + 18\ell^2 - 6\ell + 1 \tag{3b}$$
$$t(\ell) = 6\ell^2 + 1 \tag{3c}$$

また，BN 曲線の埋め込み次数は $k = 12$ であり，加えて 6 次ツイストが行える曲線として以下のように与えられる．

$$E : y^2 = x^3 + b, \qquad b \in \mathbb{F}_p \tag{4}$$

2.2 Ate ペアリング

埋め込み次数を k とするとき， $E(\mathbb{F}_{p^k})$ 上の位数 r の部分群を $E(\mathbb{F}_{p^k})[r]$ と表記する．また，$[i]R$ を有理点 R に対する i 倍算とするとき，Ate ペアリング [3] は非退化な双線形写像 $\alpha(\cdot,\cdot)$ として次のように定義される．

$$\mathbb{G}_1 = E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\phi - [1]) \tag{5a}$$
$$\mathbb{G}_2 = E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\phi - [p]) \tag{5b}$$

$$\alpha(\cdot,\cdot) : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{F}_{p^k}^* / (\mathbb{F}_{p^k}^*)^r \tag{6}$$

式(5a)，式(5b)に示すように，$\mathbb{G}_1$ は素体上の有理点群，$\mathbb{G}_2$ は 2.4 節で述べる有理点の Frobenius 写像 ϕ と p 倍算が一致する特別な有理点群となることを表している．

2.3 ツイスト写像

本節では，BN 曲線で行うことが可能である 6 次ツイストについて述べる．まず，6 次ツイストを可能にするためには，標数 p が $6 \mid (p-1)$ を満たす必要がある．そして，楕円曲線 E の埋め込み次数を k とし，$k = 6e$ (e は任意の自然数) で与えられ，なおかつ，楕円曲線が $\mathbb{F}_p$ 上の元 b を用いて以下の形で与えられる場合を考える．

$$E:\ y^2 = x^3 + b \tag{7a}$$
$$E':\ y^2 = x^3 + bv^{-1} \tag{7b}$$
$$E'':\ y^2 = x^3 + bv^{-5} \tag{7c}$$

ここで $v \in \mathbb{F}_{p^e}$ は平方非剰余かつ，立方非剰余元とする．このとき，その楕円曲線は 6 次ツイスト可能である．ただし，6 次ツイストについては曲線の形が E', E'' の 2 種類あり，どちらか一方の曲線上にのみ，ペアリングに用いる位数 r の $\mathbb{G}_2$ と同型な部分群 $\mathbb{G}_2'$ が存在する．そして，曲線上に $\mathbb{G}_2'$ の存在する方をツイスト曲線とする．ここで，楕円曲線 E とその 6 次ツイスト曲線を E'(または E'') とすると $E(\mathbb{F}_{p^k})$ と $E'(\mathbb{F}_{p^e})$(または $E''(\mathbb{F}_{p^e})$ の間にはツイスト写像 ψ が存在する．以下に 6 次ツイストのツイスト写像を示す．

$$\psi : \begin{cases} E'(\mathbb{F}_{p^e}) & \longmapsto E(\mathbb{F}_{p^{6e}}) \\ (x, y) & \longmapsto (v^{1/3}x, v^{1/2}y) \end{cases} \tag{8a}$$

または

$$\psi : \begin{cases} E''(\mathbb{F}_{p^e}) & \longmapsto E(\mathbb{F}_{p^{6e}}) \\ (x, y) & \longmapsto (v^{5/3}x, v^{5/2}y) \end{cases} \tag{8b}$$

本稿で扱う BN 曲線は，埋め込み次数 $k = 12$ であり，標数 p は式 (3a) より $6|(p-1)$ を満たす．また，BN 曲線の式 (4) は 6 次ツイストの条件となる式 (7a) と一致することから，6 次ツイスト可能な曲線であることがわかる． 本稿では説明を簡単にするために，BN 曲線 E の 6 次ツイスト曲線 E' が以下の式 (9) で与えられている場合を考える．

$$E' : y^2 = x^3 + bv^{-1} \tag{9}$$

ここで，v は $\mathbb{F}_{p^2}$ 上の平方非剰余元かつ立方非剰余元とする．このツイスト曲線上の有理点群には，式 (5b) を満たす有理点群 $\mathbb{G}_2$ と同型な有理点群が存在し，これを有理点群 $\mathbb{G}_2'$ とする．BN 曲線を用いた場合では，有理点群 $\mathbb{G}_2$ は $E(\mathbb{F}_{p^{12}})$ 上で定義され，ツイスト曲線上の有理点群 $\mathbb{G}_2'$ は $E'(\mathbb{F}_{p^2})$ 上で定義される．そして，$\mathbb{G}_2'$ 上の有理点を (x', y') とすると，有理点群 $\mathbb{G}_2$ と $\mathbb{G}_2'$ の間には次のようなツイスト写像が与えられる．

$$\psi : \begin{cases} \mathbb{G}_2' \subset E'(\mathbb{F}_{p^2}) & \longmapsto \quad \mathbb{G}_2 \subset E(\mathbb{F}_{p^{12}}) \\ (x', y') & \longmapsto \quad (v^{1/3}x', v^{1/2}y') \end{cases} \tag{10}$$

本稿では，この $\mathbb{G}_2'$ に対しての Rho 法の効率化を考える．

2.4 Frobenius 写像

拡大体 $\mathbb{F}_{p^n}$ の元 a に対し，$a \to a^p$ となる写像を $\mathbb{F}_p$ に関する Frobenius 写像と呼ぶ．さらに，楕円曲線 E の係数体が $\mathbb{F}_p$ であるとき，$E(\mathbb{F}_{p^n})$ 上の有理点 $Q = (x, y)$ に対して次のような写像を考える．

$$\phi : (x, y) \to (x^p, y^p), \qquad x, y \in \mathbb{F}_{p^n} \tag{11}$$

このような写像 ϕ を，本稿では有理点 Q に対する Frobenius 写像と呼び，$\phi(Q)$ もまた $E(\mathbb{F}_{p^n})$ 上の有理点となる．さらに，この ϕ は $\phi^n(Q) = Q$ を満たす．このように，係数体が $\mathbb{F}_p$ であるとき $E(\mathbb{F}_{p^n})$ 上の有理点に対する Frobenius 写像 ϕ は周期 n をもつ自己同型写像である．BN 曲線上の有理点群 $\mathbb{G}_2$ の点に対して，有理点の Frobenius 写像 ϕ は周期 12 をもち，加えて，$Q \in \mathbb{G}_2$ とするとき，式 (5b) より以下の関係が成り立つ．

$$\phi(Q) = [p]Q \tag{12}$$

また，2.3 節で述べた，$\mathbb{G}_2$ と同型なツイスト曲線上の有理点群 $\mathbb{G}_2'$ 上の有理点は，式 (10) で与えられるツイスト写像 ψ によって，$\mathbb{G}_2$ 上の有理点と一対一対応する． ここで，$\mathbb{G}_2'$ 上の有理点 $P' = (x', y')$ を，$\mathbb{G}_2$ 上の有理点 $P = \psi(P')$ へ

ツイスト写像し，有理点に対する Frobenius 写像を行った後，$\mathbb{G}_2$ 上の有理点から $\mathbb{G}_2'$ の有理点へ逆ツイスト写像することを考える．この一連の写像を skew–Frobenius 写像 [10] と呼び，$\tilde{\phi}$ と表記すると，$\tilde{\phi}(P')$ は以下のように与えられる．

$$\tilde{\phi}(P') = \psi^{-1}(\phi(\psi(P'))) \tag{13a}$$
$$= (v^{\frac{p-1}{3}}x'^p, v^{\frac{(p-1)}{2}}y'^p) \tag{13b}$$

BN 曲線により構成された $\mathbb{G}_2'$ 上の有理点では，$\mathbb{G}_2$ と同様に skew–Frobenius 写像 $\tilde{\phi}$ は周期 12 をもつ．加えて，$Q' \in \mathbb{G}_2'$ とするとき，以下の関係が成り立つ．

$$\tilde{\phi}(Q') = [p]Q' \tag{14}$$

2.5 ノルム

拡大体 $\mathbb{F}_{p^n}$ の元を a とするとき，a の $\mathbb{F}_p$ に関する共役元は a^{p^i} (ただし $i = 0, 1, 2, \ldots, n-1$) で与えられる．そして，a を含むこれらの共役元の総積を元 a の $\mathbb{F}_p$ に関するノルムとして以下のように表す．

$$N(a) = a \times a^p \times \cdots \times a^{p^{n-1}} \tag{15a}$$
$$= a^{(1+p+\cdots+p^{n-1})} \tag{15b}$$

このとき，$N(a)$ は $\mathbb{F}_p$ 上の元となる．

2.6 共役有理点

2.4 節で述べた Frobenius 写像 ϕ および，skew–Frobenius 写像 $\tilde{\phi}$ によって関連付けられる有理点の集合を，本稿では共役有理点と呼ぶ．ここで，$\mathbb{G}_2'$ に含まれる有理点を $P' = (x', y')$ とすると， P' の共役有理点は式 (13b) より，以下のようになる．

$$\begin{cases} \tilde{\phi}^i(P') & = (v^{\frac{p^i-1}{3}}x', v^{\frac{p^i-1}{2}}y'), (i : \text{偶数}) \\ \tilde{\phi}^i(P') & = (v^{\frac{p^i-1}{3}}x'^p, v^{\frac{p^i-1}{2}}y'^p), (i : \text{奇数}) \end{cases} \tag{16}$$

以下では，$4|(p-1)$ の場合を考える．ここで，x 座標について注目する． $\mathbb{F}_{p^2}$ 上で平方非剰余元かつ立方非剰余元である v を，以下の式を満たすような元 $\tau \in \mathbb{F}_{p^2}$ を用いて構成する．

$$v = \tau^{\frac{p+1}{2}} \tag{17}$$

すると，以下の式が成り立つ．

$$v^{\frac{p-1}{3}} = (\tau^{p+1})^{\frac{p-1}{6}} \tag{18}$$

τ^{p+1} は $\tau \in \mathbb{F}_{p^2}$ の $\mathbb{F}_p$ に関するノルムより $\mathbb{F}_p$ 上の元となる．さらに BN 曲線では $6|(p-1)$ が常に成り立つことから $v^{\frac{p-1}{3}}$ は $\mathbb{F}_p$ 上に存在する 1 の原始 6 乗根である．そこで $v^{\frac{p-1}{3}} = \lambda$ とすると次式が成り立つ．

$$\lambda^6 - 1 = (\lambda^3 - 1)(\lambda^3 + 1) = 0$$

ただし $\lambda^3 \neq 1$ より，

$$\therefore \lambda^3 = -1 \tag{19}$$

$$\lambda^3 + 1 = (\lambda + 1)(\lambda^2 - \lambda + 1) = 0$$

ただし $\lambda \neq 1$ より，

$$\therefore \lambda^2 = \lambda - 1 \tag{20}$$

また，y 座標に関しても $v^{\frac{p-1}{2}} = \mu$ とすると，μ は 1 の原始 4 乗根であり，同様にして次式が成り立つ．

$$\mu^2 = -1 \tag{21}$$

式 (18) ～式 (21) および $\lambda \in \mathbb{F}_p$ より，λ，μ を用いて以下の式が成り立つ．

$$v^{\frac{p-1}{3}} = \lambda \tag{22a}$$
$$v^{\frac{p^2-1}{3}} = v^{\frac{p(p-1)}{3}+\frac{(p-1)}{3}}$$
$$= (v^{\frac{p-1}{3}})^p \cdot v^{\frac{p-1}{3}} = \lambda^2 = \lambda - 1 \tag{22b}$$
$$v^{\frac{p^3-1}{3}} = v^{\frac{p(p^2-1)}{3}+\frac{(p-1)}{3}}$$
$$= (v^{\frac{p^2-1}{3}})^p \cdot v^{\frac{p-1}{3}} = \lambda^3 = -1 \tag{22c}$$
$$v^{\frac{p^4-1}{3}} = v^{\frac{p(p^3-1)}{3}+\frac{(p-1)}{3}}$$
$$= (v^{\frac{p^3-1}{3}})^p \cdot v^{\frac{p-1}{3}} = \lambda^4 = -\lambda \tag{22d}$$
$$v^{\frac{p^5-1}{3}} = v^{\frac{p(p^4-1)}{3}+\frac{(p-1)}{3}}$$
$$= (v^{\frac{p^4-1}{3}})^p \cdot v^{\frac{p-1}{3}} = \lambda^5 = -(\lambda - 1) \tag{22e}$$

$$v^{\frac{p-1}{2}} = \mu \tag{23a}$$
$$v^{\frac{p^2-1}{2}} = v^{\frac{p(p-1)}{2}+\frac{(p-1)}{2}}$$
$$= (v^{\frac{p-1}{2}})^p \cdot v^{\frac{p-1}{2}} = \mu^2 = -1 \tag{23b}$$
$$v^{\frac{p^3-1}{2}} = v^{\frac{p(p^2-1)}{2}+\frac{(p-1)}{2}}$$
$$= (v^{\frac{p^2-1}{2}})^p \cdot v^{\frac{p-1}{2}} = \mu^3 = -\mu \tag{23c}$$

これより P' の共役有理点は以下のように表される．

$$\tilde{\phi^0}(P') = (x', y') \tag{24a}$$
$$\tilde{\phi^1}(P') = (\lambda x'^p, \mu y'^p) \tag{24b}$$
$$\tilde{\phi^2}(P') = ((\lambda-1)x', -y') \tag{24c}$$
$$\tilde{\phi^3}(P') = (-x'^p, -\mu y'^p) \tag{24d}$$
$$\tilde{\phi^4}(P') = (-\lambda x', y') \tag{24e}$$
$$\tilde{\phi^5}(P') = (-(\lambda-1)x'^p, \mu y'^p) \tag{24f}$$
$$\tilde{\phi^6}(P') = (x', -y') \tag{24g}$$
$$\tilde{\phi^7}(P') = (\lambda x'^p, -\mu y'^p) \tag{24h}$$
$$\tilde{\phi^8}(P') = ((\lambda-1)x', y') \tag{24i}$$
$$\tilde{\phi^9}(P') = (-x'^p, \mu y'^p) \tag{24j}$$
$$\tilde{\phi^{10}}(P') = (-\lambda x', -y') \tag{24k}$$
$$\tilde{\phi^{11}}(P') = (-(\lambda-1)x'^p, -\mu y'^p) \tag{24l}$$

本稿における Rho 法の計算機実装では，これらの共役有理点の中から代表となる点を決定しグルーピングを行う代表元決定法 [11] を用いている．

2.7 Pollard の Rho 法

本節では，楕円曲線上の離散対数問題 (ECDLP) と，それを解く手法の 1 つである Pollard の Rho 法 [9] について述べる．

楕円曲線暗号の安全性の根拠となっている楕円曲線上の離散対数問題 (ECDLP) とは，次の問題のことを指す．

問題 ： $P, Q \in E(\mathbb{F}_{p^k})$ が与えられており，

$$Q = [s]P \tag{25}$$

となる s が存在するならば，その s を求めよ．

Rho 法では有理点を次々生成し，衝突点と呼ばれる同じ座標をもった 2 個の有理点を見つけることで ECDLP を解く．一般的な Rho 法の実装では，生成した有理点の情報を記憶しておくため，省メモリ化を考える必要がある．省メモリ化の手法としては，Rho 法の性質を利用して特徴的な点のみを保持することで記憶領域の使用を抑える手法や，共役有理点のグルーピングを利用して生成する有理点の個数を抑える手法などが提案されている．

また，保持する座標情報を一部削除することでも省メモリ化することが可能である． 本稿の対象としている $\mathbb{G}'_2$ に含まれる有理点の座標は拡大体の元で構成されているため， 複数の素体の元に分割して扱うことが可能である．そのため，一部の元の値のみ記憶して衝突判定に利用することで省メモリ化を図ることができる． ただし，この省メモリ化を行うことで座標情報の一部が失われてしまい十分な衝突点の判定を行うことができず，本来は衝突点として扱わない有理点を衝突点と見なしてしまう可能性が出てくる．このような現象を偽衝突と呼ぶ．この偽衝突の詳細は 3.1 節にて説明する．

3 有理点座標とノルム値の分布

本章では，Rho 法で座標情報を省メモリ化して保持する場合に発生する偽衝突について述べる． そして，位数 7 ビットおよび 28 ビットの $\mathbb{G}'_2$ に含まれる有理点の座標とそのノルム値を調べ，偽衝突を起こす点がそれぞれどれだけ存在しているかを報告する．

3.1 偽衝突

$\mathbb{G}'_2$ に含まれる有理点の座標は $\mathbb{F}_{p^2}$ 上の元である．ここで，$P' = (x', y') \in \mathbb{G}'_2$ とするとき，P' は素体 $\mathbb{F}_p$ の元 4 個を用いて次のように表すことができる．

$$P' = ((x_0, x_1), (y_0, y_1)),$$
$$x_0, x_1, y_0, y_1 \in \mathbb{F}_p \tag{26}$$

ここで，$\mathbb{G}'_2$ に対して効率のよい Rho 法の実装を考える場合，衝突点判定用に保持する有理点の座標を，例えば x_0 のみとすることで省メモリ化が可能である．しかしこの場合，それ以外の元情報を保持しないことから，x_0 のみ同じ値をもつような有理点を発見したときに，その点を誤って衝突点として判断してしまう．そのような現象を偽衝突と呼ぶ．偽衝突の起き得る実装では，正しい解かどうかを判断するために，求めた解を用いて式(25)が成り立つ確認が必要となる．

3.2 共役有理点のノルム

前章の式(24)より，有理点 P' の共役有理点に対して，それぞれの座標のノルムを求めたものは以下のようになる．

$$N(\tilde{\phi}^0(P')) = P' = (N(x'), N(y')) \quad (27a)$$
$$N(\tilde{\phi}^1(P')) = ((\lambda-1)N(x'), -N(y')) \quad (27b)$$
$$N(\tilde{\phi}^2(P')) = (-\lambda N(x'), N(y')) \quad (27c)$$
$$N(\tilde{\phi}^3(P')) = (N(x'), -N(y')) \quad (27d)$$
$$N(\tilde{\phi}^4(P')) = ((\lambda-1)N(x'), N(y')) \quad (27e)$$
$$N(\tilde{\phi}^5(P')) = (-\lambda N(x'), -N(y')) \quad (27f)$$
$$N(\tilde{\phi}^6(P')) = (N(x'), N(y')) \quad (27g)$$
$$N(\tilde{\phi}^7(P')) = ((\lambda-1)N(x'), -N(y')) \quad (27h)$$
$$N(\tilde{\phi}^8(P')) = (-\lambda N(x'), N(y')) \quad (27i)$$
$$N(\tilde{\phi}^9(P')) = (N(x'), -N(y')) \quad (27j)$$
$$N(\tilde{\phi^{10}}(P')) = ((\lambda-1)N(x'), N(y')) \quad (27k)$$
$$N(\tilde{\phi^{11}}(P')) = (-\lambda N(x'), -N(y')) \quad (27l)$$

式(27)より，y 座標の周期が 2 であり $N(y')$ と $-N(y')$ であることから，2 個のうち一方が求まると，もう一方は容易に求まる．このため，本稿では有理点の y 座標を用いることとする．

3.3 偽衝突を起こす点の総数

本節では，$\mathbb{G}'_2$ に含まれる r 個の有理点のうち y 座標の一部の要素として式(26)の y_0 と，y 座標のノルム値の中で，同じ値をもつものの個数を調べ報告する．

本研究では，計算機を用いて 7 ビット，および 28 ビットの位数をもつ $\mathbb{G}'_2$ の有理点を調査した．すべての有理点の y_0 座標とノルム値について調査した結果を表 1 に示す．ここで式(24)および式(27)より，同じ共役有理点集合に含まれる点には，一部同じ値をもつものが存在することがわかる． まず y_0 の場合では，式(24a), 式(24e), 式(24i)の 3 組の点が同じ y 座標の値をもつ．さらに式(24c), 式(24g), 式(24k)に関しては，y 座標の値が加法に関する逆元となっているため，容易に求めることが可能である．そこで，本稿ではこれら 6 点を 1 つのグループとした．残りの 6 点に関しても，同様にグループとして扱う．一方 y 座標のノルムでは，式(27)より，6 組の点が同じ値 $N(y')$ をもち，残りの 6 組の点が $-N(y')$ をもつ．y_0 のときと同様，$N(y')$ より $-N(y')$ が容易に求められるため，1 つの共役有理点を 1 つのグループとして扱える． そして，これらの同じグループ内に含まれる点同士では，skew–Frobenius 写像の性質を用いることで ECDLP を解くことが可能であるため，偽衝突を行う点として数えていない． そのため，表 1 の結果に現れている値は，同じ値をもつにもかかわらず ECDLP を解くことのできない別グループの数となっている．

そして今回調査した位数の $\mathbb{G}'_2$ では，座標の y_0 の値に比べてノルム値の方が，偽衝突を起こす有理点の数は少ない傾向があることが判明した．

表 1: 偽衝突を起こす点

位数 [bit]	y 座標のノルム値 [グループ (12)]	y_0 座標 [グループ (6)]
7	3	6
28	1,697,129	6,430,175

() 内の値は 1 グループあたりの有理点の個数

4 計算機実装

本稿では，共役有理点の中から代表元を選出するグルーピング化と，特徴点のみ保持する省

メモリ化を行った Rho 法を通常の Rho 法と呼称する．そして，通常の Rho 法を基に保持する有理点情報のうち，衝突点判定に用いる情報を座標の一部の情報から y 座標のノルムにした Rho 法を提案する．

通常の Rho 法からの変更点としては，有理点の情報を保持するときに座標のノルム計算処理が増えている．具体的な実装は以下の通りである．

1. 有理点を生成
2. 座標の y_0 の要素を確認
3. y_0 の値の下位数ビットが全て 0 ならノルム計算
4. 計算結果の値を保持

この特徴点のみ保持する手法を利用することで，有理点を保持する個数を大幅に抑えることが可能である．このために，情報を保持する際に行うノルム計算の処理時間を全体の実行時間に比べて短くすることが可能である．

ここで，提案手法と通常の Rho 法の実装環境を表 2 に示す．そして，提案手法と通常の Rho 法の性能比較を行った結果を表 3 に示す．比較結果より，両手法の実行時間の差がわずかであることがわかる．

表 2: 提案法および通常の Rho 法の実装環境

OS	Windows7 Professional
CPU	Intel Core 2 Quad (2.83GHz)
メモリ	2GiB
言語	C++
ライブラリ	ntl-5.5.2
コンパイラ	g++ 4.5.2

5 結論

本稿では，まずペアリングに使用される拡大体上の有理点群 $\mathbb{G}'_2$ の座標とそのノルムを求め，偽衝突の原因となる同じ値をもつ点の個数を調査した．調査の結果，28 ビットの位数をもつ $\mathbb{G}'_2$ では，ノルムに比べて座標には偽衝突を起こす値をもつ有理点が約 4 倍多く存在することがわかった．それゆえ，座標に比べてそのノルムでは同じ値をもつものが少ない傾向があると推測できる．

表 3: 提案法と通常の Rho 法の性能比較

位数 [bit]	提案法 [sec]	従来法 [sec]	差 [%]	保持点 生成点
28	1.1	1.1	0.0	54
				6,760
39	34.8	34.6	−1.4	147
				147,000
48	1,310	1,307	0.2	600
				5,090,000

そこで，$\mathbb{G}'_2$ を対象とした衝突判定に座標のノルムを用いた Rho 法を提案した．具体的には，代表元決定法と特徴点のみ保持する省メモリ化を行った Rho 法を基に，衝突点判定用の情報に座標のノルムを用いたものを提案した． そして，提案手法とその基となった Rho 法の性能を比較を行い，実行速度がほぼ同等となる結果を得た．

6 謝辞

本研究は「科学研究費補助金：基盤研究（C）（22560378）スケーラブルな失効可能グループ署名方式の提案とその実装」の助成を受けて行われた．

参考文献

[1] R. Sakai, K. Ohgishi, and M. Kasahara, “Cryptosystems based on pairing,” 暗号と情報セキュリティシンポジウム (SCIS2002), 2000.

[2] T. Nakanishi and N. Funabiki, “Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability

from Bilinear Maps," Asiacrypt2005, *LNCS*, vol. 3788, pp. 443-454, 2005.

[3] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto, "Optimised versions of the Ate and Twisted Ate Pairings," IEICE transactions on fundamentals of electronics, communications and computer sciences 92(7), pp. 1660–1667, 2009.

[4] E. Lee, H. Lee, and C. Park, "Efficient and Generalized Pairing Computation on Abelien Varieties," IACR ePrint archive, available at http://eprint.iacr.org/2008/040

[5] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto, "Optimised versions of the Ate and Twisted Ate Pairings," IMA2007, LNCS, Vol. 4887, pp. 302-312, 2007.

[6] F. Vercauteren, "Optimal Pairings," IACR ePrint archive, available at http://eprint.iacr.org/2008/096

[7] Y. Nogami, Y. Sakemi, H. Kato, M. Akane, and Y. Morikawa, "Integer Variable χ–Based Cross Twisted Ate Pairing and Its Optimization for Barreto–Naehrig Curve," IEICE transactions on fundamentals of electronics, communications and computer sciences 92(8), pp. 1859–1867, 2009.

[8] P. S. L. M. Barreto and M. Naehrig, "Pairing–Friendly Elliptic Curves of Prime Order," SAC2005, LNCS 3897, Springer–Verlag, pp. 319–331, 2006.

[9] J. Pollard, "Monte Carlo Methods for Index Computation (mod p)," Math. Comp, vol. 32, pp. 918–924, 1978.

[10] T. Iijima, K. Matsuo, J. Chao, S. Tsuji, "Construction of Frobenius maps of twists elliptic curves and its application to elliptic scalar multiplication." In: Proc. of SCIS 2002, IEICE, Japan, pp. 699-702 (2002),

[11] 河野祐輝, 根角健太, 森佑樹, 有井智紀, 野上保之, "BN 曲線における $\mathbb{G}_2$ 上の ρ 法に関する効率的な代表元決定法," 情報理論研究会, 電子情報通信学会技術者報告, IT2012