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 \(\chi\)-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 \(G_1 \times G_2 \rightarrow G_3\), where \(G_1\) and \(G_2\) are additive
cyclic sub-groups of order \( r \) on a certain elliptic curve \( E \) over a finite extension field \( \mathbb{F}_{p^k} \) and \( G_3 \) 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 \(^{\dagger} \) 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.

\(^{\dagger} \) 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 \( \mathbb{F}_{p^{12}} \) as follows:

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

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.

\[
p(u) = (u - 1)^2(u^4 - u^2 + 1)/3 + u, \quad (2a)
\]

\[
r(u) = (u^4 - u^2 + 1) \quad (2b)
\]

\[
t(u) = u + 1, \quad (2c)
\]

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 \( \mathbb{F}_{p^{12}} \), rational points on the curve \( E \) also forms an additive Abelian group denoted as \( E(\mathbb{F}_{p^{12}}) \).

2.2 Extension Field Arithmetic and Towering

In extension field arithmetic, higher level computations can be improved by towerings. In towerings, 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.

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

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 \( G_1, G_2 \) and a multiplicative group \( G_3 \) of order \( r \) are considered. \( G_1, G_2 \) and \( G_3 \) are defined as follows:

\[
\begin{align*}
G_1 & = E(\mathbb{F}_{p^r})[r] \cap \ker(\pi_p - [1]), \\
G_2 & = E(\mathbb{F}_{p^r})[r] \cap \ker(\pi_p - [p]), \\
G_3 & = \mathbb{F}_{p^r}/(\mathbb{F}_{p^r})^r, \\
e & : G_1 \times G_2 \rightarrow G_3, 
\end{align*}
\]  

(4)

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

In the case of BLS-12, the above \( G_1 \) is just \( E(\mathbb{F}_p) \). In what follows, rest of this paper considers \( P \in G_1 \subset E(\mathbb{F}_p) \) and \( Q \in G_2 \subset E(\mathbb{F}_{p^{12}}) \) for BLS-12 curve. Optimal-Ate pairing \( e(Q, P) \) is given as follows:

\[
e(Q, P) = f_{u,Q}(P)^{p^{12} \cdot 1},
\]

(5)

where \( f_{u,Q}(P) \) is the Miller’s algorithm’s result and \([\log_2(u)]\) is the loop length. The bilinearity of Ate pairing is satisfied after calculating the final exponentiation \( p^{12} \cdot 1 \).

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 Ghamam et al.’s final exponentiation algorithm [10].

**Algorithm 1:** Optimal Ate pairing on BLS-12 curve

**Input:** \( u, P \in G_1, Q' \in G'_2 \)

**Output:** \((Q, P) \)

1. \( f \leftarrow 1, T \leftarrow Q' \)
2. for \( i = [\log_2(u)] \) downto 1 do
3. \( f \leftarrow f^2 \cdot l_{1,T}(P), T \leftarrow [2]T \)
4. if \( u[i] = 1 \) then
5. \( f \leftarrow f \cdot l_{T,Q'}(P), T \leftarrow T + Q' \)
6. \( f \leftarrow f^{p^{12} \cdot 1} \)
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 \( Q \in E(\mathbb{F}_{p^r})[r] \cap \ker(\pi_p - [p]) \) belongs to. This sub-field isomorphic rational point group includes a twisted point of \( Q \), typically denoted as \( Q' \in E'(\mathbb{F}_{p^{12}/3}) \), 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 \( \mathbb{F}_{p^r} \), 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 \( E(\mathbb{F}_{p^r}) \). Since the pairing-friendly BLS-12 [4] curve has CM discriminant of \( D = 3 \) and \( 6k \), therefore sextic twist is available. Let \((\alpha + 1)\) be a certain quadratic and cubic non residue in \( \mathbb{F}_{p^r} \). The sextic twisted curve \( E'_b \) of curve \( E_b \) and their isomorphic mapping \( \psi_b \) are given as follows:

\[
E'_b : y^2 = x^3 + b(\alpha + 1), \quad b \in \mathbb{F}_p, \\
\psi_b : E'_b(\mathbb{F}_{p^r})[r] \rightarrow E_b(\mathbb{F}_{p^{12}})[r] \cap \ker(\pi_p - [p]), \\
(x, y) \mapsto ((\alpha + 1)^{-1}x^2, (\alpha + 1)^{-1}y\beta_1). 
\]

(6)

where \( \ker(\cdot) \) denotes the kernel of the mapping and \( \pi_p \) denotes Frobenius mapping for rational point.

Table 2 shows a the vector representation of \( Q = (x_Q, y_Q) = ((\alpha + 1)^{-1}x_Q^2, (\alpha + 1)^{-1}y_Q\beta_1) \in \mathbb{F}_{p^{12}} \) 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 \( \mathbb{F}_{p^r} \).

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

<table>
<thead>
<tr>
<th>$M_{\rho^2}$</th>
<th>$S_{\rho^2}$</th>
<th>$M_{\rho^2}$</th>
<th>$S_{\rho^2}$</th>
<th>$M_{\rho^2}$</th>
<th>$S_{\rho^2}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3M_p + 5\lambda p + 1\alpha \rightarrow 3M_p$</td>
<td>$2S_p + 3A_p \rightarrow 2S_p$</td>
<td>$5A_p + 2\beta \rightarrow 18M_p$</td>
<td>$9A_p + 2\gamma \rightarrow 12S_p$</td>
<td>$5A_p + 2\beta \rightarrow 54M_p$</td>
<td>$2M_p + 5A_p + 2\gamma \rightarrow 36S_p$</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>$x_Q$</th>
<th>$\alpha$</th>
<th>$\beta$</th>
<th>$\alpha \gamma$</th>
<th>$\beta \gamma$</th>
<th>$\alpha \beta \gamma$</th>
<th>$\alpha \beta^2 \gamma$</th>
<th>$\beta \gamma^2$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$b_1$</td>
<td>$b_2$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

(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 $P \mapsto \tilde{P}$ and same map for $Q \mapsto \tilde{Q}$ defined over curve $\tilde{E}$.

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

(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 $T=(\gamma x_T, \gamma y_T)$, $Q=(\gamma x_Q, \gamma y_Q)$ and $P=(x_P, y_P)$, where $x_P, y_P \in \mathbb{F}_p$ be given in affine coordinates on the curve $E(\mathbb{F}_p)$ 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.

$$l_{T,T}(P) = (y_p - y_T)(\alpha + 1)^{-1} \beta \gamma - \lambda_{T,T}(x_p - x_T)(\alpha + 1)^{-1} \beta^2 \gamma,$$

when $T=Q$,

$$\lambda_{T,T} = \frac{3x_T^2 \beta \gamma}{2x_T y_T^3} = \lambda'_{T,T} \gamma = \lambda'_{T,T}(\alpha + 1)^{-1} \beta^2 \gamma. \quad \text{(7)}$$

The line evaluation and ECD are obtained as follows:

$$l_{T,T}(P) = (y_p + (\lambda'_{T,T} x_T - y_T)(\alpha + 1)^{-1} \beta \gamma$$

$$-\lambda'_{T,T} x_T y_T)(\alpha + 1)^{-1} \beta^2 \gamma,$$

$$x_{2T} = ((\lambda'_{T,T} y_T^2 - 2x_T)(\alpha + 1)^{-1} \beta^2,$$

$$y_{2T} = ((x_T - x_{2T})(\alpha + 1)^{-1} \beta^2$$

The above calculations can be optimized as follows:

$$A = \frac{1}{x_T^2}, B = 3x_T^2, C = AB, D = 2x_T.$$
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 \( y_p^{-1}l_{rQ}(P) \) in the left side and \( x_p y_p^{-1} E y_p \) 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** \( P \in \mathbb{G}_1 \mapsto \hat{P} \in \mathbb{G}_1' \):

\[
E : y^2 = x^3 + b \bar{z},
\]
\[
\bar{E} : y^2 = x^3 + b\bar{z},
\]
\[
\bar{E}(F_p)[r] \mapsto E(F_p)[r],
\]
\[
(x, y) \mapsto (z^{-1}x, \bar{z}^{-3/2}y), \tag{10}
\]

where \( \bar{z} \in F_p \) is a quadratic and cubic residue in \( F_p \). Equation (10) maps rational point \( P \) to \( \hat{P}(x_p, y_p) \) such that \((x_p, y_p^{-1}) = 1 \). The twist parameter \( \bar{z} \) is obtained as:

\[
\bar{z} = (x_p y_p^{-1})^6 \tag{11}
\]

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

\[
\hat{P}(x_p, y_p) = (x_p z^{-1}, y_p \bar{z}^{-3/2})
\]
\[
= (x^2_p y_p^{-2}, x_p y_p^{-2}) \tag{12a}
\]
\[
\hat{Q}'(x_p y_p, y_p') = (x^2_p y_p^{-3} x_Q', x^2_p y_p^{-3} y_Q') \tag{12b}
\]

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

\[
y_p^{-1}l_{r,T}(\hat{P}) = 1 + (a + 1)^{-1} E y_p^{-1} \beta \gamma - (a + 1)^{-1} C x_p y_p^{-1} \beta^2 \gamma,
\]
\[
\bar{l}_{r,T}(\hat{P}) = 1 + (a + 1)^{-1} E (x_p^{-3} y_p^3) \beta \gamma - (a + 1)^{-1} C \beta^2 \gamma. \tag{13a}
\]

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 \( \hat{P} \) and \( \hat{Q}' \),
- \((x_p^{-3} y_p^3)\)

Here \((a + 1)^{-1}\) 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 \( F_p \) and 2 multiplication, 2 squaring in \( F_{p^3} \). Finally, pseudo 8-sparse multiplication for BLS-12 is given in Alg. 3.

**Algorithm 2:** Pre-calculation and mapping \( P \mapsto \hat{P} \) and \( Q' \mapsto \hat{Q}' \)

**Input:** \( P = (x_p, y_p) \in \mathbb{G}_1, Q' = (x_{Q'}, y_{Q'}) \in \mathbb{G}_2' \)

**Output:** \( \hat{Q}', \hat{P}, y_{\hat{P}}^{-1} \)

1. \( A \leftarrow (x_p y_p^{-1}) \)
2. \( B \leftarrow A x_p y_p^{-1} \)
3. \( C \leftarrow A y_p \)
4. \( D \leftarrow D x_{Q'} \)
5. \( x_{Q'} \leftarrow D x_{Q'} \)
6. \( y_{Q'} \leftarrow B D y_{Q'} \)
7. \( x_p, y_p \leftarrow D x_p \)
8. \( y_p^{-1} \leftarrow C^3 y_p \)
9. return \( \hat{Q}' = (x_{Q'}, y_{Q'}), \hat{P} = (x_p, y_p), y_p^{-1} \)

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

**Input:** \( a, b \in F_{p^{12}} \)

\[
a = (a_0 + a_1 \beta + a_2 \beta^2) + (a_3 + a_4 \beta + a_5 \beta^2) \gamma,
\]
\[
b = 1 + b_4 \beta_7 + b_5 \beta_6 \gamma
\]

where \( a_i, b_j, c_i \in F_{p^2} \)

**Output:** \( c = ab = (c_0 + c_1 \beta + c_2 \beta^2) + (c_3 + c_4 \beta + c_5 \beta^2) \gamma \in F_{p^{12}} \)

1. \( c_4 \leftarrow a_0 \times b_4, t_1 \leftarrow a_1 \times b_5, t_2 \leftarrow a_0 + a_1, S_0 = b_4 + b_5 \)
2. \( c_5 \leftarrow t_2 \times S_0 = (c_4 + t_1), t_2 \leftarrow a_2 \times b_5, \)
\[
t_2 \leftarrow t_2 \times (a + 1),
\]
3. \( c_4 \leftarrow c_4 + t_2, t_0 \leftarrow a_2 \times b_4, t_0 \leftarrow t_0 + t_1 \)
4. \( c_3 \leftarrow t_0 \times (a + 1), t_0 \leftarrow a_3 \times b_4, t_1 \leftarrow a_4 \times b_5, \)
\[
t_2 \leftarrow a_3 + a_4,
\]
5. \( t_2 \leftarrow t_2 \times S_0 = (t_0 + t_1) \)
6. \( c_6 \leftarrow t_2 \times (a + 1), t_2 \leftarrow a_5 \times b_4, t_2 \leftarrow t_1 + t_2 \)
7. \( c_1 \leftarrow t_2 \times (a + 1), t_1 \leftarrow a_5 \times b_5, t_1 \leftarrow t_1 \times (a + 1) \)
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 \( p^{k-1/r} \) by decomposing it using cyclotomic polynomial \( \Phi_k \) 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., $P \cdot Q$ 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)        |
| **OS**          | Ubuntu 16.04 LTS |
| **Memory**      | 4Gb             |
| **L1 Cache**    | 256 KiB         |
| **Language**    | C               |

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.

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 suitable 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

Table 6 Operation count in $F_p$ for 1 single pairing operation

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


