$\mathbb{F}_{p^2}$ 上で 6 次ツイストした BN 曲線上ペアリング有理点群に対する Rho 法の適用

角力 大地, 森 佑樹, 野上 保之 *
松嶋 智子 † 上原 聡 ‡

* 岡山大学 工学部
岡山県岡山市北区津島中 3-1-1
{sumo, mori, nogami}@trans.cne.okayama-u.ac.jp

† 職業能力開発総合大学校
神奈川県相模原市緑区橋本台 4-1-1
tomoko@uitec.ac.jp

‡ 北九州市立大学
福岡県北九州市若松区ひびきの 1-1
uehara@env.kitakyu-u.ac.jp

あらまし BN 曲線を用いた最近の効率のよいペアリングでは、これを $\mathbb{F}_{p^2}$ 上で 6 次ツイストして与えられるペアリング有理点群が用いられる。これに対して、定義体 $\mathbb{F}_{p^2}$ を OEF を用いて構成した場合の、Rho 法の効率のよい適用について考える。

Rho Method for Pairing Rational Point Group on Sextic-twisted BN Curve over $\mathbb{F}_{p^2}$

Taichi Sumo, Yuki Mori, Yasuyuki Nogami*
Tomoko Matsushima† Satoshi Uehara‡

* Faculty of Engineering, Okayama University
3–1–1, Tsushima, Kita, Okayama, Okayama
{sumo, mori, nogami}@trans.cne.okayama-u.ac.jp

†Polytechnic University
4–1–1, Hashimotodai, Sagamihara, Kanagawa
tomoko@uitec.ac.jp

‡The University of Kitakyushu
1–1, Wakamatsu, Kitakyushu, Fukuoka
uehara@env.kitakyu-u.ac.jp

Abstract Recent efficient pairings with BN curve use a pairing rational point group with sextic twist over $\mathbb{F}_{p^2}$. For the twisted pairing rational point group, this research considers to efficiently apply the rho method for which OEF technique plays an important role.

1 Introduction

Recently, pairing based cryptographic applications such as ID-based cryptography and group signature schemes have received much attention. Barreto–Naehrig (BN) curve [1] with embedding degree 12 is one of the most important families of ordinary pairing friendly curves because sextic twist is available. Recent efficient pairings with BN curve such as Ate pairing [2], twisted-Ate pairing [3] and cross–twisted Ate pairing [4] also use a pairing rational point group $\mathbb{G}_2$ on sextic twisted curve over $\mathbb{F}_{p^2}$. Thus, $\mathbb{G}_2$ has the isomorphic group $\mathbb{G}_2'$ over twisted curve $E'(\mathbb{F}_{p^2})$. This paper focuses on the isomorphic groups. In order to solve ECDLPs, Pollard's rho method [5] that uses random walks and collisions is well-known. In detail, let $E(\mathbb{F}_q)$ be an elliptic curve and let $P, Q \in E(\mathbb{F}_q)$ satisfy $P = [s]Q$. In order to solve the discrete logarithm $[s] = \log_P(Q)$, Pollard's rho method tries to find some col-

lision points $R_{i_1} = R_{i_2}$ among a lot of *random walks* $R_i = [a_i]P + [b_i]Q$ with random scalars a_i and b_i. If any efficient automorphisms such as $[u]P = \psi(P)$ exist, not only collision points themselves but also their conjugates with respect to efficient automorphism is useful. In order to activate the automorphism attack with rho method, it is needed to deside some coset leader from 12 conjugate rational points. It is known that normal basis representations of x, y coordinates of rational points efficiently work over $\mathbb{G}_2$. This paper show an approach with sextic twist, normal basis conversion, and optimal extension field [6].

2 Fundamentals

Let us briefly review elliptic curve discrete logarithm problem, rho method [5], non symmetric pairing groups on BN curve [1], and automorphism attach for $\mathbb{G}_2$ on BN curve.

2.1 Elliptic curve discrete logarithm problem (ECDLP)

Let $\mathbb{F}_p$ be a prime field and E be an *ordinary* elliptic curve over $\mathbb{F}_p$. $E(\mathbb{F}_p)$ that denotes the set of rational points on the curve, including the *infinity point* $\mathcal{O}$, forms an additive Abelian group. In general, the defining equation of the curve is written in the form of

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

In what follows, let the order denoted by $\#E(\mathbb{F}_p)$ be a prime number r to make the discussion simple. Usually, $\#E(\mathbb{F}_p)$ is written as

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

where t is the Frobenius trace of $E(\mathbb{F}_p)$. Then, let P and s be a certain rational point in $E(\mathbb{F}_p)$ and positive integer less than $\#E(\mathbb{F}_p)$, respectively. The rational point $Q = [s]P$ is easily obtained by a scalar multiplication. However, its inverse problem that solves the scalar s only with the x and y coordinates of the rational points P and Q is difficult when the order is enough large. This problem is called *elliptic curve discrete logarithm problem* (ECDLP).

The cryptographies based on ECDLPs requires that the order $\#E(\mathbb{F}_p)$ is sufficient large such as more than 160–bit number. Let r be the group order, the probability of success of collision–based attacks such as the well–known Pollard's rho method [5], for example, is roughly given by $1/\sqrt{r}$.

2.2 Pollard's rho method

Let x_P and y_P be the x and y coordinates of rational point $P \in E(\mathbb{F}_p)$. In what follows, it is often denoted by $P(x_P, y_P)$ or $P = (x_P, y_P)$.

In order to solve ECDLPs, rho method with *random walks* is well–known. In brief, suppose that a rational point Q is given by $[s]P$ with a certain scalar s and a rational point $P \in E(\mathbb{F}_p)$. Iteratively calculating the following random walks with random numbers a_i and b_i less than r,

$$R_i = [a_i]P + [b_i]Q, \qquad (3)$$

for a certain pair of integers u and w, one may find the following collision points.

$$R_u = R_w, \text{ in detail, } x_{R_u} = x_{R_w} \text{ and } \ y_{R_u} = y_{R_w}. \qquad (4a)$$

Simply, listing and sorting the coordinates (x_{R_i}, y_{R_i}) and random scalars (a_i, b_i) of the random walks R_i, the collision points R_u and R_w will be found by noting that their x and y coordinates becomes the same. Then, the scalar s is successfully obtained by

$$s = -(a_u - a_w)(b_u - b_w)^{-1} \bmod r. \qquad (4b)$$

According to [5], the number of iterations such that the collision points are 90% successfully found becomes about $2.15\sqrt{r}$.

In general, the next random point R_{i+1} based on R_i is given by some simple operations such as just an elliptic curve addition. For example, pre–compute several random points W_j, then R_{i+1} is given by R_i plus a certain one of the pre–computed random points. For activating rho method, the one needs to be uniquely determined from some information of R_i,

2.3 Non–symmetric pairing groups on BN curve

According to Barreto et al. [1], BN curve that is one of the most efficient pairing– friendly curves is given in the form of

$$E : y^2 = x^3 + b,\ b \in \mathbb{F}_p, \tag{5}$$

where the setting parameters p (characteristic) and r (group order) are systematically given with an integer variable χ as

$$\begin{aligned} p &= 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1, & \text{(6a)} \\ r &= 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1. & \text{(6b)} \end{aligned}$$

Since the embedding degree of BN curve is 12, consider $E(\mathbb{F}_{p^{12}})$ and its *non–symmetric* pairings such as Ate pairing use the two rational point groups $\mathbb{G}_1$ and $\mathbb{G}_2$ as

$$\begin{aligned} \mathbb{G}_1 &= E(\mathbb{F}_{p^{12}})[r] \cap \mathrm{Ker}(\phi - [1]), & \text{(7a)} \\ \mathbb{G}_2 &= E(\mathbb{F}_{p^{12}})[r] \cap \mathrm{Ker}(\phi - [p]), & \text{(7b)} \end{aligned}$$

where ϕ is Frobenius endomorphism, ı.e.,

$$\phi : E \to E : (x, y) \mapsto (x^p, y^p). \tag{8}$$

According to [7], the coordinates x_P and y_P of every rational point in $\mathbb{G}_2$ are elements in $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^4}$, respectively. In addition, $\mathbb{G}_2$ has its isomorphic group $\mathbb{G}_2'$ that is a subgroup of a certain *sextic* twisted *subfield* curve $E'(\mathbb{F}_{p^2})$. Costello et al. [8] have efficiently used $\mathbb{G}_2'$ for accelerating pairing–related calculations.

2.4 Automorphism attack for $\mathbb{G}_2$ on BN curve

This paper focuses on the isomorphic groups $\mathbb{G}_2$ and $\mathbb{G}_2'$. First, Eq.(7b) means that a rational point $P \in \mathbb{G}_2$ satisfies

$$[p]P = \phi(P). \tag{9}$$

Since the embedding degree is 12, the scalar multiplication $[p]$ and Frobenius endomorphism ϕ have period 12 such as $[p^{12}]P = \phi^{12}(P) = P$. For $P \in \mathbb{G}_2$, there are 12 variants as

$$[p^l]P = \phi^l(P) = (x_P^{p^l}, y_P^{p^l}),\ l = 0, 1, \cdots, 11. \tag{10}$$

In this paper, they are called *conjugate* rational points. Since $p^{12} \equiv 1 \pmod r$, let $\lambda_{12} = p$ be a primitive 12–th root of unity modulo r.

Then, briefly suppose that a rational point Q is given by $[s]P$ with a certain scalar s and a rational point $P \in \mathbb{G}_2$. Iteratively calculate the following random walks with random numbers a_i and b_i less than r,

$$R_i = [a_i]P + [b_i]Q. \tag{11}$$

Then, for a certain pair of integers u and w, one may find the following collision points R_u and R_w such that one of the following 12 equations based on the automorphism ϕ hold.

$$\begin{aligned} R_u = \left[\lambda_{12}^l\right] R_w = \phi^l(R_w), \quad & \text{(12a)} \\ l = 0, 1, 2, \cdots, 11. \end{aligned}$$

For example, suppose that $R_u = [\lambda_{12}]R_w$ is satisfied. Then, the scalar s is successfully obtained by

$$s = -(a_u - \lambda_{12} a_w)(b_u - \lambda_{12} b_w)^{-1} \bmod r. \tag{12b}$$

Thus, the 12 *conjugate rational points* contribute to reduce the computational cost for the attack about $1/\sqrt{12}$ [2].

In order to activate the automorphism attack with rho method, a coset leader of the automorphism class $\phi^l(R_w),\ l = 0, 1, 2, \cdots, 11$ needs to be uniquely determined with out any complicated arithmetic operations. For this purpose, it is known that normal basis representations of the x, y coordinates of rational points efficiently work according to Eq.(10) [9]. For example, let the x coordinate of rational point be represented with a certain normal bases as follows,

$$\begin{aligned} (x_0, x_1, x_2, \cdots, x_{11}), \quad & \text{(13)} \\ x_i \in \mathbb{F}_p,\ i = 0, 1, 2, \cdots, 11. \end{aligned}$$

Then, its conjugates with respect to $\mathbb{F}_p$ are simply given by the cyclic shifts of vector coefficients of x. Thus, a certain coset leader for the next random walk will be uniquely determined, for example, by $\max\{x_i\}$ as flagging. It is important that the determination needs no arithmetic operations. Then, the next random point will be efficiently determined.

3 Automorphism attack for $\mathbb{G}'_2$ on BN curve

In the preceding sections, it is introduced that Frobenius map ϕ and normal basis are efficiently work for collision–based attack together with rho method. However, for its isomorphic group $\mathbb{G}'_2$ on BN curve, they does not simply work because it is defined with *sextic* twist. In what follows, it is shown that optimal extension field (OEF) [6] efficiently activates these techniques.

3.1 Constructing $\mathbb{F}_{p^{12}}$ as an OEF

Especially in the case that 4 divides $(p-1)$, OEF extensively accelerates the arithmetic operations including isomorphic mapping between $\mathbb{G}_2$ and sextic twisted $\mathbb{G}'_2$ on BN curve. Most of cases satisfy the condition and thus in this case $(p-1)$ will be divisible by 12.

First, consider an quadratic and cubic non residue c in the prime field $\mathbb{F}_p$ such that

$$c^{(p-1)/3} \neq 1 \quad \text{and} \quad c^{(p-1)/2} \neq 1. \tag{14}$$

Then, $x^{12}-c$ becomes irreducible over $\mathbb{F}_p$. Let ω be its zero, $\mathbb{F}_{p^2}$, $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, and $\mathbb{F}_{p^{12}}$ are respectively constructed with the settings ass shown in **Table** 1. As an important property, for an arbitrary element $A = (a_0, a_1) = a_0 + a_1\alpha = a_0 + a_1\omega^6$ in $\mathbb{F}_{p^2}$, multiplying $\beta = \omega^3$ for example results in $\beta A = a_0\beta + a_1\beta^3 = a_0\omega^3 + a_1\omega^9 = (0, a_0, 0, a_1)$. It is easily found that it becomes an element in $\mathbb{F}_{p^4}$ and it does not need any arithmetic operations. In the same, multiplying $\gamma = \omega^2$ results in $\gamma A = (0, a_0, 0, 0, a_1, 0)$.

3.2 Sextic twisted curve E' and isomorphic map between $\mathbb{G}_2$ and $\mathbb{G}'_2$

Let the BN curve be $E : y^2 = x^3 + b$, the sextic twisted curve E' over $\mathbb{F}_{p^2}$ is given by

$$y^2 = x^3 + b\alpha \quad \text{or} \quad y^2 = x^3 + b\alpha^5. \tag{15}$$

In brief, suppose that the former curve is the *objective* twisted one. According to [7], $E'(\mathbb{F}_{p^2})$ has a subgroup of order r, that is denoted by $E'(\mathbb{F}_{p^2})[r]$. As previously introduced, it is just $\mathbb{G}'_2$. Since $\mathbb{G}_2$ and $\mathbb{G}'_2$ are isomorphic to each other, the following isomorphic map is given.

$$\begin{aligned} \varphi : \mathbb{G}'_2 &\rightarrow \mathbb{G}_2, & \text{(16a)} \\ (x, y) &\mapsto (\alpha^{1/3}x, \alpha^{1/2}y). & \text{(16b)} \end{aligned}$$

Based on $\alpha = \omega^6$, $\alpha^{1/3} = \omega^2$ and $\alpha^{1/2} = \omega^3$ respectively belong to $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^4}$. Thus, for every rational point $P(x_P, y_P) \in \mathbb{G}_2$, x_P and y_P respectively belong to $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^4}$.

3.3 A step for the automorphism attack for $\mathbb{G}'_2$

As introduced in **Sec**.2.4, the normal bases representation of coordinates of rational point will be desired. Since OEF of course adopts polynomial bases as shown in **Table** 1, they would like to be converted to some normal bases representations. In addition, the calculation cost for the bases conversion is preferred to be negligible.

According to [10], the following normal bases are available in $\mathbb{F}_{p^4}$, $\mathbb{F}_{p^6}$, and $\mathbb{F}_{p^{12}}$,

$$\{\theta_4, \theta_4^p, \cdots, \theta_4^{p^3}\},\ \theta_4 = \sum_{i=0}^{3} \beta^i, \tag{17a}$$

$$\{\theta_6, \theta_6^p, \cdots, \theta_6^{p^5}\},\ \theta_6 = \sum_{i=0}^{5} \gamma^i, \tag{17b}$$

$$\{\theta_{12}, \theta_{12}^p, \cdots, \theta_{12}^{p^{11}}\},\ \theta_{12} = \sum_{i=0}^{11} \omega^i. \tag{17c}$$

Then, the conversions Eqs.(18) respectively hold for $\mathbb{F}_{p^4}$ and $\mathbb{F}_{p^6}$, where μ and ϵ are primitive quartic and sextic roots of unity, respectively. Thus, the polynomial basis representations such as $(0, a_0, 0, a_1)$ and $(0, a_0, 0, 0, a_1, 0)$ in $\mathbb{F}_{p^4}$ and $\mathbb{F}_{p^6}$ are converted to their normal basis representations as Eqs.(19). Therefore, the basis conversion just needs to calculate $\mu a_0, \mu a_1, \epsilon a_0$ and ϵa_1.

Then, based on the normal basis representations, the coset leaders will be efficiently determined. In addition, the hash lists for searching collisions will be also prepared as previously introduced. As an optional technique, norms for coordinates are also available for no false collisions [11].

	modular polynomial	basis for vector representation	
$\mathbb{F}_{p^2}$	$x^2 - c$	$\{1, \omega^6\}$	$\{1, \alpha\},\ \alpha = \omega^6$
$\mathbb{F}_{p^4}$	$x^4 - c$	$\{1, \omega^3, \omega^6, \omega^9\}$	$\{1, \beta, \beta^2, \beta^3\},\ \beta = \omega^3$
$\mathbb{F}_{p^6}$	$x^6 - c$	$\{1, \omega^2, \omega^4, \omega^6, \omega^8, \omega^{10}\}$	$\{1, \gamma, \gamma^2, \gamma^3, \gamma^4, \gamma^5\},\ \gamma = \omega^2$
$\mathbb{F}_{p^{12}}$	$x^{12} - c$	$\{1, \omega, \omega^2, \omega^3, \omega^4, \cdots, \omega^{11}\}$	

Table 1: modular polynomial and basis for each field construction

$$\begin{bmatrix} \theta_4 \\ \theta_4^p \\ \theta_4^{p^2} \\ \theta_4^{p^3} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \mu & -1 & -\mu \\ 1 & -1 & 1 & -1 \\ 1 & -\mu & -1 & \mu \end{bmatrix} \begin{bmatrix} 1 \\ \beta \\ \beta^2 \\ \beta^3 \end{bmatrix}, \tag{18a}$$

$$\begin{bmatrix} \theta_6 \\ \theta_6^p \\ \theta_6^{p^2} \\ \theta_6^{p^3} \\ \theta_6^{p^4} \\ \theta_6^{p^5} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \epsilon & -(\epsilon+1) & -1 & -\epsilon & \epsilon+1 \\ 1 & -(\epsilon+1) & -\epsilon & 1 & -(\epsilon+1) & -\epsilon \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -\epsilon & -(\epsilon+1) & 1 & -\epsilon & -(\epsilon+1) \\ 1 & \epsilon+1 & -\epsilon & -1 & -(\epsilon+1) & \epsilon \end{bmatrix} \begin{bmatrix} 1 \\ \gamma \\ \gamma^2 \\ \gamma^3 \\ \gamma^4 \\ \gamma^5 \end{bmatrix}. \tag{18b}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & \mu & -1 & -\mu \\ 1 & -1 & 1 & -1 \\ 1 & -\mu & -1 & \mu \end{bmatrix} \begin{bmatrix} 0 \\ a_0 \\ 0 \\ a_1 \end{bmatrix} = \begin{bmatrix} a_0 + a_1 \\ \mu a_0 - \mu a_1 \\ -a_0 - a_1 \\ -\mu a_0 + \mu a_1 \end{bmatrix}, \tag{19a}$$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \epsilon & -(\epsilon+1) & -1 & -\epsilon & \epsilon+1 \\ 1 & -(\epsilon+1) & -\epsilon & 1 & -(\epsilon+1) & -\epsilon \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -\epsilon & -(\epsilon+1) & 1 & -\epsilon & -(\epsilon+1) \\ 1 & \epsilon+1 & -\epsilon & -1 & -(\epsilon+1) & \epsilon \end{bmatrix} \begin{bmatrix} 0 \\ a_0 \\ 0 \\ 0 \\ a_1 \\ 0 \end{bmatrix} = \begin{bmatrix} a_0 + a_1 \\ \epsilon a_0 - \epsilon a_1 \\ -\epsilon a_0 - \epsilon a_1 - a_0 - a_1 \\ -a_0 + a_1 \\ -\epsilon a_0 - \epsilon a_1 \\ \epsilon a_0 - \epsilon a_1 + a_0 - a_1 \end{bmatrix}. \tag{19b}$$

4 Conclusion

This paper has shown an automorphism improvement for the collision based attack on $\mathbb{G}'_2$ with BN curve. Since Frobenius map for rational points is available on $\mathbb{G}_2$, this paper has shown an approach with sextic twist, normal basis conversion, and optimal extension field. The approach can be directly applied on $\mathbb{G}'_2$.

References

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

[2] H. Cohen and G. Frey, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, *Discrete Mathematics and Its Applications*, Chapman & Hall CRC, 2005.

[3] 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.

[4] M. Akane, Y. Nogami, and Y. Morikawa, "Fast Ate Pairing Computation of Embedding Degree 12 Using Subfield–Twisted Elliptic Curve," IEICE Trans, vol. E92–A, no. 2, pp. 508–516, Feb. 2009.

[5] J. M. Pollard, "Monte Carlo methods for index computation (mod p)," Math. Comp., 32(143), pp. 918–924, 1978.

[6] D. Bailey and C. Paar, "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms," *Crypto' 98*, LNCS 1462, Springer–Verlag,, pp. 637–650, 1998.

[7] Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa, "Integer Variable χ–based Ate Pairing," *Pairing2008*, LNCS 5209, Springer–Verlag, pp. 178–191, 2008.

[8] C. Costello, T. Lange, and M. Naehrig, "Faster Pairing Computations on Curves with High-Degree Twists," *PKC2010*, LNCS 6056, Springer–Verlag, pp. 224–242, 2010.

[9] R. Gallant, R. Lambert, S. Vanstone, "Improving the Parallelized Pollard Lambda Search on Binary Anomalous Curves" *Mathematics of Computation*, vol. 69 Issue 232, 2000.

[10] Y. Nogami, Y. Morikawa, "A Method to Construct a Normal Basis over OEF," 23th Symposium on Information Theory and its Applications(SITA2000), vol.1 of 2, pp. 113–116, 2000.

[11] H. Kato, S. Takeuchi, Y. Nogami, Y. Morikawa T. Matsushima, "A Consideration of the Efficient Discrete Logarithm Computation by Using Norm on Barreto-Naehrig Curve Defined over an Extension Field" Computer Security Symposium 2010(CSS2010) vol. 2, pp. 471–476, 2010.