An Improvement of Optimal Ate Pairing on KSS Curve with Pseudo 12-Sparse Multiplication

Md. Al-Amin Khandaker[1(✉)], Hirotaka Ono[1], Yasuyuki Nogami[1], Masaaki Shirase[2], and Sylvain Duquesne[3]

[1] Graduate School of Natural Science and Technology, Okayama University, Okayama, Japan
{khandaker,hirotaka.ono}@s.okayama-u.ac.jp, yasuyuki.nogami@okayama-u.ac.jp
[2] Future University Hakodate, Hakodate, Japan
shirase@fun.ac.jp
[3] Université Rennes I, Rennes, France
sylvain.duquesne@univ-rennes1.fr

Abstract. Acceleration of a pairing calculation of an Ate-based pairing such as 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. Some recent works have shown the implementation of Optimal Ate pairing over Kachisa-Schaefer-Scott (KSS) curve of *embedding degree* 18. Pairing over KSS curve is regarded as the basis of next generation security protocols. This paper has proposed a *pseudo 12-sparse multiplication* to accelerate Miller's loop calculation in KSS curve by utilizing the property of rational point groups. In addition, this papers has showed an enhancement of the elliptic curve addition and doubling calculation in Miller's algorithm by applying implicit mapping of its sextic twisted isomorphic group. Moreover this paper has implemented the proposal with recommended security parameter settings for KSS curve at 192 bit security level. The simulation result shows that the proposed *pseudo 12-sparse multiplication* gives more efficient Miller's loop calculation of an Optimal Ate pairing operation along with recommended parameters than pairing calculation without sparse multiplication.

Keywords: KSS curve · Sparse multiplication · Optimal Ate pairing

1 Introduction

From the very beginning of the cryptosystems that utilizes elliptic curve pairing; proposed independently by Sakai et al. [18] and Joux [10], has unlocked numerous novel ideas to 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 [5] and group signature authentication by Nakanishi et al. [16] has come into the focus. In such outcome,

S. Hong and J.H. Park (Eds.): ICISC 2016, LNCS 10157, pp. 208–219, 2017.
DOI: 10.1007/978-3-319-53177-9_11

Ate-based pairings such as Ate [6], Optimal-ate [22], twisted Ate [14], R-ate [13], and χ-Ate [17] 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 time consuming operation.

Bilinear pairing operation consist of two predominant parts, named as Miller's loop and final exponentiation. Finding pairing friendly curves [8] and construction of efficient extension field arithmetic are the ground work for any pairing operation. Many research has been conducted for finding pairing friendly curves [3,7] and efficient extension field arithmetic [2]. Some previous work on optimizing the pairing algorithm on pairing friendly curve such Optimal Ate pairing by Matsuda et al. [14] on Barreto-Naehrig (BN) curve [4] is already carried out. The previous work of Mori et al. [15] has showed the *pseudo 8-sparse multiplication* to efficiently calculate Miller's algorithm defined over BN curve. Apart from it, Aranha et al. [1] has improved Optimal Ate pairing over KSS curve for 192 bit security level by utilizing the relation $t(\chi) - 1 \equiv \chi + 3p(\chi) \bmod r(\chi)$ where $t(\chi)$ is the Frobenius trace of KSS curve, χ is an integer also known as *mother parameter*, $p(\chi)$ is the prime number and $r(\chi)$ is the order of the curve. This paper has exclusively focused on efficiently calculating the Miller's loop of Optimal Ate pairing defined over KSS curve [11] for 192-bit security level by applying *pseudo 12-sparse multiplication* technique along with other optimization approaches. The parameter settings recommended in [1] for 192 bit security on KSS curve is used in the simulation implementation. But in the recent work, Kim et al. [12] has suggested to update the key sizes associated with pairing-based cryptography due to the new development of discrete logarithm problem over finite field. The parameter settings of [1] doesn't end up at the 192 bit security level according to [12]. However the parameter settings of [1] is primarily adapted in this paper in order to show the resemblance of the proposal with the experimental result.

In general, pairing is a bilinear map from two rational point groups $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group $\mathbb{G}_3$ [21]. When KSS pairing-friendly elliptic curve of embedding degree $k = 18$ is chosen for Ate-based pairing, then the bilinear map is denoted by $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$, where $\mathbb{G}_1 \subset E(\mathbb{F}_p)$, $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ and $\mathbb{G}_3 \subset \mathbb{F}^*_{p^{18}}$ and p denotes the characteristic and E is the curve defined over corresponding extension field $\mathbb{F}_{p^k}$. Rational point in $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ has a special vector representation where out of 18 $\mathbb{F}_p$ coefficients 3 continuous $\mathbb{F}_p$ coefficients are non-zero and the others are zero. By utilizing such representation along with the sextic twisted isomorphic sub-field property of $\mathbb{F}_{p^{18}}$, this paper has computed the elliptic curve doubling and elliptic curve addition in the Miller's algorithm as $\mathbb{F}_{p^3}$ arithmetic without any explicit mapping from $\mathbb{F}_{p^{18}}$ to $\mathbb{F}_{p^3}$.

Finally this paper proposes *pseudo 12-sparse multiplication* in affine coordinates for line evaluation in the Miller's algorithm by considering the fact that multiplying or dividing the result of Miller's loop calculation by an arbitrary non-zero $\mathbb{F}_p$ element does not change the result as the following final exponentiation cancels

the effect of multiplication or division. Following the division by a non-zero $\mathbb{F}_p$ element, one of the 7 non-zero $\mathbb{F}_p$ coefficients (which is a combination of 1 $\mathbb{F}_p$ and 2 $\mathbb{F}_{p^3}$ coefficients) becomes 1 that yields calculation efficiency. The calculation overhead caused from the division is canceled by isomorphic mapping with a quadratic and cubic residue in $\mathbb{F}_p$. This paper doesn't end up by giving only the theoretic proposal of improvement of Optimal Ate pairing by pseudo 12-sparse multiplication. In order to evaluate the theoretic proposal, this paper shows some experimental results with recommended parameter settings.

2 Fundamentals

This section briefly reviews the fundamentals of KSS curve [11], towering extension field with irreducible binomials [2], sextic twist, pairings and sparse multiplication [15].

2.1 KSS Curve

Kachisa-Schaefer-Scott (KSS) curve [11] is a non supersingular pairing friendly elliptic curve of embedding degree 18. The equation of KSS curve defined over $\mathbb{F}_{p^{18}}$ is given as follows:

$$E : y^2 = x^3 + b, \quad b \in \mathbb{F}_p \tag{1}$$

together with the following parameter settings,

$$p(\chi) = (\chi^8+5\chi^7+7\chi^6+37\chi^5+188\chi^4+259\chi^3+343\chi^2+1763\chi+2401)/21, \tag{2a}$$
$$r(\chi) = (\chi^6+37\chi^3+343)/343, \tag{2b}$$
$$t(\chi) = (\chi^4+16\chi+7)/7, \tag{2c}$$

where $b \neq 0$, $x, y \in \mathbb{F}_{p^{18}}$ and characteristic p (prime number), Frobenius trace t and order r are obtained systematically by using the integer variable χ, such that $\chi \equiv 14 \pmod{42}$.

2.2 Towering Extension Field

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. Since KSS curve is defined over $\mathbb{F}_{p^{18}}$, this paper has represented extension field $\mathbb{F}_{p^{18}}$ as a tower of sub-fields to improve arithmetic operations. In some previous works, such as Bailey et al. [2] explained tower of extension by using irreducible binomials. In what follows, let $(p-1)$ be divisible by 3 and c is a certain quadratic and cubic non residue in $\mathbb{F}_p$. Then for KSS-curve [11], where $k = 18$, $\mathbb{F}_{p^{18}}$ is constructed as tower field with irreducible binomial as follows:

$$\begin{cases} \mathbb{F}_{p^3} &= \mathbb{F}_p[i]/(i^3 - c), \\ \mathbb{F}_{p^6} &= \mathbb{F}_{p^3}[v]/(v^2 - i), \\ \mathbb{F}_{p^{18}} &= \mathbb{F}_{p^6}[\theta]/(\theta^3 - v). \end{cases} \tag{3}$$

Here isomorphic sextic twist of KSS curve defined over $\mathbb{F}_{p^{18}}$ is available in the base extension field $\mathbb{F}_{p^3}$.

2.3 Sextic Twist

Let z be a certain quadratic and cubic non residue $z \in \mathbb{F}_{p^3}$. The sextic twisted curve E' of KSS curve E defined in Eq. (1) and their isomorphic mapping ψ_6 are given as follows:

$$\begin{aligned} &E' : y^2 = x^3 + bz, \quad b \in \mathbb{F}_p \\ &\psi_6 : E'(\mathbb{F}_{p^3})[r] \longmapsto E(\mathbb{F}_{p^{18}})[r] \cap \mathrm{Ker}(\pi_p - [p]), \\ &\qquad (x, y) \longmapsto (z^{-1/3}x, z^{-1/2}y) \end{aligned} \tag{4}$$

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

$$\pi_p : (x, y) \longmapsto (x^p, y^p). \tag{5}$$

The order of the sextic twisted isomorphic curve $\#E'(\mathbb{F}_{p^3})$ is also divisible by the order of KSS curve E defined over $\mathbb{F}_p$ denoted as r. Extension field arithmetic by utilizing the sextic twisted sub-field curve $E'(\mathbb{F}_{p^3})$ based on the isomorphic twist can improve pairing calculation. In this paper, $E'(\mathbb{F}_{p^3})[r]$ shown in Eq. (4) is denoted as $\mathbb{G}'_2$.

Isomorphic mapping between $\mathbf{E(\mathbb{F}_p)}$ and $\hat{\boldsymbol{E}}(\mathbb{F}_p)$ Let us consider $\hat{E}(\mathbb{F}_p)$ is isomorphic to $E(\mathbb{F}_p)$ and $\hat{z}$ as a quadratic and cubic residue in $\mathbb{F}_p$. Mapping between $E(\mathbb{F}_p)$ and $\hat{E}(\mathbb{F}_p)$ is given as follows:

$$\begin{aligned} &\hat{E} : y^2 = x^3 + b\hat{z}, \\ &\quad \hat{E}(\mathbb{F}_p)[r] \longmapsto E(\mathbb{F}_p)[r], \\ &\quad (x, y) \longmapsto (\hat{z}^{-1/3}x, \hat{z}^{-1/2}y), \\ &\quad \textbf{where } \hat{z}, \hat{z}^{-1/2}, \hat{z}^{-1/3} \in \mathbb{F}_p. \end{aligned} \tag{6}$$

2.4 Pairings

As described earlier bilinear pairing requires two rational point groups to be mapped to a multiplicative group. In what follows, Optimal Ate pairing over KSS curve of embedding degree $k = 18$ is described as follows.

Optimal Ate Pairing. Let us consider the following two additive groups as $\mathbb{G}_1$ and $\mathbb{G}_2$ and multiplicative group as $\mathbb{G}_3$. The Ate pairing α is defined as follows:

$$\begin{aligned} \mathbb{G}_1 &= E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\pi_p - [1]), \\ \mathbb{G}_2 &= E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\pi_p - [p]). \end{aligned}$$

$$\alpha : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{F}'_{p^k}/(\mathbb{F}^*_{p^k})^r. \tag{7}$$

where $\mathbb{G}_1 \subset E(\mathbb{F}_p)$ and $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ in the case of KSS curve.

Let $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$, Ate pairing $\alpha(Q, P)$ is given as follows.

$$\alpha(Q, P) = f_{t-1,Q}(P)^{\frac{p^k-1}{r}}, \tag{8}$$

where $f_{t-1,Q}(P)$ symbolize the output of Miller's algorithm. The bilinearity of Ate pairing is satisfied after calculating the final exponentiation. It is noted that improvement of final exponentiation is not the focus of this paper. Several works [19,20] have been already done for efficient final exponentiation.

The previous work of Aranha et al. [1] has mentioned about the relation $t(\chi) - 1 \equiv \chi + 3p(\chi) \bmod r(\chi)$ for Optimal Ate pairing. Exploiting the relation, Optimal Ate pairing on the KSS curve is defined by the following representation.

$$(Q, P) = (f_{\chi,Q} \cdot f^p_{3,Q} \cdot l_{[\chi]Q,[3p]Q})^{\frac{p^{18}-1}{r}}, \tag{9}$$

where χ is the mother parameter. The calculation procedure of Optimal Ate pairing is shown in Algorithm 1. In what follows, the calculation steps from 1 to 5 shown in Algorithm 1 is identified as Miller's loop. Steps 3 and 5 are line evaluation along with elliptic curve doubling and addition. These two steps are key steps to accelerate the loop calculation. As an acceleration technique *pseudo 12-sparse multiplication* is proposed in this paper.

2.5 Sparse Multiplication

In the previous work, Mori et al. [15] has substantiated the pseudo 8-sparse multiplication for BN curve. Adapting affine coordinates for representing rational points, we can apply Mori's work in the case of KSS curve. The doubling phase and addition phase in Miller's loop can be carried out efficiently by the following calculations. Let $P = (x_P, y_P)$, $T = (x, y)$ and $Q = (x_2, y_2) \in E'(\mathbb{F}_{p^3})$ be given in affine coordinates, and let $T + Q = (x_3, y_3)$ be the sum of T and Q.

Step 3: Elliptic curve doubling phase ($T = Q$)

$$\begin{aligned} A = \tfrac{1}{2y}, B = 3x^2, C = AB, D = 2x, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, F = C\overline{x}_P, \\ l_{T,T}(P) = y_P + Ev + F\theta = y_P + Ev - Cx_P\theta, \end{aligned} \tag{10}$$

where $\overline{x}_P = -x_P$ will be pre-computed. Here $l_{T,T}(P)$ denotes the tangent line at the point T.

Step 5: Elliptic curve addition phase ($T \neq Q$)

$$\begin{aligned} A = \tfrac{1}{x_2-x}, B = y_2 - y, C = AB, D = x + x_2, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, F = C\overline{x}_P, \\ l_{T,Q}(P) = y_P + Ev + F\theta = y_P + Ev - Cx_P\theta, \end{aligned} \tag{11}$$

where $\overline{x}_P = -x_P$ will be pre-computed. Here $l_{T,Q}(P)$ denotes the tangent line between the point T and Q.

Analyzing Eqs. (10) and (11), we get that E and Cx_P are calculated in $\mathbb{F}_{p^3}$. After that, the basis element 1, v and θ identifies the position of y_P, E and Cx_P in $\mathbb{F}_{p^{18}}$ vector representation. Therefore vector representation of $l_{\psi_6(T),\psi_6(T)}(P) \in \mathbb{F}_{p^{18}}$ consists of 18 coefficients. Among them at least 11 coefficients are equal to zero. In the other words, only 7 coefficients $y_P \in \mathbb{F}_p$, $Cx_P \in \mathbb{F}_{p^3}$ and $E \in \mathbb{F}_{p^3}$ are perhaps to be non-zero. $l_{\psi_6(T),\psi_6(Q)}(P) \in \mathbb{F}_{p^{18}}$ also has the same vector structure. Thus, the calculation of multiplying $l_{\psi_6(T),\psi_6(T)}(P) \in \mathbb{F}_{p^{18}}$ or $l_{\psi_6(T),\psi_6(Q)}(P) \in \mathbb{F}_{p^{18}}$ is called sparse multiplication. In the above mentioned instance especially called 11-sparse multiplication. This sparse multiplication accelerates Miller's loop calculation as shown in Algorithm 1. This paper comes up with pseudo 12-sparse multiplication.

Algorithm 1. Optimal Ate pairing on KSS curve

Input: $\chi, P \in \mathbb{G}_1, Q \in \mathbb{G}_2'$
Output: (Q, P)
1 $f \leftarrow 1, T \leftarrow Q$
2 **for** $i = \lfloor \log_2(\chi) \rfloor$ **downto** 1 **do**
3 $\quad f \leftarrow f^2 \cdot l_{T,T}(P)$, $T \leftarrow [2]T$
4 $\quad$ **if** $\chi[i] = 1$ **then**
5 $\quad\quad f \leftarrow f \cdot l_{T,Q}(P)$, $T \leftarrow T + Q$
6 $f_1 \leftarrow f_{3,Q}^p$, $f \leftarrow f \cdot f_1$
7 $Q_1 \leftarrow [\chi]Q$, $Q_2 \leftarrow [3p]Q$
8 $f \leftarrow f \cdot l_{Q_1,Q_2}(P)$
9 $f \leftarrow f^{\frac{p^{18}-1}{r}}$
10 **return** f

3 Improved Optimal Ate Pairing for KSS Curve

In this section we describe the main proposal. Before going to the details, at first we give an overview of the improvement procedure of Optimal Ate pairing in KSS curve. The following two ideas are proposed in order to efficiently apply 12-sparse multiplication on Optimal Ate pairing on KSS curve.

1. In Eqs. (10) and (11) among the 7 non-zero coefficients, one of the non-zero coefficients is $y_P \in \mathbb{F}_p$. And y_P remains uniform through Miller's loop calculation. Thereby dividing both sides of those Eqs. (10) and (11) by y_P, the coefficient becomes 1 which results in a more efficient sparse multiplication by $l_{\psi_6(T),\psi_6(T)}(P)$ or $l_{\psi_6(T),\psi_6(Q)}(P)$. This paper calls it *pseudo 12-sparse multiplication.*

2. Division by y_P in Eqs. (10) and (11) causes a calculation overhead for the other non-zero coefficients in the Miller's loop. To cancel this additional cost in Miller's loop, the map introduced in Eq. (6) is applied.

It is to be noted that this paper doesn't focus on making final exponentiation efficient in Miller's algorithm since many efficient algorithms are available. From Eqs. (10) and (11) the above mentioned ideas are introduced in details.

3.1 Pseudo 12-Sparse Multiplication

As said before y_P shown in Eq. (10) is a non-zero elements in $\mathbb{F}_p$. Thereby, dividing both sides of Eq. (10) by y_P we obtain as follows:

$$y_P^{-1} l_{T,T}(P) = 1 + E y_P^{-1} v - C(x_P y_P^{-1})\theta. \tag{12}$$

Replacing $l_{T,T}(P)$ by the above $y_P^{-1} l_{T,T}(P)$, the calculation result of the pairing does not change, since *final exponentiation* cancels $y_P^{-1} \in \mathbb{F}_p$. One of the non-zero coefficients becomes 1 after the division by y_P, which results in more efficient vector multiplications in Miller's loop. This paper calls it *pseudo* $12-$*sparse multiplication*. Algorithm 2 introduces the detailed calculation procedure of pseudo 12-sparse multiplication.

Algorithm 2. Pseudo 12-sparse multiplication

Input: $a, b \in \mathbb{F}_{p^{18}}$
$a = (a_0 + a_1\theta + a_2\theta^2) + (a_3 + a_4\theta + a_5\theta^2)v$, $b = 1 + b_1\theta + b_3 v$
where $a_i, b_j, c_i \in \mathbb{F}_{p^3} (i = 0, \cdots, 5, j = 1, 3)$
Output: $c = ab = (c_0 + c_1\theta + c_2\theta^2) + (c_3 + c_4\theta + c_5\theta^2)v \in \mathbb{F}_{p^{18}}$
1 $c_1 \leftarrow a_0 \times b_1, c_5 \leftarrow a_2 \times b_3, t_0 \leftarrow a_0 + a_2, S_0 \leftarrow b_1 + b_3$
2 $c_3 \leftarrow t_0 \times S_0 - (c_1 + c_5)$
3 $c_2 \leftarrow a_1 \times b_1, c_6 \leftarrow a_3 \times b_3, t_0 \leftarrow a_1 + a_3$
4 $c_4 \leftarrow t_0 \times S_0 - (c_2 + c_6)$
5 $c_5 \leftarrow c_5 + a_4 \times b_1, c_6 \leftarrow c_6 + a_5 \times b_1$
6 $c_7 \leftarrow a_4 \times b_3, c_8 \leftarrow a_5 \times b_3$
7 $c_0 \leftarrow c_6 \times i$
8 $c_1 \leftarrow c_1 + c_7 \times i$
9 $c_2 \leftarrow c_2 + c_8 \times i$
10 $c \leftarrow c + a$
11 return $c = (c_0 + c_1\theta + c_2\theta^2) + (c_3 + c_4\theta + c_5\theta^2)v$

3.2 Line Calculation in Miller's Loop

The comparison of Eqs. (10) and (12) shows that the calculation cost of Eq. (12) is little bit higher than Eq. (10) for $E y_P^{-1}$. The cancellation process of $x_P y_P^{-1}$ terms by utilizing isomorphic mapping is introduced next. The $x_P y_P^{-1}$ and y_P^{-1} terms

are pre-computed to reduce execution time complexity. The map introduced in Eq. (6) can find a certain isomorphic rational point $\hat{P}(x_{\hat{P}}, y_{\hat{P}}) \in \hat{E}(\mathbb{F}_p)$ such that

$$x_{\hat{P}} y_{\hat{P}}^{-1} = 1. \tag{13}$$

Here the twist parameter z of Eq. (4) is considered to be $\hat{z} = (x_P y_P^{-1})^6$ of Eq. (6), where $\hat{z}$ is a quadratic and cubic residue in $\mathbb{F}_p$ and $\hat{E}$ denotes the KSS curve defined by Eq. (6). From the isomorphic mapping Eq. (4), such z is obtained by solving the following equation considering the input $P(x_P, y_P)$.

$$z^{1/3} x_P = z^{1/2} y_P, \tag{14}$$

Afterwards the $\hat{P}(x_{\hat{P}}, y_{\hat{P}}) \in \hat{E}(\mathbb{F}_p)$ is given as

$$\hat{P}(x_{\hat{P}}, y_{\hat{P}}) = (x_P^3 y_P^{-2}, x_P^3 y_P^{-2}). \tag{15}$$

As the x and y coordinates of $\hat{P}$ are the same, $x_{\hat{P}} y_{\hat{P}}^{-1} = 1$. Therefore, corresponding to the map introduced in Eq. (6), first mapping not only P to $\hat{P}$ shown above but also Q to $\hat{Q}$ shown below.

$$\hat{Q}(x_{\hat{Q}}, y_{\hat{Q}}) = (x_P^2 y_P^{-2} x_Q, x_P^3 y_P^{-3} y_Q). \tag{16}$$

When we define a new variable $L = (x_P^{-3} y_P^2) = y_{\hat{P}}^{-1}$, the line evaluations, Eqs. (10) and (11) become the following calculations. In what follows, let $\hat{P} = (x_{\hat{P}}, y_{\hat{P}}) \in E(\mathbb{F}_p)$, $T = (x, y)$ and $Q = (x_2, y_2) \in E'(\mathbb{F}_{p^3})$ be given in affine coordinates and let $T + Q = (x_3, y_3)$ be the sum of T and Q.

Step 3: Doubling phase ($T = Q$)

$$\begin{gathered} A = \tfrac{1}{2y}, B = 3x^2, C = AB, D = 2x, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, \\ \hat{l}_{T,T}(P) = y_P^{-1} l_{T,T}(P) = 1 + ELv - C\theta, \end{gathered} \tag{17}$$

where $L = y_{\hat{P}}^{-1}$ will be pre-computed.

Step 5: Addition phase ($T \neq Q$)

$$\begin{gathered} A = \tfrac{1}{x_2 - x}, B = y_2 - y, C = AB, D = x + x_2, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, \\ \hat{l}_{T,Q}(P) = y_P^{-1} l_{T,Q}(P) = 1 + ELv - C\theta, \end{gathered} \tag{18}$$

where $L = y_{\hat{P}}^{-1}$ will be pre-computed.

As we compare the above equation with to Eqs. (10) and (11), the third term of the right-hand side becomes simple since $x_{\hat{P}} y_{\hat{P}}^{-1} = 1$.

In the above procedure, calculating $\hat{P}$, $\hat{Q}$ and L by utilizing x_P^{-1} and y_P^{-1} will create some computational overhead. In spite of that, calculation becomes efficient as it is performed in isomorphic group together with pseudo 12-sparse multiplication in the Miller's loop. Improvement of Miller's loop calculation is presented by experimental results in the next section.

4 Cost Evaluation and Experimental Result

This section shows some experimental results with evaluating the calculation costs in order to the signify efficiency of the proposal. It is to be noted here that in the following discussions "Previous method" means Optimal Ate pairing with no use the sparse multiplication, "11-sparse multiplication" means Optimal Ate pairing with 11-sparse multiplication and "Proposed method" means Optimal Ate pairing with Pseudo 12-sparse multiplication.

4.1 Parameter Settings and Computational Environment

In the experimental simulation, this paper has considered the 192 bit security level for KSS curve. Table 1 shows the parameters settings suggested in [1] for 192 bit security over KSS curve. However this parameter settings does not necessarily comply with the recent suggestion of key size by Kim et al. [12] for 192 bit security level. The sole purpose to use this parameter settings in this paper is to compare the literature with the experimental result.

To evaluate the operational cost and to compare the execution time of the proposal based on the recommended parameter settings, the following computational environment is considered. Table 2 shows the computational environment.

4.2 Cost Evaluation

Let us consider m, s, a and i to denote the times of multiplication, squaring, addition and inversion $\in \mathbb{F}_p$. Similarly, $\tilde{m}, \tilde{s}, \tilde{a}$ and $\tilde{i}$ denote the number of multiplication, squaring, addition and inversion $\in \mathbb{F}_{p^3}$ and $\hat{m}, \hat{s}, \hat{a}$ and $\hat{i}$ to denote the count of multiplication, squaring, addition and inversion $\in \mathbb{F}_{p^{18}}$ respectively. Tables 3 and 4 show the calculation costs with respect to operation count.

Table 1. Parameters

Security level	χ	$p(\chi)$ [bit]	c Eq. (3)	b Eq. (1)
192-bit	$-2^{64} - 2^{51} + 2^{46} + 2^{12}$	508	2	2

Table 2. Computing environment

CPU	Core i5 6600
Memory	8.00 GB
OS	Ubuntu 16.04 LTS
Library	GMP 6.1.0 [9]
Compiler	gcc 5.4.0
Programming language	C

Table 3. Operation count of line evaluation

$E(\mathbb{F}_{p^{18}})$ Operations	Previous method	11-sparse multiplication	Proposed method
Precomputation	-	$\tilde{a}$	$6\tilde{m} + 2\tilde{i}$
Doubling + $l_{T,T}(P)$	$9\hat{a} + 6\hat{m} + 1\hat{i}$	$7\tilde{a} + 6\tilde{m} + 1\tilde{i}$	$7\tilde{a} + 6\tilde{m} + 1\tilde{i}$
Addition + $l_{T,Q}(P)$	$8\hat{a} + 5\hat{m} + 1\hat{i}$	$6\tilde{a} + 5\tilde{m} + 1\tilde{i}$	$6\tilde{a} + 5\tilde{m} + 1\tilde{i}$

Table 4. Operation count of multiplication

$\mathbb{F}_{p^{18}}$ Operations	Previous method	11-sparse multiplication	Proposed method
Vector Multiplication	$30\tilde{a} + 18\tilde{m} + 8a$	$1\hat{a} + 11\tilde{a} + 10\tilde{m} + 3a + \mathbf{18m}$	$1\hat{a} + 11\tilde{a} + 10\tilde{m} + 3a$

Table 5. Calculation time of Optimal Ate pairing at the 192-bit security level

Operation	Previous method	11-sparse multiplication	Proposed method
Doubling+ $l_{T,T}(P)$ $[\mu s]$	681	44	44
Addition+ $l_{T,Q}(P)$ $[\mu s]$	669	39	37
Multiplication $[\mu s]$	119	74	65
Miller's Algorithm $[ms]$	524	142	140

By analyzing the Table 4 we can find that 11-sparse multiplication requires 18 more multiplication in $\mathbb{F}_p$ than pseudo 12-sparse multiplication.

4.3 Experimental Result

Table 5 shows the calculation times of Optimal Ate pairing respectively. In this execution time count, the time required for final exponentiation is excluded. The results (time count) are the averages of 10000 iterations on PC respectively. According to the experimental results, pseudo 12-sparse contributes to a few percent acceleration of 11-sparse.

5 Conclusion and Future Works

This paper has proposed pseudo 12-sparse multiplication for accelerating Optimal Ate pairing on KSS curve. According to the calculation costs and experimental results shown in this paper, the proposed method can calculate Optimal Ate pairing more efficiently. As a future work we would like to evaluate the efficiency in practical case by implementing it in some pairing based protocols.

Acknowledgment. This work is 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., Fuentes-Castañeda, L., Knapp, E., Menezes, A., Rodríguez-Henríquez, F.: Implementing pairings at the 192-bit security level. In: Abdalla, M., Lange, T. (eds.) Pairing 2012. LNCS, vol. 7708, pp. 177–195. Springer, Heidelberg (2013). doi:10.1007/978-3-642-36334-4_11
2. Bailey, D.V., Paar, C.: Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. J. Crypt. **14**(3), 153–176 (2001). http://dx.doi.org/10.1007/s001450010012
3. Barreto, P.S.L.M., Lynn, B., Scott, M.: Constructing elliptic curves with prescribed embedding degrees. In: Cimato, S., Persiano, G., Galdi, C. (eds.) SCN 2002. LNCS, vol. 2576, pp. 257–267. Springer, Heidelberg (2003). doi:10.1007/3-540-36413-7_19
4. Barreto, P.S.L.M., Naehrig, M.: Pairing-friendly elliptic curves of prime order. In: Preneel, B., Tavares, S. (eds.) SAC 2005. LNCS, vol. 3897, pp. 319–331. Springer, Heidelberg (2006). doi:10.1007/11693383_22
5. Boneh, D., Lynn, B., Shacham, H.: Short signatures from the Weil pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 514–532. Springer, Heidelberg (2001). doi:10.1007/3-540-45682-1_30
6. Cohen, H., Frey, G., Avanzi, R., Doche, C., Lange, T., Nguyen, K., Vercauteren, F.: Handbook of Elliptic and Hyperelliptic Curve Cryptography. CRC Press, Boca Raton (2005)
7. Dupont, R., Enge, A., Morain, F.: Building curves with arbitrary small MOV degree over finite prime fields. J. Crypt. **18**(2), 79–89 (2005)
8. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Crypt. **23**(2), 224–280 (2010)
9. Granlund, T.: The GMP development team: GNU MP: The GNU Multiple Precision Arithmetic Library, 6.1.0 edn. (2015). http://gmplib.org/
10. Joux, A.: A one round protocol for tripartite Diffie–Hellman. In: Bosma, W. (ed.) ANTS 2000. LNCS, vol. 1838, pp. 385–393. Springer, Heidelberg (2000). doi:10.1007/10722028_23
11. Kachisa, E.J., Schaefer, E.F., Scott, M.: Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field. In: Galbraith, S.D., Paterson, K.G. (eds.) Pairing 2008. LNCS, vol. 5209, pp. 126–135. Springer, Heidelberg (2008). doi:10.1007/978-3-540-85538-5_9
12. Kim, T., Barbulescu, R.: Extended tower number field sieve: A new complexity for medium prime case. Technical report, IACR Cryptology ePrint Archive, 2015: 1027 (2015)
13. Lee, E., Lee, H.S., Park, C.M.: Efficient and generalized pairing computation on abelian varieties. IEEE Trans. Inf. Theor. **55**(4), 1793–1803 (2009)
14. Matsuda, S., Kanayama, N., Hess, F., Okamoto, E.: Optimised versions of the ate and twisted ate pairings. In: Galbraith, S.D. (ed.) Cryptography and Coding 2007. LNCS, vol. 4887, pp. 302–312. Springer, Heidelberg (2007). doi:10.1007/978-3-540-77272-9_18
15. Mori, Y., Akagi, S., Nogami, Y., Shirase, M.: Pseudo 8–sparse multiplication for efficient ate–based pairing on Barreto–Naehrig curve. In: Cao, Z., Zhang, F. (eds.) Pairing 2013. LNCS, vol. 8365, pp. 186–198. Springer, Heidelberg (2014). doi:10.1007/978-3-319-04873-4_11
16. Nakanishi, T., Funabiki, N.: Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps. In: Roy, B. (ed.) ASIACRYPT 2005. LNCS, vol. 3788, pp. 533–548. Springer, Heidelberg (2005). doi:10.1007/11593447_29

17. Nogami, Y., Akane, M., Sakemi, Y., Katou, H., Morikawa, Y.: Integer variable chi-based ate pairing. In: Proceedings of the Second International Conference on Pairing-Based Cryptography - Pairing 2008, Egham, UK, pp. 178–191, 1–3 September 2008. http://dx.doi.org/10.1007/978-3-540-85538-5_13
18. Sakai, R., Kasahara, M.: ID based cryptosystems with pairing on elliptic curve. IACR Cryptology ePrint Archive 2003, p. 54 (2003)
19. 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: Shacham, H., Waters, B. (eds.) Pairing 2009. LNCS, vol. 5671, pp. 78–88. Springer, Heidelberg (2009). doi:10.1007/978-3-642-03298-1_6
20. Shirase, M., Takagi, T., Okamoto, E.: Some efficient algorithms for the final exponentiation of η_T pairing. In: Dawson, E., Wong, D.S. (eds.) ISPEC 2007. LNCS, vol. 4464, pp. 254–268. Springer, Heidelberg (2007). doi:10.1007/978-3-540-72163-5_20
21. Silverman, J.H., Cornell, G., Artin, M.: Arithmetic Geometry. Springer, Heidelberg (1986)
22. Vercauteren, F.: Optimal pairings. IEEE Trans. Inf. Theor. **56**(1), 455–461 (2010)