Integer Variable χ–Based Ate Pairing

Yasuyuki Nogami[1], Masataka Akane[2], Yumi Sakemi[1], Hidehiro Kato[1],
and Yoshitaka Morikawa[1]

[1] Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushima-naka, Okayama, Okayama 700-8530, Japan
[2] Mitsubishi Electric Corporation, Inazawa Works,
1, Hishimachi, Inazawashi, Aichi, 492-8161, Japan
{nogami,sakemi,kato,morikawa}@trans.cne.okayama-u.ac.jp

Abstract. In implementing an efficient pairing calculation, it is said that the lower bound of the number of iterations of Miller's algorithm is $\log_2 r/\varphi(k)$, where $\varphi(\cdot)$ is the Euler's function. Ate pairing reduced the number of the loops of Miller's algorithm of Tate pairing from $\lfloor \log_2 r \rfloor$ to $\lfloor \log_2(t-1) \rfloor$. Recently, it is known to systematically prepare a pairing–friendly elliptic curve whose parameters are given by a polynomial of integer variable "χ". For the curve, this paper gives *integer variable* χ*–based* Ate pairing that achieves the lower bound by reducing it to $\lfloor \log_2 \chi \rfloor$.

Keywords: Ate pairing, Miller's algorithm.

1 Introduction

Recently, pairing–based cryptographic applications such as ID–based cryptography [4] and group signature authentication [16] have received much attentions. In order to make these applications practical, pairing calculation needs to be efficiently carried out. For this purpose, several efficient pairings such as Tate, Ate [5], twisted Ate [15], and *subfield–twisted* Ate [6],[1] have been proposed. In this paper, Barreto–Naehrig (BN) curve, that is a typical class of non–supersingular (ordinary) pairing–friendly elliptic curves of embedding degree 12, is mainly dealt with. As a typical feature of BN curve, its characteristic p and Frobenius trace t are given by using *integer variable* χ as

$$p(\chi) = 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1, \tag{1a}$$

$$t(\chi) = 6\chi^2 + 1. \tag{1b}$$

Pairings can be roughly classified by the inputs for Miller's algorithm [10]. In general, as the inputs, Miller's algorithm needs two rational points and the number of iterations. Let us suppose a prime order BN curve of embedding degree 12 as $E : y^2 = x^3 + b,\ b \in \mathbb{F}_p$, where p is the characteristic and let

S.D. Galbraith and K.G. Paterson (Eds.): Pairing 2008, LNCS 5209, pp. 178–191, 2008.

the order be a prime number r. Since the embedding degree is 12, r divides $p^{12}-1$ and then r^2 divides $\#E(\mathbb{F}_{p^{12}})$. Tate pairing $\tau(\cdot,\cdot)$ uses rational points $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^{12}})/rE(\mathbb{F}_{p^{12}})$, the number of iterations of Miller's algorithm is $\lfloor \log_2 r \rfloor$. Tate pairing mainly uses P for calculation. The output of Miller's algorithm is denoted by $f_{r,P}(Q)$. Ate pairing $\alpha(\cdot,\cdot)$ uses rational points $P \in E(\mathbb{F}_p)$ and $Q \in E[r] \cap \mathrm{Ker}(\phi - [p])$, but the number of iterations is $\lfloor \log_2(t-1) \rfloor$, where ϕ is Frobenius map for rational point, $E[r]$ is the subgroup of rational points of order r in $E(\mathbb{F}_{p^{12}})$, and t is the Frobenius trace of $E(\mathbb{F}_p)$, that is $\#E(\mathbb{F}_p) = r = p+1-t$. The number of iterations is about half of that of Tate pairing; however, Ate pairing mainly uses Q for calculation. The output of Miller's algorithm is denoted by $f_{t-1,Q}(P)$ and thus plain Ate pairing is slower than Tate pairing.

Devegili et al.'s work [6] accelerated Ate pairing by using *subfield–twisted* BN curve $E'(\mathbb{F}_{p^2})$, where the twisted BN curve is given by $E' : y^2 = x^3 + bv^{-1}$ and v is a quadratic non residue and cubic non residue in $\mathbb{F}_{p^2}$. In detail, in addition to $P \in E(\mathbb{F}_p)$, it mainly uses $Q' \in E'(\mathbb{F}_{p^2})$ for calculation. The authors have also improved Ate pairing so as to substantially use subfield arithmetic operations [1]. In what follows, it is called *improved subfield–twisted* Ate (improved St–Ate) pairing. Both of these works [6],[1] have $\lfloor \log_2(t-1) \rfloor$ iterations in Miller's algorithm. According to [2], integer variable χ of small Hamming weight is efficient for Ate pairing with BN curve.

Let k be the embedding degree, it is said that the lower bound of the number of iterations of Miller's algorithm is $\log_2 r/\varphi(k)$, where $\varphi(\cdot)$ is the Euler's function. Ate pairing reduced the number of the iterations of Miller's algorithm from $\lfloor \log_2 r \rfloor$ to $\lfloor \log_2(t-1) \rfloor$. By reducing it to $\lfloor \log_2 \chi \rfloor$, this paper gives a bilinear map that achieves the lower bound. In detail, using Frobenius map and BN curve whose embedding degree is 12, this paper proposes *integer variable χ–based* Ate (Xate) pairing. First, based on Eqs.(1), the following relation is shown.

$$6\chi \equiv 1 + p + p^3 + p^{10} \pmod{r}. \tag{2}$$

Though plain Ate pairing calculates $f_{t-1,Q}(P)$ by using Miller's algorithm, where $P \in E(\mathbb{F}_p)$ and $Q \in E[r] \cap \mathrm{Ker}(\phi - [p])$, based on Eq.(2), the proposed Xate pairing calculates $f_{\chi,Q}(P)$. Noting that $\lfloor \log_2 \chi \rfloor$ is about half of $\lfloor \log_2(t-1) \rfloor$, Miller's part of Xate pairing is about twice more efficient than that of plain Ate pairing. The idea of [6] or improved St–Ate pairing [1] can be efficiently applied for Xate pairing. The authors simulated Xate pairing and also improved St–Xate pairing on Pentium4 (3.0GHz) with C language and GMP library [9]. Then, it is shown that, when r is a 254–bit prime number, improved St–Xate pairing that includes so–called *final exponentiation* is calculated within 11.0 milli–seconds. After that, it is shown that improved St–Xate is applied not only for BN curve but also Freeman's curve of embedding degree 10. Then, some recent works [19],[14] are introduced and compared to Xate pairing. Note that Eq.(2) is also efficient for scalar multiplications in $E(\mathbb{F}_{p^{12}})$ and *subfield–twisted* BN curve $E'(\mathbb{F}_{p^2})$, moreover exponentiation in $\mathbb{F}_{p^{12}}$.

Throughout this paper, p and k denote characteristic and extension degree, respectively. $\mathbb{F}_{p^k}$ denotes k-th extension field over $\mathbb{F}_p$ and $\mathbb{F}^*_{p^k}$ denotes the multiplicative group in $\mathbb{F}_{p^k}$. $X \mid Y$ and $X \nmid Y$ mean that X divides and does not divide Y, respectively.

2 Fundamentals

We briefly go over elliptic curve, Tate, Ate, improved St–Ate pairings, and divisor theorem. For instance, we mainly consider Barreto–Naehrig (BN) curve of embedding degree 12, that is a class of *ordinary pairing–friendly curves* [7].

2.1 Elliptic Curve and Barreto–Naehrig Curve

Let $\mathbb{F}_p$ be a prime field and E be an elliptic curve over $\mathbb{F}_p$. $E(\mathbb{F}_p)$ that is a set of rational points on the curve, including the *infinity point* $\mathcal{O}$, forms an additive Abelian group. Let $\#E(\mathbb{F}_p)$ be its order, consider a large prime r that divides $\#E(\mathbb{F}_p)$. The smallest positive integer k such that r divides $p^k - 1$ is especially called *embedding degree*. One can consider pairings such as Tate and Ate pairings by using $E(\mathbb{F}_{p^k})$. In general, $\#E(\mathbb{F}_p)$ is given as

$$\#E(\mathbb{F}_p) = p + 1 - t, \tag{3}$$

where t is the Frobenius trace of $E(\mathbb{F}_p)$. The characteristic p and Frobenius trace t of Barreto–Naehrig (BN) curve [3] are given by using an integer variable χ as Eqs.(1). In addition, the BN curve E is given by

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

whose embedding degree is 12. In this paper, let $\#E(\mathbb{F}_p)$ be a prime r.

2.2 Tate Pairing

Let $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$, Tate pairing $\tau(\cdot,\cdot)$ is defined as

$$\tau(\cdot,\cdot) : \begin{cases} E(\mathbb{F}_p) \times E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k}) & \to \mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r \\ (P, Q) & \mapsto f_{r,P}(Q)^{(p^k-1)/r}. \end{cases} \tag{5}$$

In general, $A = f_{r,P}(Q)$ is calculated by Miller's algorithm [5], then so–called *final exponentiation* $A^{(p^k-1)/r}$ follows. The number of iterations of Miller's algorithm for Tate pairing is determined by r, in detail $\lfloor \log_2 r \rfloor$. Twisted Ate pairing [15] reduced the number of iterations of Miller's algorithm. Let d be the twist degree such as $d = 2, 3, 4, 6$, it is reduced to $(t-1)^{k/d} \pmod{r}$.

2.3 Ate Pairing

Let ϕ be Frobenius endomorphism, i.e.,

$$\phi : E \to E : (x, y) \mapsto (x^p, y^p), \tag{6}$$

where x and y are x–coordinate and y–coordinate of rational point, respectively. Then, let $\mathbb{G}_1$ and $\mathbb{G}_2$ be

$$\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\phi - [1]), \tag{7a}$$

$$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\phi - [p]), \tag{7b}$$

and let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, Ate pairing $\alpha(\cdot, \cdot)$ is defined as

$$\alpha(\cdot,\cdot) : \begin{cases} \mathbb{G}_2 \times \mathbb{G}_1 & \to \mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r \\ (Q, P) & \mapsto f_{T,Q}(P)^{(p^k-1)/r}, \end{cases} \tag{8}$$

where $T = t-1$, $E[r]$ denotes a subgroup of rational points of order r in $E(\mathbb{F}_{p^k})$, and $[i]$ denotes $[i] : P \mapsto iP$. The number of iterations of Miller's algorithm for Ate pairing is determined by $t - 1$, in detail $\lfloor \log_2(t - 1) \rfloor$.

In the case of using BN curve for Ate pairing, $\mathbb{G}_1$ and $\mathbb{G}_2$ become as

$$\mathbb{G}_1 = E(\mathbb{F}_p), \tag{9a}$$

$$\mathbb{G}_2 = (\phi - [1]) \left\{ E(\mathbb{F}_{p^{12}})/rE(\mathbb{F}_{p^{12}}) \right\}, \tag{9b}$$

therefore, compared to Tate paring, the number of iterations becomes about half; however, Miller's algorithm needs a lot of calculations in the above defined $\mathbb{G}_2$. Thus, plain Ate pairing is not superior to Tate pairing.

Devegili et al.'s work [6] and the authors [1],[2] have improved Ate pairing with BN curve by using subfield–twisted elliptic curve $E'(\mathbb{F}_{p^2})$ over $\mathbb{F}_{p^2}$. It is given as

$$E' : y^2 = x^3 + bv^{-1},\ b \in \mathbb{F}_p,\ v \in \mathbb{F}_{p^2}, \tag{10}$$

where v is a quadratic non residue and cubic non residue in $\mathbb{F}_{p^2}$. It is also called *sextic twisted* curve. In this case, we have the following isomorphism.

$$\psi : E'(\mathbb{F}_{p^2}) \ \to E(\mathbb{F}_{p^{12}}) \tag{11a}$$

$$Q'(x_{Q'}, y_{Q'}) \ \mapsto Q(x_{Q'} v^{\frac{1}{3}}, y_{Q'} v^{\frac{1}{2}}), \tag{11b}$$

Thus, noting that $E(\mathbb{F}_{p^{12}})$ and $E'(\mathbb{F}_{p^{12}})$ are isomorphic to each other, [6] efficiently used *subfield–twisted elliptic curve* $E'(\mathbb{F}_{p^2})$. In detail, it calculates $f_{T,\psi(Q')}$ (P) by using Q'. The authors have also improved Ate pairing so as to substantially use subfield arithmetic operations [1]. In what follows, it is called improved St–Ate pairing. In our previous work [2], it is shown that integer variable χ of small Hamming weight is quite efficient for Ate pairing. It is also efficient for twisted Ate pairing [18].

2.4 Relation between Tate and Ate Pairings

Table 1 shows the parameter settings for Miller's algorithm using BN curve of embedding degree 12.

Table 1. Parameter settings for calculating $f_{A,B}(C)$ with Miller's algorithm

pairing	A	group for B	group for C
plain Tate	r	$E(\mathbb{F}_p)$	$E(\mathbb{F}_{p^{12}})$
Twisted Ate [15]	$(t-1)^2 \pmod r$	$E(\mathbb{F}_p)$	$E(\mathbb{F}_{p^{12}})$
plain Ate	$t-1$	$E(\mathbb{F}_{p^{12}})$	$E(\mathbb{F}_p)$
Devegili et al.'s Ate [6]	$t-1$	$E'(\mathbb{F}_{p^2})$	$E(\mathbb{F}_p)$
improved St–Ate [2]	$t-1$	$E'(\mathbb{F}_{p^2})$	$E(\mathbb{F}_p)$

Between Tate and Ate pairings, we have the following relation [10].

$$\tau(Q,P)^L = f_{T,Q}(P)^{c(p^k-1)/N}, \tag{12}$$

where $c \equiv kp^{k-1} \pmod r$ and

$$N = \gcd(T^k-1, p^k-1),\ T^k-1 = LN,\ T = t-1. \tag{13}$$

Thus, let $N = ru$, according to Eq.(8), we have

$$\tau(Q,P)^{uL} = \alpha(Q,P)^c. \tag{14}$$

$r \nmid L$ is needed for Ate pairing to be nondegenerate.

2.5 Divisor

Let D be the principal divisor of $Q \in E$ given as

$$D = (Q) - (\mathcal{O}) = (Q) - (\mathcal{O}) + div\,(1)\,. \tag{15}$$

For scalars $a, b \in Z$, let aD and bD be written as

$$aD = (aQ) - (\mathcal{O}) + div\,(f_{a,Q})\,, \tag{16a}$$

$$bD = (bQ) - (\mathcal{O}) + div\,(f_{b,Q})\,, \tag{16b}$$

where $f_{a,Q}$ and $f_{b,Q}$ are the rational functions for aD and bD, respectively. Then, addition for divisors is carried out as

$$aD + bD = (aQ) + (bQ) - 2(\mathcal{O}) + div\,(f_{a,Q} \cdot f_{b,Q} \cdot g_{aQ,bQ})\,, \tag{17a}$$

where $g_{aQ,bQ} = l_{aQ,bQ}/v_{aQ+bQ}$, $l_{aQ,bQ}$ denotes the line passing through two points aQ, bQ, and v_{aQ+bQ} denotes the vertical line passing through $aQ + bQ$. Moreover, the following relation holds.

$$a(bD) = \sum_{i=0}^{a-1}(bQ) - a(\mathcal{O}) + div\left(f_{b,Q}^{a} \cdot f_{a,bQ}\right). \tag{17b}$$

Thus, let $(a + b)D$ and $(ab)D$ be written as

$$(a + b)D = ((a + b)Q) - (\mathcal{O}) + div\left(f_{a+b,Q}\right), \tag{18a}$$

$$(ab)D = (abQ) - (\mathcal{O}) + div\left(f_{ab,Q}\right), \tag{18b}$$

we have the following relation.

$$f_{a+b,Q} = f_{a,Q} \cdot f_{b,Q} \cdot g_{aQ,bQ}, \tag{19a}$$

$$f_{ab,Q} = f_{b,Q}^{a} \cdot f_{a,bQ} = f_{a,Q}^{b} \cdot f_{b,aQ}. \tag{19b}$$

Consider Frobenius map $\phi(Q)$ for rational point $Q \in E(\mathbb{F}_{p^k})$ as

$$\phi(\cdot) : \begin{cases} E(\mathbb{F}_{p^k}) \to E(\mathbb{F}_{p^k}) \\ (x_Q, y_Q) \mapsto (x_Q^p, y_Q^p). \end{cases} \tag{20}$$

In the case of Ate pairing, according to Eq.(7b) we have

$$\phi(Q) = pQ, \text{ where } Q \in \mathbb{G}_2. \tag{21}$$

Thus, for $Q \in \mathbb{G}_2$, let $f_{p,Q}$ be given as

$$pD = (pQ) - \mathcal{O} + div\left(f_{p,Q}\right), \tag{22}$$

Eq.(19b) with $b = p$ leads to

$$f_{ap,Q} = f_{p,Q}^{a} f_{a,pQ} = f_{p,Q}^{a} f_{a,\phi(Q)} = f_{p,Q}^{a} f_{a,Q}^{p}. \tag{23}$$

Iteratively applying the above relation from $a = p^{i-1}$, we have

$$f_{p^i,Q} = f_{p,Q}^{ip^{i-1}}. \tag{24}$$

3 Main Proposal

In this section, using BN curve of embedding degree 12, *integer variable χ–based* Ate pairing (Xate pairing) is proposed. First, derive $\sum_j d_j\chi^i = \sum_i c_i p^i$ with small coefficients c_j and d_j. Based on the p–adic expansion, then consider efficient bilinear map with Frobenius map, namely Xate pairing.

3.1 Frobenius Expansion with χ

Note that $\mathbb{G}_2$ is defined as $E[r] \cap \mathrm{Ker}(\phi - [p])$, the parameter settings of BN curve are Eq.(1), and $\#E(\mathbb{F}_p)$ is a prime number r. First, this section considers p–adic (Frobenius) expansion with respect to χ. In the case of BN curve, the expansion of 6χ is systematically obtained. According to Eq.(1b) and Eq.(3),

$$6\chi^2 \equiv t - 1 \equiv p \pmod{r}. \tag{25}$$

Then, substituting it to Eq.(1a), we have

$$p \equiv p^2 - 6\chi(p+1) + 4p + 1 \pmod{r}, \tag{26}$$

$$6\chi(1+p) \equiv (p^2 + 3p + 1) \pmod{r}. \tag{27}$$

Then, based on cyclotomic polynomial $p^4 - p^2 + 1 \equiv 0 \pmod{r}$ [1] and using extended Euclidean algorithm, $(1+p)^{-1}$ is calculated as

$$p^2(1-p)(1+p) \equiv 1 \pmod{r}, \tag{28}$$

$$(1+p)^{-1} \equiv p^2(1-p) \pmod{r}. \tag{29}$$

Then, substituting Eq.(29) and $p^6 \equiv -1 \pmod{r}$ to Eq.(27), we have

$$\begin{aligned} 6\chi &\equiv (1+p)^{-1}\left\{(1+p)^2 + p\right\} \\ &\equiv 1 + p + p^3 + p^{10} \pmod{r}. \end{aligned} \tag{30}$$

As introduced in **Sec**.3.4, for other pairing–friendly curves, such a p–adic (Frobenius) expansion can be obtained in the same way. In the next section, based on the above relation Eq.(30), we consider an efficient bilinear map that achieves the number of calculations of Miller's algorithm $\log_2 r/\varphi(k)$ with BN curve.

3.2 Integer Variable χ–Based Ate (Xate) Pairing

First, for $Q \in \mathbb{G}_2$, we consider the following relation.

$$f_{6\chi^2,Q} = f_{T,Q}. \tag{31}$$

Of course, for $\forall P \in \mathbb{G}_1$, we have

$$f_{6\chi^2,Q}(P)^{(p^{12}-1)/r} = f_{T,Q}(P)^{(p^{12}-1)/r} = \alpha(Q,P). \tag{32}$$

In order to apply Eq.(30), according to **Sec**.2.5, we rewrite $f_{6\chi^2,Q}$ as

$$f_{6\chi^2,Q}^{(p^{12}-1)/r} = f_{6\chi\cdot\chi,Q}^{(p^{12}-1)/r} = f_{(1+p+p^3+p^{10})\chi,Q}^{(p^{12}-1)/r}. \tag{33}$$

from which we can obtain

$$f_{(1+p+p^3+p^{10})\chi,Q}^{(p^{12}-1)/r} = \{f_{\chi,Q} \cdot f_{\chi,Q}^{p} \cdot g_{\chi Q,p\chi Q} \cdot f_{\chi,Q}^{p^3} \cdot f_{\chi,Q}^{p^{10}} \cdot g_{p^3\chi Q,p^{10}\chi Q} \\ \cdot g_{\chi Q+p\chi Q,p^3\chi Q+p^{10}\chi Q} \cdot f_{p,\chi Q}^{1+3p^2+10p^9}\}^{(p^{12}-1)/r}. \tag{34a}$$

Then, we have $f_{6\chi\cdot\chi,Q}^{(p^{12}-1)/r} = AB^{(p^{12}-1)/r}$ with

$$A = f_{p,\chi Q}^{1+3p^2+10p^9}, \tag{35a}$$

$$B = \hat{f}_{\chi,Q}, \tag{35b}$$

$$\text{where}\quad \hat{f}_{\chi,Q} = f_{\chi,Q}^{1+p+p^3+p^{10}} \cdot g_{\chi Q,p\chi Q} \cdot g_{p^3\chi Q,p^{10}\chi Q} \\ \cdot g_{\chi Q+p\chi Q,p^3\chi Q+p^{10}\chi Q}. \tag{35c}$$

As shown in **App**.A, $f_{p,\chi Q}^{(p^{12}-1)/r} = f_{p,Q}^{\chi(p^{12}-1)/r}$. Thus, Eq.(35a) becomes

$$A^{(p^{12}-1)/r} = \{f_{p,Q}^{(1+3p^2+10p^9)\chi}\}^{(p^{12}-1)/r}. \tag{36}$$

and then $A^{(p^{12}-1)/r}$ gives a bilinear map. According to Eq.(30), we can consider the right–hand side of Eq.(30) as a polynomial of variable p such as

$$h(p) = 1 + p + p^3 + p^{10}. \tag{37}$$

Then, A is given with its *formal derivative* $h'(p)$ with respect to p as

$$A^{(p^{12}-1)/r} = \{f_{p,Q}^{\chi h'(p)}\}^{(p^{12}-1)/r}. \tag{38}$$

Finally, using A, B, Eqs.(31), (33), and (53), we have

$$\hat{f}_{\chi,Q}^{(p^{12}-1)/r} = \left\{f_{T,Q} \cdot A^{-1}\right\}^{(p^{12}-1)/r}, \tag{39}$$

we find that the right–hand side of the above equation gives a bilinear map. In what follows, we consider the following bilinear map referring as *integer variable χ–based* Ate (Xate) pairing $\zeta(\cdot,\cdot)$.

$$\zeta(\cdot,\cdot) : \begin{cases} \mathbb{G}_2 \times \mathbb{G}_1 & \to \mathbb{F}_{p^{12}}^*/(\mathbb{F}_{p^{12}}^*)^r \\ (Q,P) & \mapsto \hat{f}_{\chi,Q}(P)^{(p^{12}-1)/r}. \end{cases} \tag{40}$$

According to Eq.(35c), we find that the major computation of Xate pairing is $f_{\chi,Q}$ that achieves the lower bound $\log_2 r/\varphi(k)$. The others are efficiently calculated with Frobenius map. When one uses Miller's algorithm, the Hamming weight of χ directly affects the efficiency of calculating $\hat{f}_{\chi,Q}(P)$. Moreover, one can apply improved St–Ate pairing technique [1] to Xate paring, namely improved *subfield–twisted* Xate (improved St–Xate) pairing.

3.3 Nondegeneracy of Xate Pairing

Based on the nondegeneracies of Tate and Ate pairings, the condition that Xate pairing needs to satisfy is given as follows.

Let $N = \gcd(T^k - 1, q^k - 1)$, $T^k - 1 = LN$, and $T = t - 1$, $r \nmid L$ is needed for the nondegeneracy of Ate pairing. In the same, according to Eqs.(14), (35a), (39), (52), and (53), the following condition is needed for that of Xate pairing.

$$r \nmid uL - \chi(uL + c)h'(p), \tag{41}$$

where $c \equiv 12p^{11} \pmod r$ and $N = ru$. (*see* **App**.B)

3.4 For Other Pairing–Friendly Curves

In the case of Freeman's curve [7] whose embedding degree k is 10, the parameter settings become as

$$p(\chi) = 25\chi^4 + 25\chi^3 + 25\chi^2 + 10\chi + 3, \tag{42a}$$

$$t(\chi) = 10\chi^2 + 5\chi + 3, \tag{42b}$$

in the same way of Eq.(30), we have

$$5\chi \equiv -2p^2 + p - 2 \pmod r. \tag{43}$$

In the case of embedding degree 8 and parameter settings as follows [7],

$$p(\chi) = \chi^8 + \chi^5 - \chi^4 - \chi + 1, \tag{44a}$$

$$t(\chi) = \chi^5 - \chi + 1, \tag{44b}$$

then we have

$$\chi^2 \equiv -\chi p^5 - p^2 \pmod r. \tag{45}$$

As shown in Eq.(30), Eq.(43), and Eq.(45), the highest degree term of χ can be replaced to the other lower terms with powers of p from which the efficiency of Xate pairing comes. Thus, Eq.(30), Eq.(43), and Eq.(45) are efficient not only for constructing bilinear maps such as Eq.(40) but also scalar multiplication in $\mathbb{G}_2$ and exponentiation in $\mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r$. Furthermore, the authors have found that Eq.(30) leads to more improvement of Twisted Ate pairing.

4 Simulation

This section discusses the implementation of Xate pairing and then shows simulation result. In the discussion, suppose the following conditions.

– BN curve of prime order r and Frobenius trace t is given over $\mathbb{F}_p$ as Eq.(4).
– Using a certain integer χ, p and t are given by Eqs.(1).

- Its quadratic and cubic twisted curve is given by Eq.(10).
- $\mathbb{G}_1 = E(\mathbb{F}_p)$, $\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\phi - [p])$, and $\mathbb{G}'_2 = \psi^{-1}(\mathbb{G}_2)$, where ψ is defined as Eqs.(11) and ψ^{-1} is its inverse map.
- $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, $Q' \in \mathbb{G}'_2$, and Eq.(41) is satisfied.
- In this case, $v_{aQ+bQ}(P)$ becomes 1 at *final exponentiation* (*see* **App**.A).

4.1 Implementation

As shown in Eq.(35c), the major calculation of Xate pairing is $f_{\chi,Q}(P)$. It is efficiently calculated by using Miller's algorithm. In the Miller's algorithm for calculating $f_{\chi,Q}(P)$, we obtain $\chi Q \in E'(\mathbb{F}_{p^2})$. Then, efficiently using χQ and Frobenius map, the other parts of Xate pairing are calculated. By the way, *final exponentiaion* for f given by Eq.(46) is calculated by Algorithm 1 [6].

$$f = \hat{f}_{\chi,Q}(P). \tag{46}$$

Algorithm 1. Final exponentiation $f^{(p^6-1)(p^2+1)(p^4-p^2+1)/r}$

```
 Input : $f$ given by Eq.(46), $\chi$, $p$
Output : $f^{(p^6-1)(p^2+1)(p^4-p^2+1)/r}$
Procedure :
    $f \leftarrow f^{p^6} \cdot f^{-1}$
    $f \leftarrow f^{p^2} \cdot f$
    $a \leftarrow (f^6)^{\chi} \cdot (f^5)^{p^6}$
    $b \leftarrow a^p$
    $b \leftarrow a \cdot b$
    compute $f^p, f^{p^2}$, and $f^{p^3}$
    $c \leftarrow b \cdot (f^p)^2 \cdot f^{p^2}$
    $f \leftarrow f^{p^3} \cdot (c^6)^{\chi^2} \cdot c \cdot b \cdot (f^p \cdot f)^9 \cdot a \cdot f^4$
    Return $f$
```

4.2 Simulation Result

Using the following positive integer χ of small Hamming weight,

$$\chi = 2^{62} + 2^{55} + 1, \tag{47}$$

by which the order r becomes 254–bit prime number and the size of $\mathbb{F}_{p^{12}}$ becomes 3048–bit, the authors simulated improved St–Xate pairing. For constructing $\mathbb{F}_{p^{12}}$, the authors used the previous work [12] and tower field technique as $\mathbb{F}_{(p^4)^3}$ [17]. The detail of the implementation is introduced in **App**.C.

According to Eq.(1b), $\log_2(t-1) \approx 2\log_2(\chi)$. Therefore, it is understood that Miller's part of improved St–Xate pairing is about twice faster than that of improved St–Xate pairing. The simulation result also shows it.

Table 2. Comparison of timings of pairings with BN curve of 254–bit prime order

[unit:ms]

pairing	Miller's part	final exponentiation	total
plain Tate	22.1	5.1	27.2
Twisted Ate [18]	13.9		19.0
plain Ate	26.5		31.6
improved St–Ate [2]	10.5		15.6
Xate	**13.6**		**18.7**
improved St–Xate	**5.4**		**10.5**
Devegili et al.'s Ate [6]	NA	NA	23.2

Remark : Pentium4 (3.0GHz), C language, and GMP [9] are used.
The authors did not use 64–bit mode of Pentium4.

4.3 Some Recent Works and Comparison

As the most recent works, Vercauteren [19] and Lee et al. [14] have proposed efficient Ate pairings. Vercauteren introduced *optimal pairings.* According to [19], the basic idea is finding $\lambda = mr,\ r \nmid m$ that has p–adic expansion $\lambda = \sum c_i p^i$ with small coefficients c_i. Then, *optimal pairing* uses $f_{c_i,Q}$ with Miller's algorithm calculation. Lee et al. introduced R–ate pairing [14]. Lee's basic idea is finding $T_x = \sum c_i p^i$ with small coefficients c_i, where $T_x = (t-1)^x$. In the same, R–ate pairing uses $f_{c_i,Q}$ with Miller's algorithm calculation.

As described in **Sec**.3, the proposed method derives $\sum_j d_j \chi^i = \sum_i c_i p^i$ with small coefficients c_j and d_j, thus our approach is different from theirs [19],[14]. For example, R–ate pairing for BN curve of embedding degree 12 calculates $f_{6\chi+2,Q}$ but Xate pairing calculates $f_{\chi,Q}$ from which the difference could be understood though their calculation costs are almost the same. As previously introduced, our proposal, that is characterized by Eq.(30), Eq.(43), and Eq.(45), are efficient not only for constructing Xate pairing such as Eq.(40) but also scalar multiplication in $\mathbb{G}_2$ and exponentiation in $\mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r$ to which the techniques [19] and [14] cannot be directly applied. For example, when one calculates $sQ,\ Q \in \mathbb{G}_2$ with Eq.(30), calculate the 6χ–adic representation of scalar s, then substitute 6χ by $1 + p + p^3 + p^{10}$. Then, using some Frobenius maps based on $pQ = \phi(Q)$, sQ can be efficiently calculated. *Skew Frobenius map* for $Q' \in \mathbb{G}'_2$ is also efficient as $pQ' = \psi^{-1}(\phi(\psi(Q')))$ with Eq.(11b). Efficient scalar multiplication using *skew Frobenius map* is shown in Galbraith et al.'s work [8]. Furthermore, the authors have found that Eq.(30) leads to more improvement of Twisted Ate pairing.

5 Conclusion

Using BN curve whose embedding degree is 12, this paper proposed *integer variable χ–based* Ate (Xate) pairing. First, the following relation was shown.

$$6\chi \equiv 1 + p + p^3 + p^{10} \pmod{r}, \tag{48}$$

where the characteristic p of BN curve was given with *integer variable* χ as

$$p(\chi) = 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1. \tag{49}$$

Let ϕ and t be Frobenius map and its trace, respectively, though plain Ate pairing calculates $f_{t-1,Q}(P)$ by using Miller's algorithm, the proposed Xate pairing calculates $f_{\chi,Q}(P)$ using χ, where $P \in E(\mathbb{F}_p)$ and $Q \in E[r] \cap \mathrm{Ker}(\phi - [p])$. Noting that $\lfloor \log_2 \chi \rfloor$ is about half of $\lfloor \log_2(t-1) \rfloor$, it was shown that Miller's part of Xate pairing was about twice more efficient than that of plain Ate pairing. Then, the authors simulated Xate pairing on Pentium4 (3.0GHz) with C language and GMP library [9], it was shown that, when r was a 254–bit prime number, improved St–Xate pairing that included so–called *final exponentiation* was calculated within 11.0 milli–seconds.

Acknowledgements

We thank Steven D. Galbraith for a lot of suggestions and comments.

References

1. Akane, M., Kato, H., Okimoto, T., Nogami, Y., Morikawa, Y.: An Improvement of Miller's Algorithm in Ate Pairing with Barreto–Naehrig Curve. In: Proc. of Computer Security Symposium 2007 (CSS 2007), pp. 489–494 (2007)
2. Akane, M., Kato, H., Okimoto, T., Nogami, Y., Morikawa, Y.: Efficient Parameters for Ate Pairing Computation with Barreto-Naehrig Curve. In: Proc. of Computer Security Symposium 2007 (CSS 2007), pp. 495–500 (2007)
3. Barreto, P.S.L.M., Naehrig, M.: Pairing–Friendly. Elliptic Curves of Prime Order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (2006)
4. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001)
5. Cohen, H., Frey, G.: Handbook of Elliptic and Hyperelliptic Curve Cryptography, Discrete Mathematics and Its Applications. Chapman & Hall CRC (2005)
6. Devegili, A.J., Scott, M., Dahab, R.: Implementing Cryptographic Pairings over Barreto-Naehrig Curves. In: Takagi, T., Okamoto, T., Okamoto, E., Okamoto, T. (eds.) Pairing 2007. LNCS, vol. 4575, pp. 197–207. Springer, Heidelberg (2007)
7. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves (preprint, 2006), `http://math.berkeley.edu/~dfreeman/papers/taxonomy.pdf`
8. Galbraith, S.D., Scott, M.: Exponentiation in pairing-friendly groups using homomorphisms. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS. Springer, Heidelberg (to appear, 2008)

9. GNU MP, http://gmplib.org/
10. Hess, F., Smart, N., Vercauteren, F.: The Eta Pairing Revisited. IEEE Trans. Information Theory, 4595–4602 (2006)
11. Itoh, T., Tsujii, S.: A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Bases. Inf. and Comp. 78, 171–177 (1988)
12. Kato, H., Nogami, Y., Yoshida, T., Morikawa, Y.: Cyclic Vector Multiplication Algorithm Based on a Special Class of Gauss Period Normal Basis. ETRI Journal 29(6), 769–778 (2007),http://etrij.etri.re.kr/Cyber/servlet/BrowseAbstract?paperid=RP0702-0040
13. Knuth, D.: The Art of Computer Programming. Seminumerical Algorithms, vol. 2. Addison-Wesley, Reading (1981)
14. Lee, E., Lee, H., Park, C.: Efficient and Generalized Pairing Computation on Abelien Varieties, IACR ePrint archive, http://eprint.iacr.org/2008/040
15. Matsuda, S., Kanayama, N., Hess, F., Okamoto, E.: Optimised Versions of the Ate and Twisted Ate Pairings. In: Galbraith, S.D. (ed.) Cryptography and Coding 2007. LNCS, vol. 4887, pp. 302–312. Springer, Heidelberg (2007)
16. Nakanishi, T., Funabiki, N.: Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 443–454. Springer, Heidelberg (2005)
17. Nogami, Y., Morikawa, Y.: A Fast Implementation of Elliptic Curve Cryptosystem with Prime Order Defined over F_{p^8}. Memoirs of the Faculty of Engineering Okayama University 37(2), 73–88 (2003)
18. Sakemi, Y., Kato, H., Akane, M., Okimoto, T., Nogami, Y., Morikawa, Y.: An Improvement of Twisted Ate Pairing Using Integer Variable with Small Hamming Weight. In: The 2008 Symposium on Cryptography and Information Security (SCIS 2008), January 22-25 (2008)
19. Vercauteren, F.: Optimal Pairings, IACR ePrint archive,
http://eprint.iacr.org/2008/096

A Bilinearity of $f_{p,Q}$

First, we have

$$f_{r,Q} = f_{p-T,Q} = f_{p,Q} \cdot g_{pQ,-TQ} \cdot f_{T,Q}^{-1} = f_{p,Q} \cdot v_{pQ} \cdot f_{T,Q}^{-1}, \tag{50}$$

where v_{pQ} denotes the vertical line that goes through $pQ = \phi(Q)$. Thus,

$$\begin{aligned}\left\{f_{p,Q}(P) \cdot v_{\phi(Q)}(P)\right\}^{(p^{12}-1)/r} &= f_{r,Q}(P)^{(p^{12}-1)/r} \cdot f_{T,Q}(P)^{(p^{12}-1)/r} \\ &= \tau(Q,P) \cdot \alpha(Q,P), \end{aligned} \tag{51}$$

According to Eq.(11b), the x–coordinate of $Q \in \mathbb{G}_2$ is given by $x_{Q'}v^{1/3}$, where $x_{Q'}$ and $v^{1/3}$ belong to $\mathbb{F}_{p^2}$ and $\mathbb{F}_{p^6}$, respectively. Therefore, $v_{\phi(Q)}(P)^{(p^{12}-1)/r}$ becomes 1. Because, the x–coordinate of P belongs to $\mathbb{F}_p$. Thus, we have

$$f_{p,Q}(P)^{(p^{12}-1)/r} = \tau(Q,P) \cdot \alpha(Q,P). \tag{52}$$

Therefore $f_{p,Q}(P)^{(p^{12}-1)/r}$ gives a bilinear map from which Eq.(35a) becomes

$$f_{p,\chi Q}^{(p^{12}-1)/r} = f_{p,Q}^{\chi(p^{12}-1)/r}. \tag{53}$$

The bilinearity of $f_{p,Q}$ has been also shown in [15].

B Proof of Eq.(41)

Eq.(14) means

$$f_{r,Q}^{uL(p^{12}-1)/r} = f_{T,Q}^{c(p^{12}-1)/r}. \tag{54}$$

From Eq.(52), we have

$$f_{r,Q}^{uL(p^{12}-1)/r} \cdot f_{T,Q}^{uL(p^{12}-1)/r} = f_{p,Q}^{uL(p^{12}-1)/r}. \tag{55}$$

Substituting Eq.(54) to Eq.(55), we have

$$f_{T,Q}^{(uL+c)(p^{12}-1)/r} = f_{p,Q}^{uL(p^{12}-1)/r}. \tag{56}$$

The $(uL+c)$–th power of the right–hand side of Eq.(39) becomes

$$\left\{f_{T,Q}^{uL+c} \cdot A^{-(uL+c)}\right\}^{(p^{12}-1)/r} = \left\{f_{p,Q}^{w}\right\}^{(p^{12}-1)/r}, \tag{57}$$

where using Eq.(56) w is given as

$$w = uL - \chi(uL+c)h'(p). \tag{58}$$

Thus, we obtain the condition as Eq.(41).

C Constructing $\mathbb{F}_{p^{12}}$ and Its Subfields $\mathbb{F}_{p^2}, \mathbb{F}_{p^4}, \mathbb{F}_{p^6}$

First, the authors prepared $\mathbb{F}_{p^4}$ with type–$\langle 1,4\rangle$ Gauss period normal basis (GNB) [5] and also $\mathbb{F}_{p^3}$ with type–$\langle 2,3\rangle$ GNB. Then, the authors prepared $\mathbb{F}_{p^{12}}$ as *tower field* $\mathbb{F}_{(p^4)^3}$ by towering $\langle 2,3\rangle$ GNB over $\mathbb{F}_{p^4}$ [17]. For multiplication with GNB, the authors implemented *cyclic vector multiplication algorithm* (CVMA) [12]. For example, CVMA calculates a multiplication in $\mathbb{F}_{(p^m)^n}$ by

$$M_{mn} = \frac{n(n+1)}{2}M_m = \frac{mn(m+1)(n+1)}{4}M_1. \tag{59}$$

For inversions in extension field and prime field, the authors implemented Itoh–Tsujii inversion algorithm [11] and *binary extended* Euclidean algorithm [13], respectively. Since GNB is a class of normal bases, one can easily prepare arithmetic operations in subfields $\mathbb{F}_{p^2}, \mathbb{F}_{p^4}, \mathbb{F}_{(p^2)^3}$.