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

Yumi Sakemi, Hidehiro Kato, Yasuyuki Nogami, and Yoshitaka Morikawa

Graduate School of Natural Science and Technology, Okayama University
3-1-1, Tsushima-naka, Okayama, Okayama 700-8530, Japan
E-mail: {sakemi, kato, nogami, morikawa} @trans.cne.okayama-u.ac.jp

Abstract

This paper proposes 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 shows some simulation results by which it is shown that the improvement accelerates twisted–Ate pairing.

1 Introduction

Recently, pairing–based cryptographic applications such as ID-based cryptography [1] and group signature scheme [2] have received much attention. In order to make it practical, various pairings such as Ate pairing [3], subfield–twisted pairing [4] and subfield–twisted Ate pairing [5] have been proposed. This paper focuses on twisted–Ate pairing with Barreto–Naehrig (BN) curve [8]. 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 \( \chi \) as follows.

\[
\begin{align*}
p(\chi) & = 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1, \quad (1a) \\
r(\chi) & = 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1, \quad (1b) \\
t(\chi) & = 6\chi^2 + 1. \quad (1c)
\end{align*}
\]

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 \( f_{(t-1)^2} \mod r, P, Q \), where \( P \) and \( Q \) are rational points in certain subgroups of order \( r \) in \( E(\mathbb{F}_p) \) and \( E(\mathbb{F}_p^{12}) \), respectively. In this case, \( (t-1)^2 \mod r \) becomes

\[
(t-1)^2 \mod r = 36\chi^3 - 18\chi^2 + 6\chi - 1, \quad (2)
\]

it corresponds to the number of iterations of Miller’s algorithm. In addition, the hamming weight of \( (t-1)^2 \mod r \) 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:

\[
\begin{align*}
p & \equiv t - 1 = 6\chi^2 \pmod{r}, \quad (3a) \\
(1-t)^2 & \equiv 36\chi^3 - 18\chi^2 + 6\chi - 1 \\
& \equiv 6\chi^2(6\chi - 3) + 6\chi - 1 \\
& \equiv ((6\chi - 3)+6\chi - 1) \pmod{r}. \quad (3b)
\end{align*}
\]

First, calculate \( f_{0(\chi-3),d}(Q) \) by Miller’s algorithm, then calculate \( f_{0(\chi-1),d}(Q) \) by using the result of the preceding calculation. Then, using the result, calculate \( f_{p,0(\chi-3),d}(Q) \) for which Frobenius mapping in extension field \( \mathbb{F}_p^{12} \) with respect to prime field \( \mathbb{F}_p \) is efficiently applied. In detail, since \( p \) is the characteristic of \( \mathbb{F}_p^{12} \), Frobenius mapping does not need any arithmetic operations when the extension field has fast Frobenius mapping such as OE [6]. 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. \( \mathbb{F}_p^k \) denotes \( k \)-th extension field over \( \mathbb{F}_p \) and \( \mathbb{F}_p^k \) denotes its multiplicative group. \( X \mid Y \) and \( X \nmid Y \) mean that \( X \) divides and does not divide \( Y \), respectively.

2 Fundamentals

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

2.1 Elliptic Curve and BN curve

Let \( \mathbb{F}_p \) be prime field and \( E \) be an elliptic curve over \( \mathbb{F}_p \). \( E(\mathbb{F}_p) \) that is the set of rational points on the curve, including the infinity point \( O \), forms an additive Abelian group.
Let \( \#E(\mathbb{F}_p) \) be its order, consider a large prime number \( r \) 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 a pairing such as Tate and Ate pairings on \( E(\mathbb{F}_{p^k}) \). Usually, \( \#E(\mathbb{F}_p) \) is written as

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

where \( t \) is the Frobenius trace of \( E(\mathbb{F}_p) \). Characteristic \( p \) and Frobenius trace \( t \) of Barreto–Naehrig (BN) curve [8] are given by using an integer variable \( \chi \) as Eqs. (1). In addition, BN curve \( E \) is written as

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

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

### 2.2 Twisted Ate Pairing with BN curve

Let \( \phi \) be Frobenius endomorphism, i.e.,

\[
\phi : E(\mathbb{F}_{p^2}) \rightarrow E(\mathbb{F}_{p^2}) : (x, y) \mapsto (x^{p}, y^{p}) \tag{6}
\]

Then, in the case of BN curve, let \( \mathbb{G}_1 \) and \( \mathbb{G}_2 \) be

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

\[
\mathbb{G}_2 = E[r] \cap \text{Ker} ([q] \phi^2 - [1]), \tag{7b}
\]

where \( q_0 \) is a primitive \( 6 \)-th root of unity and let \( P \in \mathbb{G}_1 \) and \( Q \in \mathbb{G}_2 \), twisted–Ate pairing \( \alpha(\cdot, \cdot) \) is defined as

\[
\alpha(\cdot, \cdot) : \begin{cases} \mathbb{G}_1 \times \mathbb{G}_2 & \rightarrow \mathbb{F}_{p^2}^*/(\mathbb{F}_{p^2}^*)^r \\ (P, Q) & \mapsto f_{s, P}(Q)^{r(\chi - 1)/r}. \end{cases} \tag{8}
\]

\( A = f_{s, P}(Q) \) is usually calculated by Miller’s algorithm[5], then so-called final exponentiation \( A^{(p^2 - 1)/r} \) follows. The number of calculation loops of Miller’s algorithm of twisted–Ate pairing with BN curve is determined by \( \lceil \log_2 s \rceil \), where \( s \) is, in this case, given by

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

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

### 2.3 Divisor

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

\[
D = (Q) - (\mathcal{O}) = (Q) - (\mathcal{O}) + \text{div}(1). \tag{10}
\]

For scalars \( a, b \in \mathbb{Z} \), let \( aD \) and \( bD \) be written as

\[
aD = (aQ) - (\mathcal{O}) + \text{div}(f_{a,Q}), \tag{11a}
\]

\[
bD = (bQ) - (\mathcal{O}) + \text{div}(f_{b,Q}), \tag{11b}
\]

where \( f_{s,Q} \) and \( f_{h,Q} \) are the rational functions for \( aD \) and \( bD \), respectively. Then, addition for divisors is given as

\[
ad + bd = (aQ) + (bQ) - (\mathcal{O}) + \text{div} (f_{a,Q} \cdot f_{b,Q} \cdot g_{a,b,Q}), \tag{12a}
\]

where \( g_{a,b,Q} = l_{a,b,Q} / v_{a,b,Q} \). Thus, let \( (a + b)D \) be written as

\[
(a + b)D = ((a + b)Q) - (\mathcal{O}) + \text{div} (f_{a+b,Q}), \tag{13a}
\]

we have the following relation.

\[
\begin{align*}
    f_{a+b,Q} &= f_{a,Q} \cdot f_{b,Q} \cdot g_{a,b,Q} \cdot , \\
    f_{a+b,Q} &= f_{a,Q}^b \cdot f_{b,Q} \cdot g_{a,b,Q}. \tag{14b}
\end{align*}
\]

Miller’s algorithm calculates \( f_{s,Q} \) efficiently.

### 3 Main Proposal

First, this section briefly goes over Miller’s algorithm. Then, an improvement of twisted–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.

In the case of twisted–Ate pairing, let \( P \in \mathbb{G}_1 \), \( Q \in \mathbb{G}_2 \) and \( s \) be given by Eq.(9), \( f_{s, P}(Q) \) becomes an element in \( \mathbb{F}_{p^2} \). 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 \( \mathbb{F}_{p^2} \), EADD and EDBL denote elliptic curve addition and doubling over \( \mathbb{G}_1 \). As shown in the algorithm, main operation is repeated \( \lceil \log_2 s \rceil \) 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 the number of additional operations.
is given as

for which Frobenius mapping is efficiently

36

in what follows, where f_{AP} and f_{BP} are the rational functions of divisors, respectively. Miller’s algorithm of twisted–Ate pairing with BN curve calculates f_{s,P}, where s is given as

\[ s \equiv (t - 1)^2 \]
\[ \equiv 36\chi^3 - 18\chi^2 + 6\chi - 1 \pmod{r} \quad (15) \]
\[ \equiv 6\chi^2(6\chi^2 - 3) + 6\chi - 1 \]
\[ \equiv p(6\chi^2 - 3) + 6\chi - 1 \pmod{r} \quad (16) \]

The proposed method calculates f_{s,P} using the following relations:

\[ p \equiv t - 1 = 6\chi^2 \pmod{r}, \quad (17a) \]

\[ s_t \text{–th bit of the binary representation of } s \text{ from the lower.} \]
\[ l_{T,T} \text{– the tangent line at } T. \]
\[ l_{T,P} \text{– the line passing through } T \text{ and } P. \]
\[ v_{T+T} \text{– the vertical line passing through } 2T. \]
\[ v_{T+P} \text{– the vertical line passing through } T + P. \]
\[ \lambda_{T,T} \text{– the slope of the tangent line } l_{T,T}. \]
\[ \lambda_{T,P} \text{– the slope of the line } l_{T,P}. \]

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

\[ f_{(6\chi^2-3),P} = f_{\chi',P} \cdot g_{\chi',P} \cdot g_{2\chi',P} \cdot P. \quad (18) \]

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

\[ f_{(6\chi^2-1),P} = f_{(6\chi^2-3),P} \cdot f_{2\chi,P} \cdot g_{(6\chi^2-3)P} \cdot P. \quad (19) \]

Then, calculate \( f_{(6\chi^2-3),P} \) by using \( f_{(6\chi^2-3),P} \). Algorithm 3 shows Miller’s algorithm whose initial value of \( f \)
Algorithm 3: Miller’s Algorithm whose initial value of $f$ is $f'$. 

| Input: $P \in \mathbb{G}_1$, $Q \in \mathbb{G}_2$, $f' \in \mathbb{F}_p^{1/2}$ |
| Output: $f_{x',p'}(Q)$ |
| 1. $f \leftarrow f'$, $T \leftarrow P$. |
| 2. For $i = \lfloor \log_2(s) \rfloor$ downto 1: |
| 3. $f \leftarrow f^2 \cdot I_{T,T}(Q) / \nu_{T+T}(Q)$. |
| 4. $T \leftarrow 2T$. |
| 5. If $s_1 = 1$, then: |
| 6. $f \leftarrow f \cdot I_{T,p}(Q) / \nu_{T+P}(Q)$. |
| 7. $T \leftarrow T + P$. |
| 8. Return $f$. |

is $f'$. Though it can be calculated by Algorithm 3 as

$$f_{(6\chi-3)6\chi^2,P} = f_{(6\chi-3),P} \cdot f_{6\chi^2,6\chi-3,P}^{|f_1-1|}$$

(20)

according to Eq.(17a), this paper calculates it by Algorithm 3 as follows.

$$f_{(6\chi-3)6\chi^2,P} = f_{(6\chi-3),P} \cdot f_{6\chi^2,6\chi-3,P}^{|f_1-1|}$$

$$= f_{(6\chi-3),P} \cdot f_{6\chi^2,6\chi-3,P}^{|f_1-1|}$$

Finally, we have

$$f_{6\chi^2(6\chi-3),6\chi-1,P} = f_{6\chi^2,6\chi-3,P} \cdot f_{6\chi^1,6\chi-1,P}^{|f_1-1|}$$

$$= g_{(6\chi-1),6\chi-3,P}^{|f_1-1|}$$

(21)

(22)

The proposed method has the following advantages.

- $\chi$ of small hamming weight efficiently works.
- It can reduce a multiplication in $\mathbb{F}_p^{1/2}$ at Step6 of Algorithm 3 by Frobenius mapping.

4 Simulation

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 $\chi$ 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 $\mathbb{F}_p^{1/2}$ and squaring(sqr) in $\mathbb{F}_p^{1/2}$. 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%.

### Table 3. parameters of twisted–Ate pairing

| size of $p, r$ | 254 bit |
|---------------|---------|
| BN curve      | $y^2 = x^2 + 10$ |
| $\chi$        | $x^2 + 2^{135} + 2^{24}$ |
| Hw(s)         | 82 |
| Hw(\chi)      | 3 |

### Table 4. comparison of timings[ms]

| $p, r$ | 254bit |
|--------|---------|
| Miller part | conventional | proposed |
| final exponentiation | 4.45 | 1.8 |
| total | 19.0 | 16.3 |

*Average timings with random scalars and exponents of $\lfloor \log_2(r) \rfloor$ bit.
**Projective coordinates are used.
Remark: Pentium4 (3.6GHz), C language, and GMP [9] are used.

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 in 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.

References

[1] R. Sakai, K. Ohgishi, and M. Kasahara, “Cryptosystems based on pairing”, SCIS2000, Jan. 2000.

[2] T. Nakanishi, and N. Funabiki, “Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps”, ASIACRYPT 2005, LNCS, Vol. 3788, Dec. 2005, pp. 533-548.
Table 5. Timings of operations in subfield
\((p: 254 \text{ bit prime number}) [\mu s]\)

| Subfield | \(\text{mul}\) | \(\text{inv}\) |
|----------|--------------|--------------|
| \(F_p\)  | 0.65         | 8.43         |
| \(F_p^2\)| 1.65         | 11.4         |
| \(F_p^3\)| 4.39         | 19.6         |
| \(F_p^4\)| 7.78         | 32.4         |
| \(F_p^{15}\)| 21.6       | 80.3         |
|          | 19.7         |              |

Remark: Pentium4 (3.6GHz), C language, and GMP [9] are used.

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

[4] S. Matsuda, N. Kanayama, F. Hess, E. Okamoto. “Optimised Versions of the Ate and Twisted Ate Pairings,” *Proc. of Eleventh IMA International Conference on Cryptography and Coding, LNCS 4887*, 2007, p. 302-312.

[5] A. J. Devegili, M. Scott, and R. Dahab, “Implementing Cryptographic Pairings over Barreto-Naehrig Curves,” *LNCS, Vol. 4575*, 2007, pp. 197-207.

[6] D. Bailey and C. Paar, “Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms,” *Proc. of Asiacrypt2000, LNCS 1976*, 2000, pp. 248-258.

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

[8] P. S. L. M. Barreto, and M. Naehrig, “Pairing-Friendly Elliptic Curves of Prime Order”, *Proc. of SAC 2005, LNCS, Vol. 3897*, 2006, pp. 319-331.

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

[10] F. Hess, N. Smart, and F. Vercauteren, “The Eta Pairing Revisited”, *IEEE Trans. Inf. Theory*, 2006, pp. 4595-4602.

[11] A. J. Devegili, M. Scott, and R. Dahab, “Implementing Cryptographic Pairings over Barreto-Naehrig Curves”, *LNCS, Vol. 4575*, 2007, pp. 197-207.