20

Efficient Pairings on Twisted Elliptic Curve

Yasuyuki Nogami, Masataka Akane,
Yumi Sakemi and Yoshitaka Morikawa
Okayama University
Japan

1. Introduction

Recently, pairing-based cryptographic applications such as ID-based cryptography (D. Boneh et al. (2001)) and group signature authentication (T. Nakanishi & N. Funabiki (2005)) 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 (H. Cohen & G. Frey (2005)), Ate (F. Hess et al. (2006)), twisted Ate (S. Matsuda et al. (2007)), and *subfield–twisted* Ate (A. J. Devegili et al. (2007)), (M. Akane et al. (2007)) have been proposed. Consider an elliptic curve E: $y^2 = x^3 + ax + b$, a, b, $\in \mathbb{F}_p$ and let its order $\#E(\mathbb{F}_p)$ be a prime number r for simplicity. Then, let the embedding degree be k, r divides $p_k - 1$ but not divide $p_i - 1$, $1 \le i < k$. Moreover, r^2 divides $\#E(\mathbb{F}_{p^k})$ and thus *pairing* is considered on r-*torsion* group of $E(\mathbb{F}_{p^k})$.

Tate, Ate, and twisted Ate pairings can be roughly classiffied by the inputs for Miller's algorithm (F. Hess et al. (2006)). In general, as the inputs, Miller's algorithm needs two rational points and the number of calculation loops. Tate pairing $\tau(\cdot, \cdot)$ uses rational points $P \in E(\mathbb{F}_p)$ and $Q \in E(\mathbb{F}_{p^k})/rE(\mathbb{F}_{p^k})$, and the number of loops of Miller's algorithm is $\lfloor \log_2 r \rfloor$. Tate pairing mainly uses P for elliptic curve additions and line calculations in the loops. Q is used only for assignment calculations. 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 loops 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, and t is the Frobenius trace of $E(\mathbb{F}_p)$, that is $\#E(\mathbb{F}_p) = r = p+1-t$. The number of loops is about half of that of Tate pairing; however, Ate pairing mainly uses Q elliptic curve additions and line calculations in the loops. The output of Miller's algorithm is denoted by $f_{t-1,Q}(P)$ and thus plain Ate pairing is slower than Tate pairing.

In the case that the embedding degree k is equal to $2e$, $3e$, $4e$, $6e$, where e is a positive integer, it is known that an isomorphic map exists between a certain subgroup of $E(\mathbb{F}_{p^k})$ and *subfield–twisted* curve $E'(\mathbb{F}_{p^e})$. Let $E : y^2 = x^3 + b$, $b \in \mathbb{F}_p$ be Barreto-Naehrig curve whose embedding degree is 12, Devegili et al. (A. J. Devegili et al. (2007)) accelerated Ate pairing by using *subfield–twisted* BN curve $E'(\mathbb{F}_{p^2})$ and OEF (optimal extension field) technique (D. Bailey & C. Paar (2000)), where the twisted BN curve is given by E': $y^2 = x^3 + bv^{-1}$ and v is a quadratic and cubic non residue in subfield $\mathbb{F}_{p^2}$. Denoting the isomorphic map

Source: Convergence and Hybrid Information Technologies, Book edited by: Marius Crisan,
ISBN 978-953-307-068-1, pp. 426, March 2010, INTECH, Croatia, downloaded from SCIYO.COM

from $E'(\mathbb{F}_{p^2})$ to the corresponding subgroup of $E(\mathbb{F}_{p^{12}})$ by ψ_6, it calculates $f_{t-1,\psi_6(Q')}(P)^{(p^{12}-1)/r}$, $P \in E(\mathbb{F}_p)$, $Q' \in \psi_6^{-1}(E[r] \cap \mathrm{Ker}(\phi - [p]))$ for which *subfield– twisted* curve E' ($\mathbb{F}_{p^2}$) and Q' are efficiently used. In this case, since the twist degree d = k=e is 6, it is called *sextic* twist.
In this paper, first let us suppose

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

$$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\phi - [p]), \tag{1b}$$

where E is a pairing-friendly curve of embedding degree k = $2e$, $3e$, $4e$, $6e$. Let E' be degree d = k/e twisted curve over $\mathbb{F}_{p^e}$. Then, one can consider an isomorphic map between $E(\mathbb{F}_{p^k})$ and $E'(\mathbb{F}_{p^e})$. Denoting it from $E'(\mathbb{F}_{p^e})$ to $E(\mathbb{F}_{p^k})$ by ψ_d, consider $\mathbb{G}_1' = \psi_d^{-1}(\mathbb{G}_1)$ and $\mathbb{G}_2' = \psi_d^{-1}(\mathbb{G}_2)$. Using $Q' \in \mathbb{G}_2'$ and $P' \in \mathbb{G}_1'$, this paper proposes a new Ate pairing that calculates

$$\alpha(Q', P') = f_{t-1,Q'}(P')^{(p^k-1)/r}, \tag{2}$$

namely *cross twisted* (Xt) Ate pairing. Compared to plain Ate pairing and the previous work (A. J. Devegili et al. (2007)), Xt-Ate pairing can substantially use arithmetic operations in subfield $\mathbb{F}_{p^e}$, thus it leads to quite efficient implementation of Ate pairing. After that, this paper shows a simulation result by using BN curve and *sextic twist*. When order r is a 254-bit prime number, it is shown that Xt-Ate pairing with BN curve is carried out within 14.0 milli-seconds for which the authors uses Pentium4 (3.6GHz), C language, and GNU MP library (GNU MP). Compared to the previous *subfield–twisted* Ate pairing (A. J. Devegili et al. (2007)), Xt-Ate pairing made the algorithmic implementation and cost evaluation much clearer.
Throughout this paper, p and k denote characteristic and embedding 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

In this section, let us briefly go over some fundamentals of elliptic curve, twist technique, Ate pairing, and Miller's algorithm.

2.1 Elliptic curve

Let $\mathbb{F}_p$ be prime field and E be an elliptic curve over $\mathbb{F}_p$ defined as

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

$E(\mathbb{F}_p)$ that is a set of rational points on the curve, including the *infinity point* $\mathcal{O}$, forms an additive Abelien 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 over $E(\mathbb{F}_{p^k})$. $\#E(\mathbb{F}_p)$ is usually given as

$$\#E(\mathbb{F}_p) = p + 1 - t, \tag{4}$$

where t is the Frobenius trace of $E(\mathbb{F}_p)$.

2.2 Twist technique

When embedding degree k is equal to $2e$, where e is a positive integer, from Eq.(3) the following quadratic-twisted elliptic curve E' is given.

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

where v is a quadratic non residue in $\mathbb{F}_{p^e}$. Then, between $E'(\mathbb{F}_{p^e})$ and $E(\mathbb{F}_{p^{2e}})$, the following isomorphism is given.

$$\psi_2 : \begin{cases} E'(\mathbb{F}_{p^e}) & \to E(\mathbb{F}_{p^{2e}}), \\ (x, y) & \mapsto (xv, yv^{3/2}). \end{cases} \tag{6}$$

In this case, E' is called *quadratic–twisted* curve.

In the same, when embedding degree k satisfies the following conditions, we can respectively consider the twisted curves.

- $k = 3e$ (cubic twist)

$$E : y^2 = x^3 + b,\ b \in \mathbb{F}_p, \tag{7a}$$

$$E' : y^2 = x^3 + bv^{-2}, \tag{7b}$$

where v is a cubic non residue in $\mathbb{F}_{p^e}$ and $3 \mid (p - 1)$.

$$\psi_3 : \begin{cases} E'(\mathbb{F}_{p^e}) & \to E(\mathbb{F}_{p^{3e}}), \\ (x, y) & \mapsto (xv^{2/3}, yv). \end{cases} \tag{7c}$$

- $k = 4e$ (quatic twist)

$$E : y^2 = x^3 + ax,\ b \in \mathbb{F}_p, \tag{8a}$$

$$E' : y^2 = x^3 + av^{-1}x, \tag{8b}$$

where v is a quadratic non residue in $\mathbb{F}_{p^e}$ and $4 \mid (p - 1)$.

$$\psi_4 : \begin{cases} E'(\mathbb{F}_{p^e}) & \to E(\mathbb{F}_{p^{4e}}), \\ (x, y) & \mapsto (xv^{1/2}, yv^{3/4}). \end{cases} \tag{8c}$$

- $k = 6e$ (sextic twist)

$$E : y^2 = x^3 + b,\ b \in \mathbb{F}_p, \tag{9a}$$

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

where v is a quadratic and cubic non residue in $\mathbb{F}_{p^e}$ and $3 \mid (p - 1)$.

$$\psi_6 : \begin{cases} E'(\mathbb{F}_{p^e}) & \to E(\mathbb{F}_{p^{6e}}), \\ (x, y) & \mapsto (xv^{1/3}, yv^{1/2}). \end{cases} \tag{9c}$$

When one uses Barreto-Naehrig curve that is a class of *pairing–friendly* curve, one can apply any quadratic, cubic, quatic, or sextic twist because its embedding degree is equal to 12. As described in the following sections, sextic twist is the most efficient for pairing calculation. Eqs.(6), (7c), (8c), and (9c) are summarized as

$$\psi_d : \begin{cases} E'(\mathbb{F}_{p^e}) & \to E(\mathbb{F}_{p^{de}}), \\ (x, y) & \mapsto (xv^{2/d}, yv^{3/d}). \end{cases} \tag{10}$$

Thus, when twist degree d is even, x-coordinate $x\ v^{2/d}$ belongs to proper subfield $\mathbb{F}_{p^{k/2}}$ because $v^{2/d} \in \mathbb{F}_{p^{k/2}}$. In addition, when d = 2 or 4, the coefficient of x of the twisted curve E' can be written as $av^{-4/d}$.

2.3 Ate pairing

Let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, Ate pairing α is defined as a bilinear map:

$$\alpha : \begin{cases} \mathbb{G}_2 \times \mathbb{G}_1 & \to \mathbb{F}_{p^k}^* / (\mathbb{F}_{p^k}^*)^r \\ (Q, P) & \mapsto f_{t-1,Q}(P)^{(p^k-1)/r}, \end{cases} \tag{11}$$

where $\mathbb{G}_1$ and $\mathbb{G}_2$ are denoted by

$$\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\phi - [1]), \tag{12a}$$

$$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\phi - [p]). \tag{12b}$$

$E[r]$ denotes a subgroup of order r in $E(\mathbb{F}_{p^k})$ and $[i]$ denotes i times scalar multiplication for a rational point. ϕ denotes Frobenius endomorphism, i.e.,

$$\phi : E \to E : (x, y) \mapsto (x^p, y^p), \tag{13}$$

where x and y are x-coordinate and y-coordinate of a rational point, respectively. In general, $A = f_{t-1,Q}(P)$ is calculated by Miller's algorithm (H. Cohen & G. Frey (2005)) and then so-called *final exponentiation* $A^{(p^k-1)/r}$ follows.

2.4 Miller's Algorithm

Several improvements for Miller's algorithm have been given. Barreto et al. proposed BKLS algorithm. Algorithm 1. shows the calculation flow of the BKLS algorithm for $f_{s,Q}(P)$. It consists of functions shown in Table 1.

In this algorithm, main computation part is Step 4, Step 5, Step 7 and Step 8. In this paper, let Step 4 and Step5 be *main routine*, and let Step 7 and Step 8 be *sub routine*. In the case of Ate pairing, $P(x_P, y_P) \in \mathbb{G}_1$, $Q(x_Q, y_Q) \in \mathbb{G}_2$, $s = t - 1$, and then $f_{s,Q}(P)$ becomes an element in $\mathbb{F}_{p^k}^*$.

As shown in the algorithm, elliptic curve addition and doubling that use rational points in $E(\mathbb{F}_{p^k})$ needs arithmetic operations in $\mathbb{F}_{p^k}$. If it has *subfield–twisted* curve such as Eq.(5), it can

be efficiently reduced to subfield arithmetic operations by isomorphic maps such as Eq.(6). Thus, twist degree d is preferred to be large such as 6, that is *sextic* twist. When the d is even number, the denominator calculations in Algorithm 1. can be ignored.

Algorithm 1 : BKLS Algorithm

Input : $s, P \in \mathbb{G}_1, Q \in \mathbb{G}_2$

Output : $f_{s,Q}(P) \in \mathbb{F}_{p^k}$

Procedure :

1. $f \leftarrow 1$
2. $T \leftarrow Q$
3. for $i \leftarrow \lfloor \log_2 s \rfloor$ downto 1 do:
4. $\quad f \leftarrow f^2 \cdot l_{T,T}(P)/l_{2T,\mathcal{O}}(P)$
5. $\quad T \leftarrow T + T$
6. $\quad$ if $s_i = 1$ then:
7. $\quad\quad f \leftarrow f \cdot l_{T,Q}(P)/l_{T+Q,\mathcal{O}}(P)$
8. $\quad\quad T \leftarrow T + Q$
9. $\quad$ end if
10. end for
11. return f

s_i :	i–th bit of s from the lowest bit.
$l_{T,T}$:	the tangent line at T.
$l_{T,Q}$:	the line passing through T and Q.
$l_{2T,\mathcal{O}}$:	the vertical line passing through $2T$.
$l_{T+Q,\mathcal{O}}$:	the vertical line passing through $T + Q$.

Table 1. Notations in Algorithm 1.

3. Main proposal

In this section, a new fast pairing, namely *cross twisted* (Xt-) Ate pairing, is proposed.

3.1 Xt–Ate pairing

Supposing that the pairing-friendly curve E has a degree $d = k/e$ twist and E' be a d-th twisted curve such as Eq.(5). From the discussion in Sec.2.3, Ate pairing α is given as

$$\alpha : \begin{cases} \mathbb{G}_2 \times \mathbb{G}_1 & \to \mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r \\ (Q, P) & \mapsto f_{s,Q}(P)^{(p^k-1)/r}. \end{cases} \tag{14}$$

On the ohter hand, Xt-Ate pairing is proposed as

$$\alpha' : \begin{cases} \mathbb{G}_2' \times \mathbb{G}_1' & \to \mathbb{F}_{p^k}^*/(\mathbb{F}_{p^k}^*)^r \\ (Q', P') & \mapsto f_{s,Q'}(P')^{(p^k-1)/r}, \end{cases} \tag{15}$$

Main routine (Step 4&5 in Algorithm 1)

Procedure	Computation
1. $[2]T$	$\lambda \leftarrow (3x_T^2 + a)/(2y_T)$
	$x_{2T} \leftarrow \lambda^2 - 2x_T$
	$y_{2T} \leftarrow (x_T - x_{2T})\lambda - y_T$
2. f^2	$f \leftarrow f^2$
3. $f \cdot l_{T,T}(P)$	$l_{T,T}(P)$
	$\leftarrow (x_P - x_T)\lambda - (y_P - y_T)$
	$f \leftarrow f \cdot l_{T,T}(P)$
4. $f/l_{2T,\mathcal{O}}(P)$	$l_{2T,\mathcal{O}}(P) \leftarrow x_P - x_{2T}$
	$f \leftarrow f/l_{2T,\mathcal{O}}(P)$

Sub routine (Step 7&8 in Algorithm 1)

Procedure	Computation
1. $T + Q$	$\lambda \leftarrow (y_Q - y_T)/(x_Q - x_T)$
	$x_{T+Q} \leftarrow \lambda^2 - x_Q - x_T$
	$y_{T+Q} \leftarrow (x_Q - x_{T+Q})\lambda - y_Q$
2. $f \cdot l_{T,Q}(P)$	$l_{T,Q}(P)$
	$\leftarrow (x_P - x_Q)\lambda - (y_P - y_Q)$
	$f \leftarrow f \cdot l_{T,Q}(P)$
3. $f/l_{T+Q,\mathcal{O}}(P)$	$l_{T+Q,\mathcal{O}}(P) \leftarrow x_P - x_{T+Q}$
	$f \leftarrow f/l_{T+Q,\mathcal{O}}(P)$

where P' is a point of $\mathbb{G}_1' = \psi_d^{-1}(\mathbb{G}_1) \subset E'(\mathbb{F}_{p^{12}})$ and Q' is a point of $\mathbb{G}_2' = \psi_d^{-1}(\mathbb{G}_2) \subset E'(\mathbb{F}_{p^2})$. Here, it is most importatnt thisng that the next equation is hold,

$$\alpha'(Q', P') = \alpha(Q, P). \tag{16}$$

The main feature of Xt-Ate pairing is that the isomorphic map ψ_d^{-1} is to P as $P' = \psi_d^{-1}(P)$. In other words, $P \in E(\mathbb{F}_p)$ is extended to $P' \in E'(\mathbb{F}_{p^k})$ and $Q \in E(\mathbb{F}_{p^k})$ is compressed to $Q' \in E'(\mathbb{F}_{p^e})$. Thus, the authors named it *cross twisted* (Xt-) Ate pairing. Fig 1. shows the key map of Xt-Ate pairing with $\mathbb{G}_1'$ and $\mathbb{G}_2'$. In spite of the inputted points P' and Q' on the twisted curvce, the miller loop s is given by $t - 1$, where t is the trace of $E(\mathbb{F}_p)$. The following three lemmas lead to Eq.(16).

Lemma 1.

$$d(p^e - 1) \mid (p^k - 1)/r. \tag{17}$$

Proof: From the definition of embedding degree,

$$r \nmid (p^e - 1). \tag{18}$$

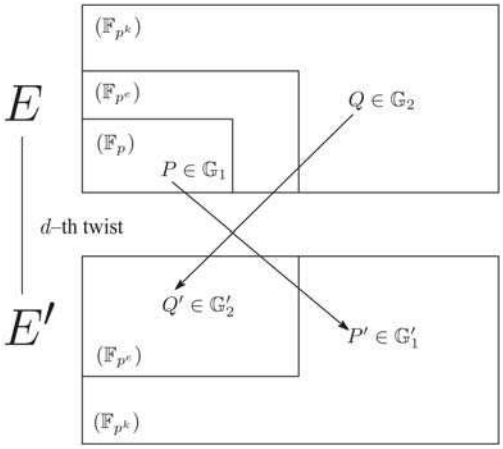

Fig. 1. Xt-Ate pairing with $\mathbb{G}_1'$ and $\mathbb{G}_2'$

Then, we have

$$\begin{aligned}\frac{(p^k-1)/r}{p^e-1} &= \left(p^{(d-1)e}+p^{(d-2)e}+\cdots+1\right)/r \\ &= \left(\sum_{i=1}^{d} p^{(d-i)e}\right)/r \\ &= \left(\sum_{i=1}^{d}(p^{(d-i)e}-1)+d\right)/r.\end{aligned} \tag{19}$$

Since $d \mid (p-1)$ and $\gcd(d, r)=1$, this lemma is shown. ■

Lemma 2.

$$l_{T',T'}(P')^{(p^k-1)/r} = l_{T,T}(P)^{(p^k-1)/r}, \tag{20}$$

$$l_{T',Q'}(P')^{(p^k-1)/r} = l_{T,Q}(P)^{(p^k-1)/r}. \tag{21}$$

Proof: Using T', $Q' \in \mathbb{F}_{p^e}$ such that $T = \psi_d(T')$ and $Q = \psi_d(Q')$, the slopes $\lambda_{T,T}$ and $\lambda_{T,Q}$ are written as

$$\begin{aligned}\lambda_{T,T} &= \frac{3x_T^2+a}{2y_T} \\ &= \frac{3\left(x_{T'}v^{2/d}\right)^2+a}{2x_{T'}v^{3/d}} \\ &= \frac{3x_{T'}^2+a/v^{4/d}}{2x_{T'}}\cdot\frac{v^{4/d}}{v^{3/d}} \\ &= \frac{3x_{T'}^2+a'}{2x_{T'}}\cdot v^{1/d} \\ &= \lambda_{T',T'}\cdot v^{1/d},\end{aligned} \tag{22a}$$

$$\begin{aligned}\lambda_{T,Q} &= \frac{y_Q - y_T}{x_Q - x_T} \\ &= \frac{y_{Q'}v^{3/d} - y_{T'}v^{3/d}}{x_{Q'}v^{2/d} - x_{T'}v^{2/d}} \\ &= \frac{y_{Q'} - y_{T'}}{x_{Q'} - x_{T'}} \cdot \frac{v^{3/d}}{v^{2/d}} \\ &= \frac{y_{Q'} - y_{T'}}{x_{Q'} - x_{T'}} \cdot v^{1/d} \\ &= \lambda_{Q',T'} \cdot v^{1/d}.\end{aligned} \tag{22b}$$

Thus, regardless of whether or not $T = Q$, we have

$$\lambda_{T,Q} = \lambda_{T',Q'} v^{1/d}. \tag{23}$$

Then, we have

$$\begin{aligned}l_{T,Q}(P) &= (x_P - x_T)\lambda_{T,Q} - (y_P - y_T) \\ &= (x_{P'}v^{2/d} - x_{T'}v^{2/d})\lambda_{T',Q'}v^{1/d} \\ &\qquad -(y_{P'}v^{3/d} - y_{T'}v^{3/d}) \\ &= (x_{P'} - x_{T'})\lambda_{T',Q'}v^{3/d} - (y_{P'} - y_{T'})v^{3/d} \\ &= l_{T',Q'}(P') \cdot v^{3/d}.\end{aligned} \tag{24}$$

Since $v \in \mathbb{F}_{p^e}$, the following equation holds.

$$\left(v^{3/d}\right)^{(p^e-1)d} = \left(v^{(p^e-1)}\right)^3 = 1. \tag{25}$$

Therefore, according to Lemma 1, $v^{3/d}$ of Eq.(24) becomes 1 at *final exponentiation* of Xt-Ate pairing. Thus, this lemma is shown. ■

Lemma 3.

$$l_{T',\mathcal{O}}(P')^{(p^k-1)/r} = l_{T,\mathcal{O}}(P)^{(p^k-1)/r}. \tag{26}$$

Proof: Since the following equation holds,

$$\begin{aligned}{}_{T,\mathcal{O}}(P) &= x_P - x_T \\ &= x_{P'}v^{2/d} - x_{T'}v^{2/d} \\ &= (x_{P'} - x_{T'}) \cdot v^{2/d} \\ &= l_{T',\mathcal{O}}(P') \cdot v^{2/d}.\end{aligned} \tag{27}$$

Note $v \in \mathbb{F}_{p^e}$, we have

$$\left(v^{2/d}\right)^{(p^e-1)d} = \left(v^{(p^e-1)}\right)^2 = 1. \tag{28}$$

Therefore, according to Lemma 1, $v^{2/d}$of Eq.(27) becomes 1 at *final exponentiation* of Xt-Ate pairing. Thus, this lemma is shown. ■

$F_{t-1,Q}(P)$ is calculated with $l_{T,T}(P)$, $l_{T,Q}(P)$, and $l_{T,\mathcal{O}}(P)$. Therefore, according to Lemma 2 and Lemma 3, Eq.(16) is shown.

3.2 Calculation procedure

Suppose the following d-th twisted curve E' over $\mathbb{F}_{p^e}$.

$$E' : y^2 = x^3 + a'x + b',\ a', b' \in \mathbb{F}_{p^e}. \tag{29}$$

Noting that $P' \in \mathbb{G}'_1 \subset E'(\mathbb{F}_{p^k})$ and $Q' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^e})$, Xt-Ate pairing is computed by Algorithm 2.. In practice, the *main routine* (Step 4&5 in Algorithm 2) and the *sub routine* (Step 7&8 in Algorithm 2) are computed as follows. First, compute

$$\lambda_{T',T'} = \frac{3x_{T'} + a'}{2y_{T'}}, \tag{30a}$$

$$\lambda_{T',Q'} = \frac{y_{Q'} - y_{T'}}{x_{Q'} - x_{T'}}. \tag{30b}$$

Algorithm 2 : Xt–Ate pairing

Input : $s = t - 1, P' \in \mathbb{G}'_1, Q' \in \mathbb{G}'_2$

Output : $\alpha'(Q', P') = f_{s,Q'}(P')^{(p^k-1)/r}$

Procedure :

1. $f \leftarrow 1$
2. $T' \leftarrow Q'$
3. for $i \leftarrow \lfloor \log_2 s \rfloor$ downto 1 do:
4. $\quad f \leftarrow f^2 \cdot l_{T',T'}(Q)/l_{2T',\mathcal{O}}(P')$
5. $\quad T' \leftarrow T' + T'$
6. $\quad$ if $s_i = 1$ then:
7. $\quad\quad f \leftarrow f \cdot l_{T',Q'}(P)/l_{T'+Q',\mathcal{O}}(P')$
8. $\quad\quad T' \leftarrow T' + Q'$
9. $\quad$ end if
10. end for
11. $f \leftarrow f^{(p^k-1)/r}$
12. return f

Regardless of whether or not $T' = Q'$, we have

$$x_{T'+Q'} = \lambda^2_{T',Q'} - x_{Q'} - x_{T'}, \tag{31a}$$

$$y_{T'+Q'} = (x_{Q'} - x_{T'+Q'})\lambda_{T',Q'} - y_{Q'}, \tag{31b}$$

and the next line calculations are computed as

$$l_{T',Q'}(P') = (x_{P'} - x_{Q'})\,\lambda_{T',Q'} - (y_{P'} - y_{Q'}), \tag{32a}$$

$$l_{T',\mathcal{O}}(P') = x_{P'} - x_{T'}. \tag{32b}$$

Every calculation excluding the one multiplication shown in Eq.(32a) are carried out in subfield $\mathbb{F}_{p^e}$. Thus, most of this algorithm is efficiently carried out by subfield arithmetic opearations in $\mathbb{F}_{p^e}$. Note that the Eq.(32a) needs the multiplication between elements in $\mathbb{F}_{p^e}$ and $\mathbb{F}_{p^{k/\gcd(d,2)}}$. When the twist degree d is even number, it has a little advantage. Of course, when the d is even, as previously introduced, the calculation of Eq.(32b) can be ignored. The *main rutine* and the *sub routine* of Xt-Ate pairing can be written as the following algorithms.

Main routine (Step 4&5 in Algorithm 2)

Procedure	Computation
1. $[2]T'$	$\lambda \leftarrow (3x_{T'}^2 + a')/(2y_{T'})$
	$x_{2T'} \leftarrow \lambda^2 - 2x_{T'}$
	$y_{2T'} \leftarrow (x_{T'} - x_{2T'})\lambda - y_{T'}$
2. f^2	$f \leftarrow f^2$
3. $f \cdot l_{T',T'}(P')$	$l_{T',T'}(P')$
	$\leftarrow (x_{P'} - x_{T'})\lambda - (y_{P'} - y_{T'})$
	$f \leftarrow f \cdot l_{T',T'}(P')$
4. $f/l_{2T',\mathcal{O}}(P')$	$l_{2T',\mathcal{O}}(P') \leftarrow x_{P'} - x_{2T'}$
	$f \leftarrow f/l_{2T',\mathcal{O}}(P')$

Sub routine (Step 7&8 in Algorithm 2)

Procedure	Computation
1. $T' + Q'$	$\lambda \leftarrow (y_{Q'} - y_{T'})/(x_{Q'} - x_{T'})$
	$x_{T'+Q'} \leftarrow \lambda^2 - x_{Q'} - x_{T'}$
	$y_{T'+Q'} \leftarrow (x_{Q'} - x_{T'+Q'})\lambda - y_{Q'}$
2. $f \cdot l_{T',Q'}(P')$	$l_{T',Q'}(P')$
	$\leftarrow (x_{P'} - x_{Q'})\lambda - (y_{P'} - y_{Q'})$
	$f \leftarrow f \cdot l_{T',Q'}(P')$
3. $f/l_{T'+Q',\mathcal{O}}(P')$	$l_{T'+Q',\mathcal{O}}(P') \leftarrow x_{P'} - x_{T'+Q'}$
	$f \leftarrow f/l_{T'+Q',\mathcal{O}}(P')$

3.3 Cost evaluation

We evaluate the calculation cost of Xt-Ate pairing. In order to simplify the cost evaluation, we only take the calculation costs for multiplication, squaring, and inversion in finite field into account. Notations in Table 2. are used.

Let the calculation costs of *main routine* and *sub routine* in Algorithm 2 be TMAIN and TSUB, respectively. When the number of the calculation loops of Miller's algorithm is $\lfloor \log_2 s \rfloor$, Xt-Ate pairing excluding the final exponentiation needs the following cost.

$$(\lfloor \log_2 s \rfloor - 1)\mathrm{TMAIN} + (\mathrm{Hw}(s) - 1)\mathrm{TSUB}, \tag{33}$$

−1's in the above equation denote that it is no needed to calculate for the most significant bit. When d is even such as 2, 4, and 6, TMAIN and TSUB are given as

$$\begin{aligned} \text{TMAIN} &= 2S_e + 2M_e + I_e + M_{e,k/\gcd(d,2)} + S_k + M_k, \\ \text{TSUB} &= S_e + 2M_e + I_e + M_{e,k/\gcd(d,2)} + M_k. \end{aligned} \tag{34}$$

When d = 3, since the vertical line calculation is needed, they becomes

$$\begin{aligned} \text{TMAIN} &= 2S_e + 2M_e + I_e + M_{e,k/\gcd(d,2)} + S_k + 2M_k, \\ \text{TSUB} &= S_e + 2M_e + I_e + M_{e,k/\gcd(d,2)} + 2M_k. \end{aligned} \tag{35}$$

Following the cost evaluation manner of (S. Matsuda et al. (2007)), (F. Hess et al. (2006)), $M_{2^i 3^j e}$ be $3^i 5^j M_e$, $M_{i,j} = (j/i)M_i$, and $S_i = M_i$ for simplicity. Then, we have Table 3. Suppose that $\mathrm{Hw}(s) \approx \lfloor \log_2 s \rfloor / 2$, $M_{5e} = 15M_e$, and roughly $I_i = 7M_i$, we have Table 4.

$M_i,\ S_i,\ I_i$:	the calculation costs of a multiplication, squaring, and inversion in $\mathbb{F}_{p^i}$, respectively.
$M_{i,j}$:	the calculation cost of a multiplication between two elements in $\mathbb{F}_{p^i}$ and $\mathbb{F}_{p^j}$, where i divides j.
$\mathrm{Hw}(s)$:	the Hamming weight of s.

Table 2. Notations for cost evaluation

d	TMAIN	TSUB
2	$11M_e + I_e$	$7M_e + I_e$
4	$22M_e + I_e$	$12M_e + I_e$
3	$19M_e + I_e$	$13M_e + I_e$
6	$34M_e + I_e$	$18M_e + I_e$

Table 3. Calculation costs of TMAIN and TSUB for Xt-Ate pairing

$\lfloor \log_2 p \rfloor$	$\lfloor \log_2 r \rfloor$	k	d	cost
384	256	8	4	$14784\,M_1$
256	256	10	2	$44352\,M_1$
256	256	12	6	$20396\,M_1$

Table 4. Calculation costs of Xt-Ate pairing

4. Efficiency of Xt-Ate pairing

This section shows the efficiency of Xt-Ate pairing.

4.1 Comparison of pairings

Table 5. shows the comparison of the input parameters of Miller's algorithm between various pairings.

pairing	s	A	B
plain Tate	r	$E(\mathbb{F}_p)$	$E(\mathbb{F}_{p^k})$
Twisted Ate (S. Matsuda et al. (2007))	$(t-1)^e \bmod r$	$E(\mathbb{F}_p)$	$E(\mathbb{F}_{p^k})$
plain Ate	$t-1$	$E(\mathbb{F}_{p^k})$	$E(\mathbb{F}_p)$
Xt–Ate	$t-1$	$E'(\mathbb{F}_{p^e})$	$E'(\mathbb{F}_{p^k})$

Table 5. Input parameters of $f_{s,A}(B)$

Consider the inputs for Miller's algorithm calculating $f_{s,A}(B)$ with s,A, and B. In detail, the number of calculation loops of Miller's algorithm is given by $\lfloor \log_2 s \rfloor$, the point A is used for a lot of calculations, and the point B has little effect on the efficiency. Therefore, plain Tate pairing uses A 2 $E(\mathbb{F}_p)$. Twisted Ate pairing (S. Matsuda et al. (2007)) uses $(t-1)^{k/d} \pmod r$ as s. For cyclotomic families such as Barreto-Naehrig curve, $(t-1)^e \pmod r$ is smaller than $t-1$ in general. Thus, twisted Ate pairing is more efficient than plain Tate pairing.

Ate pairing made the number of the calculation loops of Miller's algorithm, that is $t-1$, smaller than that of Tate pairing but it uses $A \in E(\mathbb{F}_{p^k})$. Thus, plain Ate pairing is not superior to Tate pairing. However, Ate pairing generally uses $A \in E'(\mathbb{F}_{p^{k/d}})$ instead of that in $E(\mathbb{F}_{p^k})$.

Xt-Ate pairing is more efficient than the Ate pairing. It uses $B \in \mathbb{G}_1' = \psi_d^{-1}(\mathbb{G}_1)$, where $\mathbb{G}_1 \subseteq E(\mathbb{F}_p)$. Xt-Ate pairing does not calculates $l_{T,Q}(P)$ by eq.(37) and it calculates $l_{T',Q'}(P')$ by eq.(32a) for Miller's algorithm since every calculation is carried out over twisted curve E'. It is noted that Xt-Ate pairing uses $\mathbb{G}_2'$ and $\mathbb{G}_1'$; however, for pairing–based cryptographic applications such that a lot of scalar multiplications are needed, $\mathbb{G}_1 \subseteq E(\mathbb{F}_p)$ and $\mathbb{G}_2'$ should be used for them. Appropriately using isomorphic map ψ_d and ψ_d^{-1}, not only Xt-Ate pairing but also scalar multiplications will be efficiently carried out.

As the most recent works, Vercauteren (F. Vercauteren (2008)), Lee et al. (E. Lee et al. (2008)), and the authors (Y. Nogami et al. (2008)) have proposed efficient Ate pairings, namely *optimal pairing*, *R–Ate pairing*, *Xate pairing*, respectively. They have reduced the number of the calculation loops of Miller's algorithm less than $t - 1$. For their works, *cross–twist* technique can be efficiently applied.

4.2 Xt-Ate pairing for BN curve

In order to show the efficiency of Xt-Ate pairing, this subsection considers Barreto-Naehrig (BN) curve (P. S. L. M. Barreto & M. Naehrig (2006)) of 254-bit prime order with k = 12 and d = 6. Since *sextic twist* is efficiently applied, embedding degree 12 is one of the most competitive research targets. As a typical feature of BN curve, characteristic p, order r, and Frobenius trace t are given by using an integer variable χ as

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

$$r(\chi) = 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1, \tag{36b}$$

$$t(\chi) = 6\chi^2 + 1. \tag{36c}$$

For BN curve, Devegili et al. (A. J. Devegili et al. (2007)) proposed an improved Ate pairing whose Miller's algorithm calculates elliptic curve operations of $\mathbb{G}'_2 \in E'(\mathbb{F}_{p^2})$. Then, $\mathbb{G}'_2$ is isomorphic to G_2 with ψ_6 defined by Eq.(9c), for every loop of Miller's algorithm, it needs to calculate $l_{T,Q}(P)$ as follows:

$$\begin{aligned} l_{T,Q}(P) &= (x_P - x_Q)\lambda_{T,Q} - (y_P - y_Q) \\ &= (-y_P) + (x_P \cdot \lambda_{T',Q'})z + (y_{T'} - x_{T'} \cdot \lambda_{T',Q'})z^3. \end{aligned} \tag{37}$$

This calculation needs 3 times $\mathbb{F}_p$ multiplications. On the other hand, Xt-Ate pairing needs 9 times $\mathbb{F}_p$ mutiplications to calculate $l_{T',Q'}(P')$. Thus, in this view point, Devegili et. al. work is more efficient than Xt-Ate pairing.

Though the Devegili et. al. work restricts the parameters of pairing friendly curve. As also introduced in (A. J. Devegili et al. (2007)), (Y. Sakemi et al. (2008)), (M. Akane et al. (2007)), χ of small Hamming weight is efficient for not only Miller's algorithm but also final exponentiation. Table 6. shows all χ's of Hamming weight 3 that gives 254-bit prime order BN curve. Note that, in this case, there are no χ's of Hamming weight 2 such that order r becomes 254-bit prime number.

χ	Hw(s)	E
$2^{62}+2^{35}+2^{24}$	12	$y^2=x^3+10$
$2^{62}+2^{55}+1$	12	$y^2=x^3+7$
$-2^{62}-2^{41}-2^{23}$	12	$y^2=x^3+13$

Table 6. χ of small Hamming weight that gives 254-bit prime order BN curve

5. Simulation

This section shows a simulation result of Xt-Ate pairing.

5.1 Parameters of pairing-friendly curve

In this simulation, the authors used the following χ and BN curve,

$$\chi = 2^{62} + 2^{35} + 2^{24}, \tag{38}$$

$$E : y^2 = x^3 + 10, \tag{39}$$

then r = #$E(\mathbb{F}_p)$ becomes 254-bit prime number and the order of $\mathbb{F}_{p^{12}}$ becomes 3048-bit number.

5.2 Representation of extension field

This simulation First, the authors prepared $\mathbb{F}_{p^4}$ with type-⟨1, 4⟩ Gauss period normal basis (GNB) (H. Cohen & G. Frey (2005)) and also $\mathbb{F}_{p^3}$ with type-⟨2, 3⟩ GNB. Then, the authors prepared $\mathbb{F}_{p^{12}}$ as *tower field* $\mathbb{F}_{(p^4)^3}$by towering ⟨2, 3⟩ GNB over $\mathbb{F}_{p^4}$ (Y. Nogami & Y. Morikawa (2003)). For multiplication with GNB, the authors implemented our previous work *cyclic vector multiplication algorithm* (CVMA) (H. Kato et al. (2007)). For example, CVMA calculates a multiplication in $\mathbb{F}_{(p^m)^n}$ by

$$M_{mn} = \frac{n(n+1)}{2} M_m = \frac{mn(m+1)(n+1)}{4} M_1. \tag{40}$$

For inversions in extension field and prime field, the authors implemented Itoh-Tsujii inversion algorithm (T. Itoh & S. Tsujii (1988)) and *binary extended* Euclidean algorithm (D. Knuth (1981)), respectively. Since GNB is normal basis, one can easily prepare arithmetic operations in subfields $\mathbb{F}_{p^2}, \mathbb{F}_{p^4}, \mathbb{F}_{(p^2)^3}$. Table 7. shows the timing of each operation.

[unit:μs]

extension field	operation type	254–bit p
$\mathbb{F}_p$	M_1	0.65
	I_1	8.30
$\mathbb{F}_{p^2}$	M_2	1.65
	I_2	11.5
$\mathbb{F}_{p^4}$	M_4	4.40
	I_4	20.4
$\mathbb{F}_{p^6}$	M_6	7.84
	I_6	32.2
$\mathbb{F}_{p^{12}}$	M_{12}	21.5
	I_{12}	80.7
	S_{12}	19.6

Table 7. Timings of each arithmetic operation

5.3 Final exponentiation

Using several Frobenius mappings, the final exponentiation is carried out as Algorithm 3. (A. J. Devegili et al. (2007)), where we note that the exponent $(p^{12}-1)/r$ is factorized as

$$(p^{12}-1)/r = (p^2+1)(p^6-1)\frac{p^4-p^2+1}{r}. \tag{41}$$

f^{p^i}'s shown in Algorithm 3. are given by Frobenius mappings. In the case of BN curve of embedding degree 12, referring to (A. J. Devegili et al. (2007)), final exponentiation is carried out by Algorithm 3. Note that Frobenius maps such as f^{p^i} in Algorithm 3. do not need any arithmetic operations because GNB is normal basis.

From Algorithm 3., it is found that the exponentiations of χ and χ^2 needs hard exponentiations such as binary method (square and multiply method). The calculation cost of an exponentiation closely depends on the binary representation of the exponent.

The calculation cost of final exponentiation Algorithm 3. is evaluated as

$$\begin{aligned} &\{4 + \lfloor \log_2 \chi \rfloor + \lfloor \log_2 \chi^2 \rfloor\} S_{12} \\ &+\{17 + \mathrm{Hw}(\chi) + \mathrm{Hw}(\chi^2)\} M_{12} + 2I_{12}. \end{aligned} \tag{42}$$

Substituting $S_{12} = 0.9M_{12}$ and $I_{12} = 4M_{12}$ that is base on the simulation result Table 7., we have

$$\{28.6 + 2.7\lfloor \log_2 \chi \rfloor + \mathrm{Hw}(\chi) + \mathrm{Hw}(\chi^2)\}M_{12}. \tag{43}$$

Algorithm 3 : Final exponentiation

Input : f given by $f_{t-1,Q'}(P')$, χ, p
Output : $f^{(p^6-1)(p^2+1)(p^4-p^2+1)/r}$

Procedure :

1. $f \leftarrow f^{p^6} \cdot f^{-1}$
2. $f \leftarrow f^{p^2} \cdot f$
3. $a \leftarrow (f^6)^{\chi} \cdot (f^5)^{p^6}$
4. $b \leftarrow a^p$
5. $b \leftarrow a \cdot b$
6. compute f^p, f^{p^2}, and f^{p^3}
7. $c \leftarrow b \cdot (f^p)^2 \cdot f^{p^2}$
8. $f \leftarrow f^{p^3} \cdot (c^6)^{\chi^2} \cdot c \cdot b \cdot (f^p \cdot f)^9 \cdot a \cdot f^4$
9. return f

5.4 Simulation result

Table 8. shows the simulation result. Xt-Ate pairing of 254-bit and 3048-bit security levels is carried out within 14.0 milli-seconds. Thus, it is shown that *cross twist* technique is quite efficient for Ate pairing. The authors simulated Xt-Ate pairing using Eq.(38) with the computational environment Table 9.

6. Conclusion

In this paper, supposing

$$\mathbb{G}_1 = E[r] \cap \mathrm{Ker}(\phi - [1]), \tag{44a}$$

$$\mathbb{G}_2 = E[r] \cap \mathrm{Ker}(\phi - [p]), \tag{44b}$$

where E was a pairing-friendly curve of embedding degree $k = 2e, 3e, 4e, 6e$, then denoting the isomorphic map from $E'(\mathbb{F}_{p^e})$ to $E(\mathbb{F}_{p^k})$ by ψ_d, we considered $\mathbb{G}'_1 = \psi_d^{-1}(\mathbb{G}_1)$ and $\mathbb{G}'_2 = \psi_d^{-1}(\mathbb{G}_2)$. Using $Q' \in \mathbb{G}'_2$ and $P' \in \mathbb{G}'_1$, this paper proposed a new Ate pairing that calculates

$$\alpha(Q', P') = f_{t-1,Q'}(P')^{(p^k-1)/r}, \tag{45}$$

namely *cross twisted* (Xt) Ate pairing. Compared to plain Ate pairing and Devegili's work, Xt-Ate pairing could substantially use arithmetic operations in subfield $\mathbb{F}_{p^e}$, thus it lead to quite efficient implementation of Ate pairing. Then, this paper showed a simulation result by using BN curve and *sextic twist*. When order r was a 254-bit prime number, it was shown that Xt-Ate pairing with BN curve was carried out within 14.0 milli-seconds for which the authors used Pentium4 (3.6GHz), C language, GNU MP library.

[unit:ms]

Xt–Ate pairing	
Miller's algorithm	8.80
final exponentiation	4.49
total	13.3
elliptic curve scalar multiplication$_\dagger$	
$\mathbb{G}_1 \in E(\mathbb{F}_p)_\ddagger$	2.65
$\mathbb{G}_2' \in E'(\mathbb{F}_{p^2})$	7.02
exponentiation$_\dagger$	
$\mathbb{G}_3 \in \mathbb{F}_{p^{12}}^*$	7.88

$_\dagger$with 254–bit random scalars/exponents.

$_\ddagger$ *Projective coordinate* is used.

Table 8. Timings of operations with 254-bit prime order BN curve

CPU	Pentium4 3.6GHz
cash size	2048KB
OS	Linux 2.6.21
Language	C
compiler	gcc 4.2.1
option	-O3 -march=pentium4 -fforce-mem
library	Gnu MP 4.2.1 (GNU MP)

Table 9. Computational environment

7. References

D. Bailey and C. Paar (2000). Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms, *Proc. Asiacrypt2000*, LNCS 1976, pp. 248-258.

P. S. L. M. Barreto, and M. Naehrig (2006). Pairing-Friendly Elliptic Curves of Prime Order, *Proc. of SAC2005*, LNCS 3897, pp. 319-331.

D. Boneh, B. Lynn, and H. Shacham (2001). Short signatures from the Weil pairing, *Proc. of Asiacrypt2001* , LNCS 2248, pp. 514-532.

H. Cohen and G. Frey (2005). Handbook of Elliptic and Hyperelliptic Curve Cryptography, *Discrete Mathematics and Its Applications*, Chapman & Hall CRC, pp. 280-285, p. 458.

A. J. Devegili, M. Scott, and R. Dahab (2007). Implementing Cryptographic Pairings over Barreto-Naehrig Curves, *Proc. of Pairing 2007*, LNCS 4575, pp. 197-207.

GNU MP. GNU Multiple Precision Arithmetic Library, http://gmplib.org/

F. Hess, N. Smart, and F. Vercauteren (2006). The Eta Pairing Revisited, *IEEE Trans. Information Theory*, pp. 4595-4602.

T. Itoh and S. Tsujii (1988). A Fast Algorithm for Computing Multiplicative Inverses in $GF(2^m)$ Using Normal Bases, *Inf. and Comp.*, vol. 78, pp. 171-177.

D. Knuth (1981). The Art of Computer Programming, *vol. 2: Seminumerical Algorithms*, Addison-Wesley.

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

S. Matsuda et al. (2007). Optimised versions of the Ate and Twisted Ate Pairings, IACR, ePrint, available at http://eprint.iacr.org/2007/013.pdf

T. Nakanishi and N. Funabiki (2005). Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps, *Proc. of Asiacrypt2005*, LNCS 3788, Springer-Verlag, pp. 443-454.

Y. Nogami and Y. Morikawa (2003). A Fast Implementation of Elliptic Curve Cryptosystem with Prime Order Defined over F_{p^8}, *Memoirs of the Faculty of Engineering Okayama University*, vol. 37, no. 2, pp. 73-88.

M. Akane, H. Kato, T. Okimoto, Y. Nogami, and Y. Morikawa (2007). An Improvement of Miller's Algorithm in Ate Pairing with Barreto-Naehrig Curve, *Proc. of Computer Security Symposium 2007 (CSS2007)*, pp. 489-494.

M. Akane, H. Kato, T. Okimoto, Y. Nogami, and Y. Morikawa (2007). Efficient Parameters for Ate Pairing Computation with Barreto-Naehrig Curve, *Proc. of Computer Security Symposium 2007 (CSS2007)*, pp. 495-500.

H. Kato, Y. Nogami, T. Yoshida, and Y. Morikawa (2007). Cyclic Vector Multiplication Algorithm Based on a Special Class of Gauss Period Normal Basis, *ETRI Journal*, vol. 29, no. 6, pp. 769 - 778, available at http://etrij.etri.re.kr/Cyber/servlet/BrowseAbstract?paperid=RP0702-0040

Y. Nogami, M. Akane, Y. Sakemi, H. Kato, and Y. Morikawa (2008). Integer Variable χ-based Ate Pairing, *Proc. of Pairing 2008*, LNCS 5209, pp. 178-191.

Y. Sakemi, H. Kato, M. Akane, T. Okimoto, Y. Nogami, and Y. Morikawa (2008). An Improvement of Twisted Ate Pairing Using Integer Variable with Small Hamming Weight, *The 2008 Symposium on Cryptography and Information Security (SCIS)*, Jan. 22-25.

F. Vercauteren (2008). Optimal Pairings, IACR ePrint archive, available at http://eprint.iacr.org/2008/096.

Convergence and Hybrid Information Technologies

Edited by Marius Crisan

ISBN 978-953-307-068-1
Hard cover, 426 pages
Publisher InTech
Published online 01, March, 2010
Published in print edition March, 2010

Starting a journey on the new path of converging information technologies is the aim of the present book. Extended on 27 chapters, the book provides the reader with some leading-edge research results regarding algorithms and information models, software frameworks, multimedia, information security, communication networks, and applications. Information technologies are only at the dawn of a massive transformation and adaptation to the complex demands of the new upcoming information society. It is not possible to achieve a thorough view of the field in one book. Nonetheless, the editor hopes that the book can at least offer the first step into the convergence domain of information technologies, and the reader will find it instructive and stimulating.

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821