21

An Improvement of Twisted Ate Pairing with Barreto-Naehrig Curve by using Frobenius Mapping

Yumi Sakemi, Hidehiro Kato, Yasuyuki Nogami and Yoshitaka Morikawa
Okayama University
Japan

1. Introduction

Recently, pairing-based cryptographic applications such as ID-based cryptography (Boneh et al., 2001) and group signature scheme (Nakanishi & Funabiki, 2005) have received much attention. In order to make it practical, various pairings such as Ate pairing (Cohen & Frey, 2005), *subfield-twisted* pairing (Matsuda et al., 2007) and *subfield-twisted* Ate pairing (Devegili et al., 2007) have been proposed. This paper focuses on *twisted-Ate* pairing with Barreto-Naehrig (BN) curve (Barreto & Naehrig, 2005). As a typical feature of BN curve whose embedding degree is 12, its characteristic p, its order r, and Frobenius trace t are respectively given with *integer variable* χ as follows.

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

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

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

Pairing calculation usually consists of two parts, one is Miller's algorithm calculation and the other is so-called *final exponentiation*. Let E be BN curve of characteristic p, Miller's algorithm of *twisted-Ate* pairing calculates $f_{s,P}(Q)\, f_{s,P}(Q)$, where s is given by $(t-1)^2 \bmod r$, P and Q are rational points in certain subgroups of order r in $E(F_p)$ and $E(F_{p^{12}})$, respectively. In this case, $(t-1)^2 \bmod r$ becomes

$$(t-1)^2 \bmod r = 36\chi^3 - 18\chi^2 + 6\chi - 1 \tag{2}$$

it corresponds to the number of iterations of Miller's algorithm. In addition, the hamming weight of $(t-1)^2 \bmod r$ is preferred to be small for Miller's algorithm to be fast carried out. This paper proposes an improvement of Miller's algorithm.
In the improvement, we use the following relations:

$$\begin{aligned}(t-1)^2 &\equiv 36\chi^3 - 18\chi^2 + 6\chi - 1 \\ &\equiv 6\chi^2(6\chi - 3) + 6\chi - 1 \equiv p(6\chi - 3) + 6\chi - 1 \bmod r,\end{aligned} \tag{3}$$

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

,where $p \equiv t-1 = 6\chi^2 \bmod r$ .First, calculate $f_{6\chi-3,P}(Q)$ by Miller's algorithm, then calculate $f_{6\chi-1,P}(Q)$ by using the result of the preceding calculation. Then, using the result, calculate $f_{p,(6\chi-3)P}(Q)$ for which Frobenius mapping in extension field $F_{p^{12}}$ with respect to prime field F_p is efficiently applied. In detail, since *p* is the characteristic of F_{p^m} , Frobenius mapping does not need any arithmetic operations when the extension field has fast Frobenius mapping such as OEF (Bailey & Paar, 1998). After that, the authors show some simulation results from which we find that the improvement shown in this paper efficiently accelerates *twisted-Ate* pairing including *final exponentiation* about 14.1%.
Throughout this paper, *p* and *k* denote characteristic and extension degree, respectively. F_{p^k} denotes *k*-th extension field over F_p and $F_{p^k}^*$ denotes its multiplicative group.

2. Fundamantals

This section briefly reviews elliptic curve, *twisted-Ate* pairing, and divisor theorem.

2.1 Elliptic curve and BN curve

Let F_p be prime field and E be an elliptic curve over F_p . $E(F_p)$ that is the set of rational points on the curve, including the *infinity point* O, forms an additive Abelian group. Let $\#E(F_p)$ be its order, consider a large prime number *r* that divides $\#E(F_p)$. The smallest positive integer *k* such that *r* divides p^k-1 is especially called *embedding degree*. One can consider a pairing such as Tate and Ate pairings on $E(F_{p^k})$.
Usually, $\#E(F_p)$ is written as

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

where *t* is the Frobenius trace of $E(F_p)$. Characteristic *p* and Frobenius trace *t* of Barreto--Naehrig (BN) curve (Barreto & Naehrig, 2005) are given by using an integer variable χ as Eqs.(1). In addition, BN curve E is written as

$$E(F_p) : y^2 = x^3 + b, \quad b \in F_p \tag{5}$$

whose embedding degree is 12. In this paper, let $\#E(F_p)$ be a prime number *r* for instance.

2.2 Twisted ate pairing with BN curve

Let ϕ be Frobenius endomorphism, i.e.,

$$\phi : E(F_{p^{12}}) \to E(F_{p^{12}}) : (x, y) \to (x^p, y^p) , \tag{6}$$

Then, in the case of BN curve, let G_1 and G_2 be

$$G_1 = E[r] \cap \mathrm{Ker}(\phi - [1]) , \tag{7a}$$

$$G_2 = E[r] \cap \mathrm{Ker}([\xi_6]\phi^2 - [1]) \tag{7b}$$

where ξ_6 is a primitive 6-th root of unity and let $P \in G_1$ and $Q \in G_2$, *twisted-Ate* pairing $\alpha(\cdot, \cdot)$ is defined as

$$\alpha(\cdot,\cdot):\begin{cases} G_1 \times G_2 \to F^*_{p^{12}} / (F^*_{p^{12}})^r \\ (P,Q) \mapsto f_{s,P}(Q)^{(p^{12}-1)/r}. \end{cases} \tag{8}$$

$A = f_{s,P}(Q)$ is usually calculated by Miller's algorithm (Devegili et al., 2007), then so--called *final exponentiation* $A^{(p^{12}-1)/r}$ follows. The number of calculation loops of Miller's algorithm of *twisted-Ate* pairing with BN curve is determined by $\lfloor \log_2 s \rfloor$, where s is, in this case, given by

$$s = (t-1)^2 \bmod r = 36\chi^3 - 18\chi^2 + 6\chi - 1. \tag{9}$$

It is said that calculation cost of Miller's Algorithm is about twice of that of final exponentiation.

2.3 Divisor

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

$$D = (Q) - (\mathrm{O}) = (Q) - (\mathrm{O}) + div(1). \tag{10}$$

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

$$aD = (aQ) - (\mathrm{O}) + div(f_{a,Q}), \quad bD = (bQ) - (\mathrm{O}) + div(f_{b,Q}), \tag{11}$$

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

$$aD + bD = (aQ) + (bQ) - (\mathrm{O}) + div(f_{a,Q} \cdot f_{b,Q} \cdot g_{aQ,bQ}), \tag{12a}$$

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.

$$a(bD) = \sum_{i=0}^{a-1} (bQ) - a(\mathrm{O}) + div(f_{b,Q}^{a} \cdot f_{a,bQ}). \tag{12b}$$

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

$$(a+b)D = ((a+b)Q) - (\mathrm{O}) + div(f_{a+b,Q}), \tag{13a}$$

$$(ab)D = (abQ) - (\mathrm{O}) + div(f_{ab,Q}). \tag{13b}$$

we have the following relation.

$$f_{a+b,Q} = f_{a,Q} \cdot f_{b,Q} \cdot g_{aQ,bQ}, \quad f_{ab,Q} = f_{b,Q}{}^{a} \cdot f_{a,bQ} = f_{a,Q}{}^{b} \cdot f_{b,aQ}. \tag{14}$$

Miller's algorithm calculates $f_{s,Q}$ efficiently.

3. Main proposal

First, this section briefly goes over Miller's algorithm. Then, an improvement of t*wisted-Ate* pairing with BN curve of embedding degree 12 is proposed.

3.1 Introduction of Miller's algorithm

Several improvements for Miller's algorithm have been given. Barreto et al. proposed *reduced* Miller's algorithm. **Fig. 1** shows the calculation flow of *reduced* Miller's algorithm for $f_{s,P}(Q)$. It consists of functions shown in **Algorithm 1** and **Algorithm 2,** *see* **Table 1.**

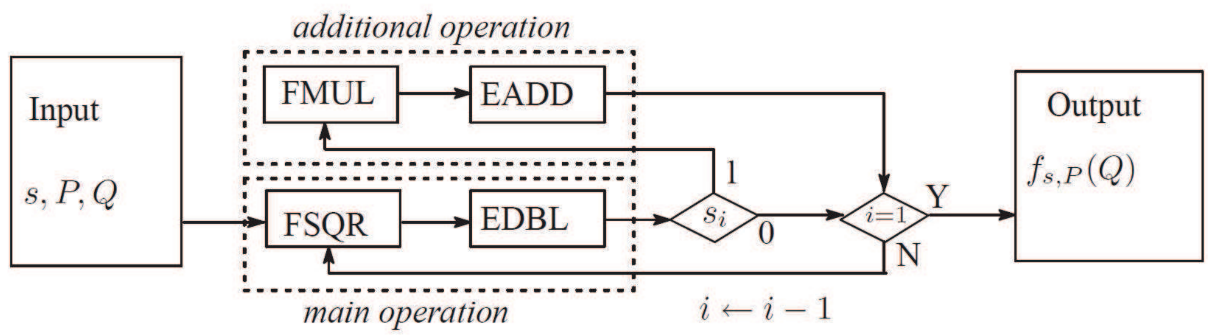


Fig. 1. Calculation flow of Miller's algorithm

In the case of *twisted-Ate* pairing, let $P \in G_1$, $Q \in G_2$ and s be given by Eq.(9), $f_{s,P}(Q)$ becomes an element in $F^*_{p^k}$. In **Fig. 1**, s_i is the i-th bit of the binary representation of s from the lower, FMUL and FSQR denote multiplication and squaring over $F_{p^{12}}$, EADD and EDBL denote elliptic curve addition and doubling over G_1. As shown in the algorithm, *main operation* is repeated $\lfloor \log_2 s \rfloor$ times but *additional operation* is only carried out when s_i is 1. Thus, the calculation cost of Miller's Algorithm can be reduced by reducing the number of *additional operations*.

Input:	$T \in G_1, Q \in G_2$
Output:	f, T
	FSQR
1.	$\lambda_{T,T} \leftarrow (3x_T^2)/(2y_T)$
2.	$l_{T,T}(Q) \leftarrow (x_Q - x_T)\lambda_{T,T} - (y_Q - y_T)$
3.	$f \leftarrow f^2 \cdot l_{T,T}(Q) / v_{T+T}(Q)$
4.	return f
	EDBL
5.	$x_{2T} \leftarrow \lambda_{T,T}^2 - 2x_T$
6.	$y_{2T} \leftarrow (x_T - x_{2T})\lambda_{T,T} - y_T$
7.	Return $T \leftarrow 2T$

Algorithm 1. FSQR and EDBL of Fig. 1

3.2 Proposed method

$f_{A,P} = f_{B,P}$ means $f_{A,P}^{(p^{12}-1)/r} = f_{B,P}^{(p^{12}-1)/r}$ in what follows, where $f_{A,P}$ and $f_{B,P}$ are the rational functions of divisors, respectively. Miller's algorithm of *twisted-Ate* pairing with BN curve calculates $f_{s,P}(Q)$, where s is given as

$$s = (t-1)^2 = 36\chi^3 - 18\chi^2 + 6\chi - 1 \bmod r. \tag{15}$$

Input:	$P \in G_1, Q \in G_2$
Output:	f, T
FMUL	
1.	$\lambda_{T,P} \leftarrow (y_P - y_T)/(x_P - x_T)$
2.	$l_{T,P}(Q) \leftarrow (x_Q - x_P)\lambda_{T,P} - (y_Q - y_P)$
3.	$f \leftarrow f \cdot l_{T,P}(Q) / v_{T+P}(Q)$
4.	return f
EADD	
5.	$x_{T+P} \leftarrow \lambda_{T,P}^2 - x_T - x_P$
6.	$y_{T+P} \leftarrow (x_P - x_{T+P})\lambda_{T,P} - y_P$
7.	return $T \leftarrow 2T$

Algorithm 2. FMUL and EADD of Fig. 1

s_i:	the i-th bit of the binary representation of s from the lower.
$l_{T,T}$:	the tangent line at T.
$l_{T,P}$:	the line passing through T and P.
v_{T+T}:	the vertical line passing through $2T$.
v_{T+P}	the vertical line passing through $T+P$.
$\lambda_{T,T}$:	the slope of the tangent line $l_{T,T}$.
$\lambda_{T,P}$:	the slope of the line $l_{T,P}$.

Table 1. Notations used in **Algorithms 1**, **2**, and **3**

$r(\chi)$	χ	Hw(s*)
254 Bits	$2^{62}+2^{46}+2^{29}$	83
	$2^{64}+2^{35}+2^{24}$	82
	$2^{62}+2^{55}+1$	36
	$-2^{62}-2^{41}-2^{23}$	43

* $s = (t-1)^2 \bmod r = 36\chi^3-18\chi^2+6\chi-1$

Table 2. χ of small Hamming weight that gives BN curve of 254 bits prime order

The proposed method calculates $f_{s,P}(Q)$ using the following relations:

$$p \equiv t - 1 = 6\chi^2 \bmod r, \tag{16a}$$

$$s \equiv 6\chi^2(6\chi - 3) + 6\chi - 1 \equiv p(6\chi - 3) + 6\chi - 1 \bmod r. \tag{16b}$$

Using χ of small Hamming weight, first calculate $f_{6\chi-3,P}(Q)$ and then calculate $f_{6\chi-1,P}(Q)$ by using the result of the preceding calculation. Then, by calculating $f_{p,(6\chi-3)P}(Q)$ for which Frobenius mapping is efficiently applied, the number of *additional operations* is substantially reduced. In detail, let $\chi' = 2\chi - 1$, calculate $f_{\chi',P}(Q)$ by Miller's algorithm. Then, calculate $f_{6\chi-3,P}(Q)$ as

$$f_{6\chi-3,P} = f_{\chi',P}^3 \cdot g_{\chi'P,\chi'P} \cdot g_{2\chi'P,\chi'P}. \tag{17}$$

Since 6 χ-1=(6 χ-3)+2, $f_{6\chi-1,P}(Q)$ is given as

$$f_{6\chi-1,P} = f_{6\chi-3,P} \cdot f_{2,P} \cdot g_{(6\chi-3)P,2P}. \tag{18}$$

Then, calculate $f_{(6\chi-3)\cdot 6\chi^2,P}$ by using $f_{6\chi-3,P}$. **Algorithm 3** shows Miller's algorithm whose initial value of f is f'. Though it can be calculated by **Algorithm 3** as

$$f_{(6\chi-3)\cdot 6\chi^2,P} = f_{6\chi^2,(6\chi-3)P} \,|_{f'=f_{(6\chi-3),P}}, \tag{19}$$

according to Eq.(16a), this paper calculates it by **Algorithm 3** as follows.

$$f_{(6\chi-3)\cdot 6\chi^2,P} = f^{6\chi^2}_{(6\chi-3),P} \cdot f_{6\chi^2,(6\chi-3)P} \,|_{f'=1} = f^{p}_{(6\chi-3),P} \cdot f_{6\chi^2,(6\chi-3)P} \,|_{f'=1} \tag{20}$$

Finally, we have

$$f_{6\chi^2(6\chi-3)+6\chi-1,P} = f_{(6\chi-1),P} \cdot f^{p}_{(6\chi-3),P} \cdot (f_{6\chi^2,(6\chi-3)P} \,|_{f'=1}) \cdot g_{(6\chi-1)P,(6\chi-3)P}. \tag{21}$$

The proposed method has the following advantages.
- χ of small hamming weight efficiently works.
- It can reduce a multiplication in $F_{p^{12}}$ at Step6 of **Algorithm 3** by Frobenius mapping.

Input:	$P \in G_1, Q \in G_2, f' \in F_{p^{12}}$
Output:	$f_{\chi,P'}(Q)$
1.	$f \leftarrow f', T \leftarrow P$
2.	For $i = \lfloor \log_2(s) \rfloor$ downto 1:
3.	$\quad f \leftarrow f^2 \cdot l_{T,T}(Q) / v_{T+T}(Q)$
4.	$\quad T \leftarrow 2T$
5.	$\quad$ If $s_i = 1$, then :
6.	$\qquad f \leftarrow f \cdot f' \cdot l_{T,P}(Q) / v_{T+P}(Q)$
7.	$\qquad T \leftarrow T + P$
8.	return f

Algorithm 3. Miller's Algorithm whose initial value of f is f'.

4. Experimental result

In order to show the efficiency of the proposed method, the authors simulated *twisted-Ate* pairing with BN curve of order $r \approx 2^{254}$. In this simulation, the authors used χ and BN curve shown in **Table 3. Table 4** shows the simulation result.

As a reference, **Table 5** shows timings of multiplication (mul), inversion (inv) in each subfield of $F_{p^{12}}$ and squaring (sqr) in $F_{p^{12}}$. According to **Table 4**, in the cases of $r \approx 2^{254}$, the proposed method reduced the calculation times of Miller's algorithm by 18.0%.

size of p, r	254 bits
BN curve	$y^2=x^3+10$
χ	$2^{64}+2^{35}+2^{24}$
Hw(s)	82
Hw(χ)	3

Table 3. Parameters of *twisted-Ate* pairing

p, r		254 bits
Miller's part	Conventional	14.5
	Proposed	11.8
final exponentiation		4.45
Total	Conventional	19.0
	Proposed	16.3
Elliptic curve scalar multiplication*	$G_1 \in E(F_p)$**	2.31
	$G_2 \in E'(F_{p^2})$	7.01

* Average timings with random scalars and exponents of

** *Projective coordinates* are used.

Remark : Pentium4 (3.6GHz), C language, and GMP 4.2.2 library are used.

Table 4. Comparison of timings [ms]

F_p	mul	0.65
	inv	8.43
F_{p^2}	mul	1.65
	inv	11.4
F_{p^4}	mul	4.39
	inv	19.6
F_{p^6}	mul	7.78
	inv	32.4
$F_{p^{12}}$	mul	21.6
	inv	80.3
	sqr	19.7

Remark: Pentium4 (3.6GHz), C language, and GMP 4.2.2 library are used.

Table 5. Timings of operations in subfield (p: 254 bit prime number)[μs]

5. Conclusion

This paper has proposed an improvement of *twisted-Ate* pairing with Barreto-Naehrig curve so as to efficiently use Frobenius mapping with respect to prime field. Then, this paper showed some simulation result by which it was shown that the improvement accelerated *twisted-Ate* pairing *including final exponentiation* about 14.1%.

6. Acknowledgement

This work is supported by ``Strategic Information and Communications R&D Promotion Programme" from the Ministry of Internal Affairs and Communications, Japan.

7. References

Bailey, D. & Paar, C. (1998). Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms, *Proceedings of CRYPT'98*, pp.472-485, ISBN: 978-3-540-64892-5, USA, August 1998, Springer-Verlag, Santa Barbara, California

Barreto, P. S. L. M. & Naehrig, M. (2006). Pairing-Friendly Elliptic Curves of Prime Order, *Proceedings of SAC2005*, pp. 319-331, ISBN: 978-3-540-33108-7, Canada, August 2005, Springer-Verlag, Kingston

Boneh, D.; Lynn, B. & Shacham, H. (2001). Short signatures from the Weil pairing, *Proceedings of Asiacrypt2001,* pp. 514-532, ISBN: 978-3-540-42987-6, Australia, December 2001, Springer-Verlag, Gold Coast

Cohen, H. & Frey, G. (2005). *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman & Hall CRC, ISBN: 1584885181

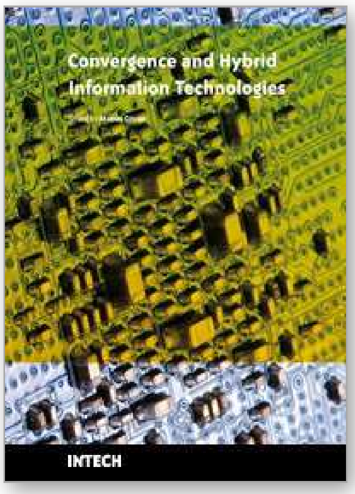
Devegili, A. J.; Scott, M. & Dahab, R. (2007). Implementing Cryptographic Pairings over Barreto-Naehrig Curves, *Proceedings of Pairing2007*, pp. 197-207, ISBN: 978-3-540-73488-8, Japan, July 2007, Springer-Verlag, Tokyo

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

Hess, F.; Smart, N.; & Vercauteren, F. (2006). The Eta Pairing Revisited, *IEEE Trans. Information Theory*, Vol. 52, No. 10, October 2006, pp. 4595-4602, ISSN: 0018-9448

Matsuda, S.; Kanayama, N; Hess, F.; & Okamoto, E. (2007). Optimised Versions of the Ate and Twisted Ate Pairings, *Proceedings of 11th IMA International Conference*, pp. 302-312, ISBN: 978-3-540-77272-9, UK, December 2007, Springer-Verlag, Cirencester.

Nakanishi, T. & Funabiki, N. (2005). Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps, *Proceedings of Asiacrypt2005,* pp. 443-454, ISBN: 978-3-540-30684-9, India, December 2005, Springer-Verlag, Chennai



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