BLS曲線におけるPseudo 8-Sparse乗算を用いた効率的なOptimal-Ateペアリングの実装

カンダカル エムディアルアミン[1]　小野 寛享[1]　南條 由紀[2]　日下 卓也[1]　野上 保之[1]

概要：本稿では、BLS 曲線における Pseudo 8-Sparse 乗算を用いた効率的な Miller のアルゴリズムの実装方法について記す。近年新たな離散対数問題の解法アルゴリズム (exTNFS) が発表されたため，本稿ではこれに対応する最新のパラメータを用いて、BLS 曲線と KSS 曲線について効率的な Optimal-Ate ペアリングの実装を行った。その結果、一回のペアリングにかかる時間は BN 曲線よりも BLS 曲線のほうが高速に実装することができた。

キーワード：ペアリング暗号, 計算効率化

Efficient Optimal-Ate Pairing on BLS-12 Curve Using Pseudo 8-Sparse Multiplication

Md. Al-Amin Khandaker[1]　Hirotaka Ono[1]　Yuki Nanjo[2]　Takuya Kusaka[1]　Yasuyuki Nogami[1]

Abstract: This paper shows an efficient Miller's algorithm implementation technique by applying pseudo 8-sparse multiplication over Barreto-Lynn-Scott (BLS12) curve of embedding degree 12. The recent development of exTNFS algorithm for solving discrete logarithm problem urges researchers to update parameter for pairing-based cryptography. Therefore, this papers applies the most recent parameters and also shows a comparative implementation of optimal-Ate pairing between BLS12 curve and Barreto-Naehrig (BN) curve. The result finds that pairing in BLS12 curve is faster than BN curve.

Keywords: pairing-based cryptography, efficient calculation

1. Introduction

At the beginning of this century, Sakai et al. [21] and Joux [12] independently proposed a cryptosystem that has unlocked many novel ideas to cryptography researchers. Many researchers tried to find out security protocol that exploits pairings to remove the need of certification by a trusted authority. In this consequence, several ingenious pairing based encryption scheme such as ID-based encryption scheme by Boneh and Franklin [6] and group signature authentication by Nakanishi et al. [19] has come into the focus. In such outcome, Ate-based pairings such as Ate [7], Optimal-ate [24], twisted Ate [16] and χ-Ate [20] pairings and their applications in cryptosystems have caught much attention since they have achieved quite efficient pairing calculation. But it has always been a challenge for researchers to make pairing calculation more efficient for being used practically as pairing calculation is regarded as quite a time-consuming operation.

Generally, a pairing is a bilinear map e typically defined as $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$, where $\mathbb{G}_1$ and $\mathbb{G}_2$ are additive

[1] 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University
[2] 岡山大学工学部電気通信系学科
Dept. of Electrical and Communication Engineering, Okayama University

cyclic sub-groups of order r on a certain elliptic curve E over a finite extension field $\mathbb{F}_{p^k}$ and $\mathbb{G}_3$ is a multiplicative cyclic group of order r over $\mathbb{F}^*_{p^k}$. This paper chooses an asymmetric variant of pairing named as Optimal-Ate [24] with Barreto-Lynn-Scott (BLS) [4] pairing friendly curve of embedding degree $k = 12$ named as BLS-12.

Acceleration of Optimal-Ate pairing depends not only on the optimization of Miller algorithm's loop parameter but also on efficient elliptic curve arithmetic operation and efficient final exponentiation. This paper has proposed a *pseudo 8-sparse multiplication* to accelerate Miller's loop calculation in the BLS-12 curve by utilizing the property of rational point groups. In addition, this paper has shown an enhancement of the elliptic curve addition and doubling calculation in Miller's algorithm by applying implicit mapping of its sextic twisted isomorphic group.

The recent development of NFS by Kim and Barbulescu [15] requires updating the parameter selection for all the existing pairings over the well know pairing friendly curve families such as BN [5], BLS [4] and KSS [13]. Barbulescu and Sylvain [3] has proposed new parameters that for 128-bit security level and found BLS-12 is the most efficient choice for Optimal-Ate pairing than well studied BN curve. Therefore the authors focus on the efficient implementation of the BLS-12 curve for Optimal-Ate pairing by applying most recent parameters. The authors also applied final exponentiation algorithm of [10] and compared the experimental implementation result with BN with similar implementation technique.

The simulation result shows that the given *pseudo 8-sparse multiplication* for BLS-12 achieved more efficient Miller's loop calculation for optimal-Ate pairing than BN curve.

Related Works.

Aranha et al. [1], Section 4 and Costello et al. [8] have well optimized the Miller's algorithm in Jacobian coordinates by 6-sparse multiplication [*1] for BN curve. Mori et al. [18] and Khandaker et al. [14] have shown a specific type of sparse multiplication for BN curve and KSS-18 curve respectively where both of the curves supports sextic twist. It is found that pseudo 8-sparse was clearly efficient than 7-sparse and 6-sparse in Jacobian coordinates. The authors have extended the previous works for the sextic twisted BLS-12 curve.

[*1] 6-Sparse refers the state when in a vector (multiplier/multiplicand), among the 12 coefficients 6 of them are zero.

2. Fundamentals

2.1 BLS-12 Curve

Barreto, Lynn and Scott propose polynomial parameterizations by an integer variable u for certain complete pairing-friendly curve families for specific embedding degrees [4]. The target curve of this paper is such pairing-friendly curve, usually called BLS-12 of embedding degree $k = 12$, defined over extension field $\mathbb{F}_{p^{16}}$ as follows:

$$E/\mathbb{F}_{p^{12}} : y^2 = x^3 + b, \quad (b \in \mathbb{F}_p) \text{ and } b \neq 0, \tag{1}$$

where $x, y \in \mathbb{F}_{p^{12}}$. Similar to other pairing-friendly curves, *characteristic* p, *Frobenius trace* t and *order* r of this curve are given by the following polynomials of integer variable u also known as *mother parameter*.

$$p(u) = (u-1)^2(u^4 - u^2 + 1)/3 + u, \tag{2a}$$

$$r(u) = (u^4 - u^2 + 1) \tag{2b}$$

$$t(u) = u + 1, \tag{2c}$$

where u is such that $6|(p-1)$. The total number of rational points $\#E(\mathbb{F}_p)$ is given by Hasse's theorem as, $\#E(\mathbb{F}_p) = p + 1 - t$. When the definition field is the k-th degree extension field $\mathbb{F}_{p^k}$, rational points on the curve E also forms an additive Abelian group denoted as $E(\mathbb{F}_{p^k})$.

2.2 Extension Field Arithmetic and Towering

In extension field arithmetic, higher level computations can be improved by towering. In towering, higher degree extension field is constructed as a polynomial of lower degree extension fields. In some previous works, such as Bailey et al. [2] explained tower of extension by using irreducible binomials. In what follows, Let $6|(p-1)$, where p is the characteristics of BLS-12 curve and -1 is a quadratic and cubic non-residue in $\mathbb{F}_p$. Since BLS-12 curve is defined over $\mathbb{F}_{p^{12}}$, this paper has represented extension field $\mathbb{F}_{p^{12}}$ as a tower of sub-fields to improve arithmetic operations.

$$\begin{cases} \mathbb{F}_{p^2} = \mathbb{F}_p[\alpha]/(\alpha^2 + 1), \\ \mathbb{F}_{p^6} = \mathbb{F}_{p^2}[\beta]/(\beta^3 - (\alpha + 1)), \\ \mathbb{F}_{p^{12}} = \mathbb{F}_{p^6}[\gamma]/(\gamma^2 - \beta). \end{cases} \tag{3}$$

Extension Field Arithmetic of $\mathbb{F}_{p^{12}}$

Among the arithmetic operations multiplication, squaring and inversion are regarded as expensive operation than addition/subtraction. The calculation cost, based on number of prime field multiplication M_p and squaring S_p is given in Table 1. The algorithms for extension field operation are implemented from [9]. The arithmetic operations in $\mathbb{F}_p$ are denoted as M_p for a multiplication, S_p for

a squaring, I_p for an inversion and m with suffix denotes multiplication with basis element.

2.3 Optimal-Ate Pairing on BLS-12 Curve

In the context of pairing on the targeted pairing-friendly curves, two additive rational point groups $\mathbb{G}_1, \mathbb{G}_2$ and a multiplicative group $\mathbb{G}_3$ of order r are considered. $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ are defined as follows:

$$\begin{aligned}\mathbb{G}_1 &= E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\pi_p - [1]),\\ \mathbb{G}_2 &= E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\pi_p - [p]),\\ \mathbb{G}_3 &= \mathbb{F}_{p^k}/(\mathbb{F}_{p^k})^r,\\ e &: \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3, \end{aligned} \tag{4}$$

here e denotes Optimal-Ate pairing [24]. $E(\mathbb{F}_{p^k})[r]$ denotes rational points of order r and $[i]$ denotes i times scalar multiplication for a rational point. π_p denotes the Frobenius map given as $\pi_p : (x, y) \mapsto (x^p, y^p)$.

In the case of BLS-12, the above $\mathbb{G}_1$ is just $E(\mathbb{F}_p)$. In what follows, rest of this paper considers $P \in \mathbb{G}_1 \subset E(\mathbb{F}_p)$ and $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{12}})$ for BLS-12 curve. Optimal-Ate pairing $e(Q, P)$ is given as follows:

$$e(Q, P) = f_{u,Q}(P)^{\frac{p^{12}-1}{r}}, \tag{5}$$

where $f_{u,Q}(P)$ is the Miller's algorithm's result and $\lfloor \log_2(u) \rfloor$ is the loop length. The bilinearity of Ate pairing is satisfied after calculating the final exponentiation $\frac{p^{12}-1}{r}$.

The generalized calculation procedure of Opt-Ate pairing is shown in Alg. 1. In what follows, the calculation steps from 1 to 5, shown in Alg. 1, is identified as Miller's Algorithm and step 6 is the final exponentiation. Steps 3 and 5 are the line evaluation together with elliptic curve doubling (ECD) and addition (ECA) inside the Miller's loop. These line evaluation steps are the focus point of this paper for acceleration. The authors extended the work of [18],[14] for BLS-12 curve to calculate *pseudo 8-sparse multiplication* described in Sect. 3. The ECA and ECD are also calculated efficiently in the twisted curve. Step 6, FE is calculated by applying Ghammam et al.'s final exponentiation algorithm [10].

Algorithm 1: Optimal Ate pairing on BLS-12 curve

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

Output: (Q, P)

1 $f \leftarrow 1, T \leftarrow Q'$

2 **for** $i = \lfloor \log_2(u) \rfloor$ **downto** 1 **do**

3 $\quad f \leftarrow f^2 \cdot l_{T,T}(P)$, $T \leftarrow [2]T$

4 $\quad$ **if** $u[i] = 1$ **then**

5 $\quad\quad f \leftarrow f \cdot l_{T,Q'}(P)$, $T \leftarrow T + Q'$

6 $f \leftarrow f^{\frac{p^{12}-1}{r}}$

7 **return** f

2.4 Sextic Twist of BLS-12 Curve

In the context of Optimal-Ate, there exists a *twisted curve* with a group of rational points of order r, isomorphic to the group where rational point $Q \in E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\pi_p - [p])$ belongs to. This sub-field isomorphic rational point group includes a twisted point of Q, typically denoted as $Q' \in E'(\mathbb{F}_{p^{k/d}})$, where k is the embedding degree and d is the twist degree.

Since points on the twisted curve are defined over a smaller field than $\mathbb{F}_{p^k}$, therefore ECA and ECD becomes faster. However, when required in the Miller's algorithm's line evaluation, the points can be quickly mapped to points on $E(\mathbb{F}_{p^k})$. Since the pairing-friendly BLS-12 [4] curve has CM discriminant of $D = 3$ and $6|k$, therefore sextic twist is available. Let $(\alpha+1)$ be a certain quadratic and cubic non residue in $\mathbb{F}_{p^2}$. The sextic twisted curve E_b' of curve E_b and their isomorphic mapping ψ_6 are given as follows:

$$\begin{aligned} E_b' &: y^2 = x^3 + b(\alpha + 1), \quad b \in \mathbb{F}_p,\\ \psi_6 &: E_b'(\mathbb{F}_{p^2})[r] \longmapsto E_b(\mathbb{F}_{p^{12}})[r] \cap \mathrm{Ker}(\pi_p - [p]),\\ &\quad (x, y) \longmapsto ((\alpha+1)^{-1} x\beta^2, (\alpha+1)^{-1} y\beta\gamma). \end{aligned} \tag{6}$$

where $\mathrm{Ker}(\cdot)$ denotes the kernel of the mapping and π_p denotes Frobenius mapping for rational point.

Table 2 shows a the vector representation of $Q = (x_Q, y_Q) = ((\alpha+1)^{-1} x_{Q'}\beta^2, (\alpha+1)^{-1} y_{Q'}\beta\gamma) \in \mathbb{F}_{p^{12}}$ according to the given towering in (3). Here, $x_{Q'}$ and $y_{Q'}$ are the coordinates of rational point Q' on sextic twisted curve E' defined over $\mathbb{F}_{p^2}$.

3. Proposal Overview

Before going to the details, the overall procedure can be described as follows:

(1) First we define the line equation for rational point $P \in E(\mathbb{F}_p)$ and Q', T' of sextic twisted curve $E'(\mathbb{F}_{p^2})$.

Table 1 Number of arithmetic operations in $\mathbb{F}_{p^{12}}$ based on (3)

$M_{p^2} = 3M_p + 5A_p + 1m_\alpha \to 3M_p$	$S_{p^2} = 2S_p + 3A_p \to 2S_p$
$M_{p^6} = 6M_{p^2} + 15A_{p^2} + 2m_\beta \to 18M_p$	$S_{p^6} = 2M_{p^2} + 3S_{p^2} + 9A_{p^2} + 2m_\beta \to 12S_p$
$M_{p^{12}} = 3M_{p^6} + 5A_{p^6} + 1m_\gamma \to 54M_p$	$S_{p^{12}} = 2M_{p^6} + 5A_{p^6} + 2m_\gamma \to 36S_p$

Table 2 Vector representation of $Q = (x_Q, y_Q) \in \mathbb{F}_{p^{12}}$

	1	α	β	$\alpha\beta$	β^2	$\alpha\beta^2$	γ	$\alpha\gamma$	$\beta\gamma$	$\alpha\beta\gamma$	$\beta^2\gamma$	$\alpha\beta^2\gamma$
x_Q	0	0	0	0	b_4	b_5	0	0	0	0	0	0
y_Q	0	0	0	0	0	0	0	0	b_8	b_9	0	0

(2) Next we obtain more sparse form by multiplying y_P^{-1} with line equations obtained at step 1.

(3) To reduce the computational overhead introduced in step 2, we obtain an isomorphic map of $P \mapsto \bar{P}$ and same map for $Q \mapsto \bar{Q}$ defined over curve $\bar{E}$.

(4) $\bar{Q} \in \bar{E}(\mathbb{F}_{p^{12}})$ is isomorphic to E, however it's sextic twisted $\bar{Q}$ defined over the curve $\bar{E}(\mathbb{F}_{p^2})$ is not isomorphic. Therefore, we again obtain the twisted map of $\bar{Q} \in \bar{E}(\mathbb{F}_{p^{12}})$ to $\bar{Q}'$, defined over $\bar{E}'(\mathbb{F}_{p^2})$.

(5) The mapping of step 2 and 3 reduces the overhead computation and help us to achieve pseudo 8-sparse multiplication.

Obtaining line equations

Let us consider $T = (\gamma x_{T'}, \gamma\omega y_{T'})$, $Q = (\gamma x_{Q'}, \gamma\omega y_{Q'})$ and $P = (x_P, y_P)$, where $x_p, y_p \in \mathbb{F}_p$ be given in affine coordinates on the curve $E(\mathbb{F}_{p^{12}})$ such that $T' = (x_{T'}, y_{T'})$, $Q' = (x_{Q'}, y_{Q'})$ are in the twisted curve E' defined over $\mathbb{F}_{p^2}$. Let the elliptic curve doubling of $T+T = R(x_R, y_R)$. The 7-sparse multiplication for BLS-12 can be derived as follows.

$$\begin{aligned} l_{T,T}(P) &= (y_p - y_{T'}(\alpha+1)^{-1}\beta\gamma) - \\ &\lambda_{T,T}(x_P - x_{T'}(\alpha+1)^{-1}\beta^2), \quad \text{when } T = Q, \\ \lambda_{T,T} &= \tfrac{3x_{T'}^2\beta\gamma}{2y_{T'}\beta^2} = \lambda'_{T,T}\tfrac{\gamma}{\beta} = \lambda'_{T,T}(\alpha+1)^{-1}\beta^2\gamma. \end{aligned} \tag{7}$$

The line evaluation and ECD are obtained as follows:

$$\begin{aligned} l_{T,T}(P) &= y_p + (\lambda'_{T,T}x_{T'} - y_{T'})(\alpha+1)^{-1}\beta\gamma \\ &\quad -\lambda'_{T,T}x_P(\alpha+1)^{-1}\beta^2\gamma, \\ x_{2T'} &= ((\lambda'_{T,T})^2 - 2x_{T'})(\alpha+1)^{-1}\beta^2, \\ y_{2T'} &= ((x_{T'} - x_{2T'})\lambda'_{T,T} - y_{T'})(\alpha+1)^{-1}\beta\gamma. \end{aligned}$$

The above calculations can be optimized as follows:

$$\begin{aligned} A = \tfrac{1}{2y_{T'}}, B = 3x_{T'}^2, C = AB, D = 2x_{T'}, \\ x_{2T'} = C^2 - D, E = Cx_{T'} - y_{T'}, \\ y_{2T'} = E - Cx_{2T'}, \\ l_{T',T'}(P) = y_P + (\alpha+1)^{-1}E\beta\gamma - \\ (\alpha+1)^{-1}Cx_P\beta^2\gamma, \end{aligned} \tag{8a}$$

$$y_P^{-1}l_{T',T'}(P) = 1 + (\alpha+1)^{-1}Ey_P^{-1}\beta\gamma - (\alpha+1)^{-1}Cx_Py_P^{-1}\beta^2\gamma. \tag{8b}$$

The elliptic curve addition phase ($T \neq Q$) and line evaluation of $l_{T,Q}(P)$ can also be optimized similar to the above procedure. Let the elliptic curve addition of $T + Q = R(x_R, y_R)$.

$$\begin{aligned} l_{T,Q}(P) &= (y_p - y_{T'})(\alpha+1)^{-1}\beta\gamma - \\ &\lambda_{T,Q}(x_P - x_{T'})(\alpha+1)^{-1}\beta^2, \quad T \neq Q, \\ \lambda_{T,Q} &= \tfrac{(y_{Q'} - y_{T'})(\alpha+1)^{-1}\beta\gamma}{(x_{Q'} - x_{T'})(\alpha+1)^{-1}\beta^2} = \lambda'_{T,Q}(\alpha+1)^{-1}\beta^2\gamma, \\ x_R &= ((\lambda'_{T,Q})^2 - x_{T'} - x_{Q'})(\alpha+1)^{-1}\beta^2, \\ y_R &= (x_{T'}\lambda'_{T,Q} - x_{R'}\lambda'_{T,Q} - y_{T'})(\alpha+1)^{-1}\beta\gamma. \end{aligned}$$

Representing the above line equations using variables as following :

$$\begin{aligned} A = \tfrac{1}{x_{Q'} - x_{T'}}, B = y_{Q'} - y_{T'}, C = AB, D = x_{T'} + x_{Q'}, \\ x_{R'} = C^2 - D, E = Cx_{T'} - y_{T'}, y_{R'} = E - Cx_{R'}, \\ l_{T',Q'}(P) = y_P + (\alpha+1)^{-1}E\beta\gamma - \\ (\alpha+1)^{-1}Cx_P\beta^2\gamma, \end{aligned} \tag{9a}$$

$$y_P^{-1}l_{T',Q'}(P) = 1 + (\alpha+1)^{-1}Ey_P^{-1}\beta\gamma - (\alpha+1)^{-1}Cx_Py_P^{-1}\beta^2\gamma, \tag{9b}$$

Here all the variables (A, B, C, D, E) are calculated as $\mathbb{F}_{p^2}$ elements. The position of the y_P, E and C in $\mathbb{F}_{p^{12}}$ vector representation is defined by the basis element 1, $\beta\gamma$ and $\beta^2\gamma$ as shown in Table 2. Therefore, among the 12 coefficients of $l_{T,T}(P)$ and $l_{T,Q}(P) \in \mathbb{F}_{p^{12}}$, only 5 coefficients $y_P \in \mathbb{F}_p$, $Cx_Py_P^{-1} \in \mathbb{F}_{p^2}$ and $Ey_P^{-1} \in \mathbb{F}_{p^2}$ are non-zero other 7 coefficients are zero. These zero coefficients leads to an efficient multiplication in Miller's loop usually called sparse multiplication.

3.1 Pseudo 8-sparse Multiplication

The line evaluations of (9b) and (8b) are identical and more sparse than (9a) and (8a). Such sparse form comes with a cost of computation overhead i.e., computing $y_P^{-1} l_{T,Q}(P)$ in the left side and $x_P y_P^{-1}$, $E y_P^{-1}$ on the right. But such overhead can be minimized by the following isomorphic mapping, which also accelerates the Miller's loop iteration.

Isomorphic mapping of $P \in \mathbb{G}_1 \mapsto \bar{P} \in \mathbb{G}'_1$:

$$\begin{aligned} \bar{E} : y^2 &= x^3 + b\bar{z}, \\ \bar{E}(\mathbb{F}_p)[r] &\longmapsto E(\mathbb{F}_p)[r], \\ (x, y) &\longmapsto (\bar{z}^{-1}x, \bar{z}^{-3/2}y), \end{aligned} \tag{10}$$

where $\bar{z} \in \mathbb{F}_p$ is a quadratic and cubic residue in $\mathbb{F}_p$. Equation (10) maps rational point P to $\bar{P}(x_{\bar{P}}, y_{\bar{P}})$ such that $(x_{\bar{P}}, y_{\bar{P}}^{-1}) = 1$. The twist parameter $\bar{z}$ is obtained as:

$$\bar{z} = (x_P y_P^{-1})^6 \tag{11}$$

From the (11) $\bar{P}$ and $\bar{Q}'$ is given as

$$\begin{aligned} \bar{P}(x_{\bar{P}}, y_{\bar{P}}) &= (x_P z^{-1}, y_P z^{-3/2}) \\ &= (x_P^3 y_P^{-2}, x_P^3 y_P^{-2}) && \text{(12a)} \\ \bar{Q}'(x_{\bar{Q}'}, y_{\bar{Q}'}) &= (x_P^2 y_P^{-2} x_{Q'}, x_P^3 y_P^{-3} y_{Q'}) && \text{(12b)} \end{aligned}$$

Using (12a) and (12b), the line evaluation of (8b) becomes

$$\begin{aligned} y_{\bar{P}}^{-1} l_{\bar{T}',\bar{T}'}(\bar{P}) &= 1 + (\alpha+1)^{-1} E y_{\bar{P}}^{-1} \beta\gamma - \\ &\quad (\alpha+1)^{-1} C x_{\bar{P}} y_{\bar{P}}^{-1} \beta^2\gamma, \\ \bar{l}_{\bar{T}',\bar{T}'}(\bar{P}) &= 1 + (\alpha+1)^{-1} E(x_P^{-3} y_P^2)\beta\gamma - \\ &\quad (\alpha+1)^{-1} C\beta^2\gamma. \end{aligned} \tag{13a}$$

Equation (9b) becomes similar to (13a). However, the to get the above form we need the following pre-computations once in every Miller's Algorithm execution.

- Computing $\bar{P}$ and $\bar{Q}'$,
- $(x_P^{-3} y_P^2)$

Here $(\alpha+1)^{-1}$ term can precomputed once since it is just inversion of the basis element. The above terms can be computed from x_P^{-1} and y_P^{-1} by utilizing Montgomery trick [17], as shown in **Alg.** 2. The pre-computation requires 21 multiplication, 2 squaring and 1 inversion in $\mathbb{F}_p$ and 2 multiplication, 2 squaring in $\mathbb{F}_{p^4}$. Finally, pseudo 8-sparse multiplication for BLS-12 is given in Alg. 3.

Algorithm 2: Pre-calculation and mapping $P \mapsto \bar{P}$ and $Q' \mapsto \bar{Q}'$

Input: $P = (x_P, y_P) \in \mathbb{G}_1, Q' = (x_{Q'}, y_{Q'}) \in \mathbb{G}'_2$
Output: $\bar{Q}', \bar{P}, y_P^{-1}$
1 $A \leftarrow (x_P y_P^{-1})$
2 $B \leftarrow A x_P^2$
3 $C \leftarrow A y_P$
4 $D \leftarrow D x_{Q'}$
5 $x_{\bar{Q}'} \leftarrow D x_{Q'}$
6 $y_{\bar{Q}'} \leftarrow BD y_{Q'}$
7 $x_{\bar{P}}, y_{\bar{P}} \leftarrow D x_P$
8 $y_P^{-1} \leftarrow C^3 y_P^2$
9 **return** $\bar{Q}' = (x_{\bar{Q}'}, y_{\bar{Q}'}), \bar{P} = (x_{\bar{P}}, y_{\bar{P}}), y_P^{-1}$

Algorithm 3: Pseudo 8-sparse multiplication for BLS-12 curves

Input: $a, b \in \mathbb{F}_{p^{12}}$
$a = (a_0 + a_1\beta + a_2\beta^2) + (a_3 + a_4\beta + a_5\beta^2)\gamma$,
$b = 1 + b_4\beta\gamma + b_5\beta^2\gamma$
where $a_i, b_j, c_i \in \mathbb{F}_{p^2} (i = 0, \cdots, 5, j = 4, 5)$
Output: $c = ab =$
$(c_0 + c_1\beta + c_2\beta^2) + (c_3 + c_4\beta + c_5\beta^2)\gamma \in \mathbb{F}_{p^{12}}$
1 $c_4 \leftarrow a_0 \times b_4$, $t_1 \leftarrow a_1 \times b_5$, $t_2 \leftarrow a_0 + a_1$, $S_0 \leftarrow b_4 + b_5$
2 $c_5 \leftarrow t_2 \times S_0 - (c_4 + t_1)$, $t_2 \leftarrow a_2 \times b_5$,
$t_2 \leftarrow t_2 \times (\alpha + 1)$
3 $c_4 \leftarrow c_4 + t_2$, $t_0 \leftarrow a_2 \times b_4$, $t_0 \leftarrow t_0 + t_1$
4 $c_3 \leftarrow t_0 \times (\alpha + 1)$, $t_0 \leftarrow a_3 \times b_4$, $t_1 \leftarrow a_4 \times b_5$,
$t_2 \leftarrow a_3 + a_4$
5 $t_2 \leftarrow t_2 \times S_0 - (t_0 + t_1)$
6 $c_0 \leftarrow t_2 \times (\alpha + 1)$, $t_2 \leftarrow a_5 \times b_4$, $t_2 \leftarrow t_1 + t_2$
7 $c_1 \leftarrow t_2 \times (\alpha + 1)$, $t_1 \leftarrow a_5 \times b_5$, $t_1 \leftarrow t_1 \times (\alpha + 1)$
8 $c_2 \leftarrow t_0 + t_1$
9 $c \leftarrow c + a$
10 return $c = (c_0 + c_1\beta + c_2\beta^2) + (c_3 + c_4\beta + c_5\beta^2)\gamma$

3.2 Final Exponentiation

Scott et al. [23] shows efficient final exponentiation $f^{p^k-1/r}$ by decomposing it using cyclotomic polynomial Φ_k as

$$(p^k - 1)/r = (p^{k/2} - 1) \cdot (p^{k/2} + 1)/\Phi_k(p) \cdot \Phi_k(p)/r. \tag{14}$$

Here, the 1st 2 terms of the right part is denoted as easy part, since it can be easily calculated by Frobenius mapping and 1 inversion in affine coordinates. The last term is called hard part which mostly effects the computation performance. According to (14), the exponent decomposition of the BLS-12 curve is shown in (15).

$$(p^{12} - 1)/r = (p^6 - 1) \cdot (p^2 + 1) \cdot (p^4 - p^2 + 1)/r \tag{15}$$

To efficiently carry out FE for the target curves we applied p-adic representation as shown in [10]. For scalar multiplication by prime p, i.e., $p[Q]$ or $[p^2]Q$, skew Frobenius map technique by Sakemi et al. [22] has been adapted.

4. Experimental Result Evaluation

This gives details of the experimental implementation. Table 3 shows implementation environment. Parameters chosen from [3] is shown in Table 4.

Table 3 Implementation and experiment settings

CPU	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz
OS	Ubuntu 16.04 LTS
Memory	4Gb
L1 Cache	256 KiB
Language	C

Table 4 Selected parameters for 128-bit security level [3]

	BLS-12	BN
u	$u = -2^{77} + 2^{50} + 2^{33}$	$u = 2^{114} + 2^{101} - 2^{14} - 1$
HW(u)	3	4
$\lfloor \log_2 u \rfloor$	77	115
$\lfloor \log_2 p(u) \rfloor$	461	462
$\lfloor \log_2 r(u) \rfloor$	308	462
$\lfloor \log_2 p^k \rfloor$	5532	5535

Table 5 shows execution time in millisecond for a single Opt-Ate pairing. Results here are the average of 10 pairing. Table 6 shows complexity of Miller's algorithm and final exponentiation. From the results we find that Miller's algorithm took fewer time for BLS-12 than BN curve. Total pairing time also faster for BLS-12 curve than BN curve. The major time difference is made by the calculation of hard part of the final exp.

Table 5 Comparative results of Miller's Algorithm and Final Exp. in [ms]

	Pairing		
	Miller Algo.	Final Exp.	Total time [ms]
BN	7.53	20.63	28.16
BLS-12	4.79	18.88	23.67

5. Conclusion and Future Work

This paper has presented an efficient Miller's loop calculation technique for BLS-12 curve and experimentally verifies that for 128-bit security level BLS-12 curve is sutable than BN curve in pairing-based cryptography.

Acknowledgment

This work was partially supported by the Strategic Information and Communications R&D Promotion Programme (SCOPE) of Ministry of Internal Affairs and Communications, Japan.

References

[1] Aranha, D.F., Karabina, K., Longa, P., Gebotys, C.H., López, J.: Faster explicit formulas for computing pairings over ordinary curves. In: Eurocrypt. vol. 6632, pp. 48–68. Springer (2011)

[2] Bailey, D.V., Paar, C.: Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. Journal of cryptology 14(3), 153–176 (2001)

[3] Barbulescu, R., Duquesne, S.: Updating key size estimations for pairings. Cryptology ePrint Archive, Report 2017/334 (2017), http://eprint.iacr.org/2017/334

[4] Barreto, P.S., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: International Conference on Security in Communication Networks. pp. 257–267. Springer (2002)

[5] Barreto, P.S., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: International Workshop on Selected Areas in Cryptography, SAC 2005. pp. 319–331. Springer (2005)

[6] Boneh, D., Lynn, B., Shacham, H.: Short signatures from the weil pairing. In: Advances in Cryptology—ASIACRYPT 2001, pp. 514–532. Springer (2001)

[7] Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of elliptic and hyperelliptic curve cryptography. CRC press (2005)

[8] Costello, C., Lange, T., Naehrig, M.: Faster pairing computations on curves with high-degree twists. In: International Workshop on Public Key Cryptography. pp. 224–242. Springer (2010)

[9] Duquesne, S., Mrabet, N.E., Haloui, S., Rondepierre, F.: Choosing and generating parameters for low level pairing implementation on bn curves. Cryptology ePrint Archive, Report 2015/1212 (2015), http://eprint.iacr.org/2015/1212

[10] Ghammam, L., Fouotsa, E.: On the computation of the optimal ate pairing at the 192-bit security level. Cryptology ePrint Archive, Report 2016/130 (2016), http://eprint.iacr.org/2016/130

[11] Granlund, T., the GMP development team: GNU MP: The GNU Multiple Precision Arithmetic Library, 6.1.0 edn. (2015), http://gmplib.org

[12] Joux, A.: A one round protocol for tripartite diffie–hellman. In: International Algorithmic Number Theory Symposium. pp. 385–393. Springer (2000)

[13] Kachisa, E., Schaefer, E., Scott, M.: Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field. Pairing-Based

Table 6 Operation count in $\mathbb{F}_p$ for 1 single pairing operation

		Multiplication	Squaring	Addition/ Subtraction	Basis multiplication	Inversion
BN	Miller's Algo.	10957	157	35424	3132	125
	Final exp.	29445	25	126308	9808	1
	Total	40402	182	161732	12940	126
BLS-12	Miller's Algo.	7089	113	23062	2030	80
	Final exp.	25737	25	111370	8572	1
	Total	32780	138	134432	10602	81

Cryptography–Pairing 2008 pp. 126–135 (2008)

[14] Khandaker, M.A.A., Ono, H., Nogami, Y., Shirase, M., Duquesne, S.: An improvement of optimal ate pairing on KSS curve with pseudo 12-sparse multiplication. In: International Conference on Information Security and Cryptology. pp. 208–219. Springer (2016)

[15] Kim, T., Barbulescu, R.: Extended tower number field sieve: A new complexity for the medium prime case. In: Advances in Cryptology - CRYPTO 2016 - Proceedings, Part I. pp. 543–571. Springer (2016)

[16] Matsuda, S., Kanayama, N., Hess, F., Okamoto, E.: Optimised versions of the ate and twisted ate pairings. In: Cryptography and Coding, pp. 302–312. Springer (2007)

[17] Montgomery, P.L.: Speeding the pollard and elliptic curve methods of factorization. Mathematics of computation 48(177), 243–264 (1987)

[18] Mori, Y., Akagi, S., Nogami, Y., Shirase, M.: Pseudo 8–sparse multiplication for efficient ate–based pairing on barreto–naehrig curve. In: Pairing-Based Cryptography–Pairing 2013, pp. 186–198. Springer (2013)

[19] Nakanishi, T., Funabiki, N.: Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps. In: Advances in Cryptology-ASIACRYPT 2005, pp. 533–548. Springer (2005)

[20] Nogami, Y., Akane, M., Sakemi, Y., Kato, H., Morikawa, Y.: Integer variable χ–based ate pairing. In: International Conference on Pairing-Based Cryptography. pp. 178–191. Springer (2008)

[21] Sakai, R.: Cryptosystems based on pairing. In: The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, Jan. pp. 26–28 (2000)

[22] Sakemi, Y., Nogami, Y., Okeya, K., Kato, H., Morikawa, Y.: Skew frobenius map and efficient scalar multiplication for pairing–based cryptography. In: International Conference on Cryptology and Network Security. pp. 226–239. Springer (2008)

[23] Scott, M., Benger, N., Charlemagne, M., Perez, L.J.D., Kachisa, E.J.: On the final exponentiation for calculating pairings on ordinary elliptic curves. In: Pairing-Based Cryptography - Pairing 2009, Third International Conference, Palo Alto, CA, USA, August 12-14, 2009, Proceedings. pp. 78–88 (2009), https://doi.org/10.1007/978-3-642-03298-1_6

[24] Vercauteren, F.: Optimal pairings. Information Theory, IEEE Transactions on 56(1), 455–461 (2010)