PAPER Special Section on Discrete Mathematics and Its Applications

Pseudo Sparse Multiplication for Optimal-Ate Pairing

Md. AL-AMIN KHANDAKER[†], ***Nonmember and*** **Yasuyuki NOGAMI**[†], ***Member***

SUMMARY Scalar multiplication over higher degree rational point groups is often regarded as the bottleneck for faster pairing based cryptography. This paper has presented a skew Frobenius mapping technique in the sub-field isomorphic *sextic twisted* curve of Kachisa-Schaefer-Scott (KSS) pairing friendly curve of *embedding degree* 18 in the context of Ate based pairing. Utilizing the skew Frobenius map along with multi-scalar multiplication procedure, an efficient scalar multiplication method for KSS curve is proposed in the paper. In addition to the theoretic proposal, this paper has also presented a comparative simulation of the proposed approach with plain binary method, sliding window method and non-adjacent form (NAF) for scalar multiplication. The simulation shows that the proposed method is about 60 times faster than plain implementation of other compared methods.

key words: *scalar multiplication, skew Frobenius mapping, KSS curve*

1. Introduction

Pairing based cryptography has attracted many researchers since Sakai et al. [1] and Joux et al. [2] independently proposed a cryptosystem based on elliptic curve pairing. This has encouraged to invent several innovative pairing based cryptographic applications such as broadcast encryption [3] and group signature authentication [4], that has increased the popularity of pairing based cryptographic research. But using pairing based cryptosytem in industrial state is still restricted by its expensive operational cost with respect to time and computational resources in practical case. In order to make it practical, several pairing techniques such as Ate [5], Optimal-ate [6], twisted Ate [7], χ-Ate [8] and *sub-field twisted* Ate [9] pairings have gained much attention since they have achieved quite efficient pairing calculation in certain pairing friendly curve. Researchers still continues on finding efficient way to implement pairing to make it practical enough for industrial standardization. In such consequences, this paper focuses on a peripheral technique of Ate-based pairings that is scalar multiplication defined over Kachisa-Schaefer-Scott (KSS) curve [10] of embedding degree 18.

In general, pairing is a bilinear map of two rational point groups $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group $\mathbb{G}_3$ [11]. The typical notation of pairing is $\mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3$. In Ate-based pairing, $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ are defined as:

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

where α denotes Ate pairing. Pairings are often defined over certain extension field $\mathbb{F}_{p^k}$, where p is the prime number, also know as characteristics and k is the minimum extension degree for pairing also called *embedding* degree. The set of rational points $E(\mathbb{F}_{p^k})$ are defined over a certain pairing friendly curve of embedded extension field of degree k. This paper has considered Kachisa-Schaefer-Scott (KSS) [10] pairing friendly curves of emebdding degree $k = 18$ described in [12].

Scalar multiplication is often considered to be one of the most time consuming operation in cryptographic scene. Efficient scalar multiplication is one of the important factors for making the pairing practical over KSS curve. There are several works [13] [14] on efficiently computing scalar multiplication defined over Barreto-Naehrig [15] curve along with efficient extension field arithmetic [16]. This paper focuses on efficiently performing scalar multiplication on rational points defined over rational point group $\mathbb{G}_2$ by scalar s, since scalar multiplication is required repeatedly in cryptographic calculation. However in asymmetric pairing such as Ate-based pairing, scalar multiplication of $\mathbb{G}_2$ rational points is important as no mapping function is explicitly given between $\mathbb{G}_1$ to $\mathbb{G}_2$. By the way, as shown in the definition, $\mathbb{G}_1$ is a set of rational points defined over prime field and there are several researches [14] for efficient scalar multiplication in $\mathbb{G}_1$. The common approach to accelerate scalar multiplication are log-step algorithm such as binary and non-adjacent form (NAF) methods, but more efficient approach is to use Frobenius mapping in the case of $\mathbb{G}_2$ that is defined over $\mathbb{F}_{p^k}$. Moreover when sextic twist of the pairing friendly curve exists, then we apply skew Frobenius map on the isomorphic sextic-twisted sub-field rational points. Such technique will reduce the computational cost in a great extent. In this paper we have exploited the sextic twisted property of KSS curve and utilized skew Frobenius map to reduce the computational time of scalar multiplication on $\mathbb{G}_2$ rational point. Utilizing the relation $z \equiv -3p + p^4 \bmod r$,[†] derived by Aranha et al, [17] and the properties of $\mathbb{G}_2$ rational point, the scalar can be expressed as z-adic representation. Together with skew

Manuscript received January 1, 2015.
Manuscript revised January 1, 2015.

[†] Graduate School of Natural Science and Technology, Okayama University, 3-1-1, Tsushima-naka, Kita, Okayama, 700-8530, E-mail: khandaker@s.okayama-u.ac.jp, yasuyuki.nogami@okayama-u.ac.jp

DOI: 10.1587/transfun.E0.A.1

[†] z is the mother parameter of KSS curve and z is about six times smaller than the size of order r.

Frobenius mapping and z-adic representation the scalar multiplication can be further accelerated. We have utilized this relation to construct z-adic representation of scalar s which is introduced in section 3. In addition with Frobenius mapping and z-adic representation of s, we applied the multi-scalar multiplication technique to compute elliptic curve addition in parallel in the proposed scalar multiplication. We have compared our proposed method with three other well studied methods named binary method, sliding-window method and non-adjacent form method. The comparison shows that our proposed method is about 60 times faster than the plain implementations of above mentioned methods in execution time. The comparison also reveals that the proposed method requires more than 5 times less elliptic curve doubling than any of the compared methods.

The rest of the paper is organized as follows. The fundamentals of elliptic curve arithmetic, scalar multiplication along with KSS curve over $\mathbb{F}_{p^{18}}$ extension field and *sextic twist* of KSS curve are described in section 2. In section 3, this paper describes the proposal in details. The experimental result is presented in section 4 which shows that our scalar multiplication technique on $\mathbb{G}_2$ rational points of KSS curve can be accelerated by 60 times than plain implementation of binary, sliding-window and NAF methods. Finally section 5 draws the conclusion with some outline how this work can be enhanced more as a future work.

Throughout this paper, p and k denote characteristic and embedding extension degree, respectively. $\mathbb{F}_{p^k}$ denotes k-th extension field over prime field $\mathbb{F}_p$ and $\mathbb{F}^*_{p^k}$ denotes the multiplicative group in $\mathbb{F}_{p^k}$.

The process of getting z-adic representation and using it for scalar multiplication over KSS curve is presented in 17th World Conference on Information Security Applications (WISA 2016), Jeju, Korea. It will be published in the conference proceedings from Springer LNCS. For the convenience of describing the total procedure, here we will discus z-adic representation in section 3.

2. Preliminaries

In this section we will go through the fundamental background of elliptic curves and its operations. We will briefly review elliptic curve scalar multiplication. After that pairing friendly curve of embedding degree $k = 18$, i.e., KSS curve and its properties will be introduced briefly.

2.1 Elliptic curve

An elliptic curve [18] defined over $\mathbb{F}_p$ is generally represented by *affine coordinates* [11] as follows;

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

where $4a^3 + 27b^2 \neq 0$ and $a, b \in \mathbb{F}_p$. A pair of coordinates x and y that satisfy Eq. (1) are known as *rational points* on the curve.

2.1.1 Point addition.

Let $E(\mathbb{F}_p)$ be the set of all rational points on the curve E including the point at infinity $\mathcal{O}$. $\#E(\mathbb{F}_p)$ denotes the order of $E(\mathbb{F}_p)$. Let us consider two rational points using affine coordinates as $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, and their addition $R = P_1 + P_2$, where $R = (x_3, y_3)$ and $P_1, P_2, R \in E(\mathbb{F}_p)$. Then the x and y coordinates of R are calculated as follows:

$$x_3 = \lambda^2 - x_1 - x_2, \tag{2a}$$
$$y_3 = (x_1 - x_3)\lambda - y_1, \tag{2b}$$

where λ is given as follows:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}; & P_1 \neq P_2, \\ \frac{3x_1^2 + a}{2y_1}; & P_1 = P_2, \end{cases} \tag{2c}$$

λ is the tangent at the point on the curve and $\mathcal{O}$ is the additive unity in $E(\mathbb{F}_p)$. If $P_1 \neq P_2$ then $P_1 + P_2$ is called elliptic curve addition (ECA). If $P_1 = P_2$ then $P_1 + P_2 = 2P_1$, which is known as elliptic curve doubling (ECD).

2.1.2 Scalar multiplication

Let scalar s is $0 \leq s < r$, where r is the order of the target rational point group. Scalar multiplication of rational points P_1, denoted as $[s]P_1$ is calculated by $(s-1)$-times additions of P_1 as,

$$[s]P_1 = \sum_{i=0}^{s-1} P_1, \quad 0 \leq s < r, \tag{3}$$

When $s = r$, then $[r]P_1 = \mathcal{O}$ where r is the order of the curve. Let $[s]P_1 = P_2$, and value of s is not obtained, then the solving s from P_1 and P_2 is known as elliptic curve discrete logarithm problem (ECDLP). The difficulty level of solving ECDLP defines the security strength of elliptic curve cryptography.

2.2 KSS curve

In [10], Kachisa, Schaefer, and Scott proposed a family of non super-singular Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field. In what follows this paper considers the KSS curve of embedding degree $k = 18$ since it holds *sextic twist*. The equation of KSS curve defined over $\mathbb{F}_{p^{18}}$ is given as follows:

$$E : Y^2 = X^3 + b, \quad (b \in \mathbb{F}_p), \tag{4}$$

where $b \neq 0$ and $X, Y \in \mathbb{F}_{p^{18}}$. Its characteristic p, Frobenius trace t and order r are given systematically by using an integer variable z as follows:

$$p(z) = (z^8 + 5z^7 + 7z^6 + 37z^5 + 188z^4 + 259z^3$$

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

where z is such that $z \equiv 14 \pmod{42}$ and the ρ value is $\rho = (\log_2 p / \log_2 r) \approx 1.33$.

In some previous work of Aranha et al. [17] and Scott et al. [19] has mentioned that the size of the characteristics p to be 508 to 511-bit with order r of 384-bit for 192-bit security level. Therefore this paper used parameter settings according to the suggestion of [17] for 192 bit security on KSS curve in the simulation implementation. In the recent work, Kim et al. [20] has suggested to update the key sizes in pairing-based cryptography due to the development of new discrete logarithm problem over finite field. The parameter settings used in this paper doesn't completely end up at the 192 bit security level according to [20]. However the parameter settings used in this paper in order to show the resemblance of the proposal with the experimental result.

2.3 $\mathbb{F}_{p^{18}}$ extension field arithmetic

Pairing based cryptography requires to perform arithmetic operation in extension fields of degree $k \geq 6$ [11]. In the previous works of Bailey et al. [21] explained optimal extension field by towering by using irreducible binomials. In this paper extension field $\mathbb{F}_{p^{18}}$ is represented as a tower of sub field to improve arithmetic operations.

Let $(p-1)$ is divisible by 3 and c is a quadratic and cubic non residue in $\mathbb{F}_p$. In KSS curve [10], where $k = 18$, $\mathbb{F}_{p^{18}}$ is constructed with irreducible binomials by the following towering scheme.

$$\begin{cases} \mathbb{F}_{p^3} = \mathbb{F}_p[i]/(i^3 - c), \text{where } c = 2 \text{ is the best choice,} \\ \mathbb{F}_{p^6} = \mathbb{F}_{p^3}[v]/(v^2 - i), \\ \mathbb{F}_{p^{18}} = \mathbb{F}_{p^6}[\theta]/(\theta^3 - v). \end{cases}$$

where the base extension field is $\mathbb{F}_{p^3}$ for the *sextic twist* of KSS curve.

2.3.1 Frobenius mapping of rational point in $E(\mathbb{F}_{p^{18}})$.

Let (x, y) be certain rational point in $E(\mathbb{F}_{p^{18}})$. Frobenius map $\pi_p : (x, y) \mapsto (x^p, y^p)$ is the p-th power of the rational point defined over $\mathbb{F}_{p^{18}}$. Sakemi et al. [14] showed an efficient scalar multiplication by applying skew Frobenius mapping in the context of Ate-based pairing in BN curve of embedding degree $k = 12$. In this paper we have utilized skew Frobenius mapping technique for efficient scalar multiplication for the KSS curve.

2.4 Sextic twist of KSS curve

Let the embedding degree $k = 6e$, where e is positive integer, *sextic* twist is given as follows:

$$E: \quad y^2 = x^3 + b, \quad b \in \mathbb{F}_p, \tag{6}$$

$$E'_6: \quad y^2 = x^3 + bu^{-1}, \tag{7}$$

where u is a quadratic and cubic non residue in $E(\mathbb{F}_{p^e})$ and $3|(p^e - 1)$. Isomorphism between $E'_6(\mathbb{F}_{p^e})$ and $E(\mathbb{F}_{p^{6e}})$, is given as follows:

$$\psi_6 : \begin{cases} E'_6(\mathbb{F}_{p^e}) \rightarrow E(\mathbb{F}_{p^{6e}}), \\ (x, y) \quad \mapsto (xu^{1/2}, yu^{1/2}). \end{cases} \tag{8}$$

In context of Ate-based pairing for KSS curve of embedding degree 18, sextic twist is considered to be the most efficient.

3. Improved Scalar Multiplication for $\mathbb{G}_2$ rational point

This section will introduce the proposal for efficient scalar multiplication of $\mathbb{G}_2$ rational points defined over KSS curve of embedding degree $k = 18$ in context of Ate-based pairing. An overview the proposed method is given next before diving into the detailed procedure.

3.0.1 Overview of the proposal

Figure 1 shows an overview of overall process of proposed scalar multiplication. Rational point groups $\mathbb{G}_1$, $\mathbb{G}_2$ and multiplicative group $\mathbb{G}_3$ groups will be defined at the beginning. Then a rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ will be calculated. Q has a special vector representation with 18 $\mathbb{F}_p$ elements for each coordinates. A random scalar s will be considered for scalar multiplication of $[s]Q$ which is denoted as input in Figure 1. After that we will consider an isomorphic map of rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ to its sextic twisted rational point $Q' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^3})$. At the same time we will obtain the z-adic representation of the scalar s. Next the some rational points defined over $E'(\mathbb{F}_{p^3})$ will be pre-computed by applying the skew Frobenius mapping. After that a multi-scalar multiplication technique will be applied to calculate the scalar multiplication in parallel. The result of this scalar multiplication will be defined over $\mathbb{F}_{p^3}$. Finally the result of the multi-scalar multiplication will be re-mapped to rational point in $E(\mathbb{F}_{p^{18}})$ to get the final result.

3.1 $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ groups

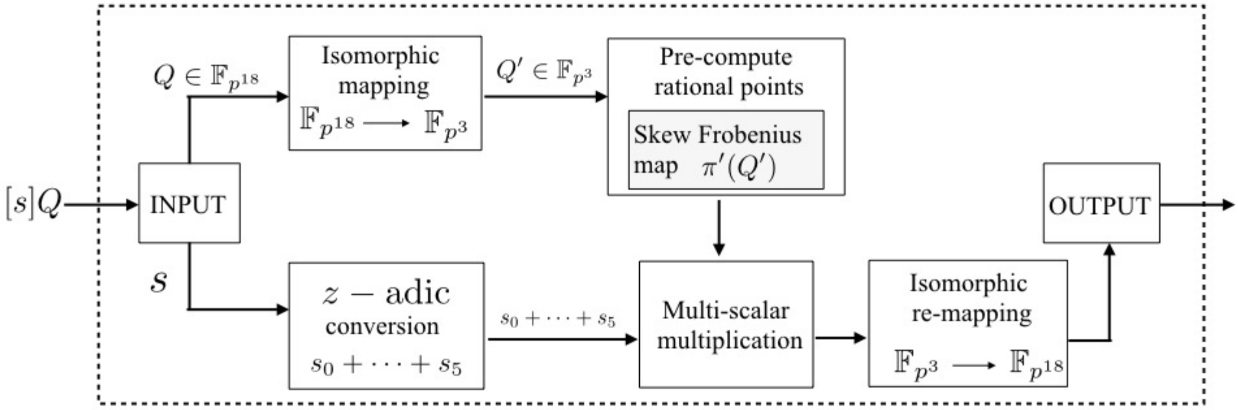
In the context of pairing-based cryptography, especially on KSS curve, three groups $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_3$ are considered. From [22], we define $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ as follows:

$$\mathbb{G}_1 = E(\mathbb{F}_{p^{18}})[r] \cap \mathrm{Ker}(\pi_p - [1]),$$
$$\mathbb{G}_2 = E(\mathbb{F}_{p^{18}})[r] \cap \mathrm{Ker}(\pi_p - [p]),$$
$$\mathbb{G}_3 = \mathbb{F}^*_{p^{18}} / (\mathbb{F}^*_{p^{18}})^r,$$

$$\alpha : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3, \tag{9}$$

where α denotes Ate pairing. In the case of KSS curve, $\mathbb{G}_1, \mathbb{G}_2$ are rational point groups and $\mathbb{G}_3$ is the multiplicative group in $\mathbb{F}_{p^{18}}$. They have the same order r.

In context of KSS curve, let us consider a rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ where Q satisfies the following relations,


$[s]Q$
INPUT
$Q \in \mathbb{F}_{p^{18}}$
s
Isomorphic mapping
$\mathbb{F}_{p^{18}} \longrightarrow \mathbb{F}_{p^3}$
$Q' \in \mathbb{F}_{p^3}$
Pre-compute rational points
Skew Frobenius map $\pi'(Q')$
$z-$adic conversion
$s_0 + \cdots + s_5$
$s_0 + \cdots + s_5$
Multi-scalar multiplication
Isomorphic re-mapping
$\mathbb{F}_{p^3} \longrightarrow \mathbb{F}_{p^{18}}$
OUTPUT

* s is a random scalar of size about 376-bit in the experiment

Fig. 1 Overview of the proposed scalar multiplication.

$$
\begin{aligned}
[p+1-t]Q &= \mathcal{O},\\
[t-1]Q &= [p]Q. \qquad (10)
\end{aligned}
$$

$$
\begin{aligned}
[\pi_p - p]Q &= \mathcal{O},\\
\pi_p(Q) &= [p]Q. \qquad (11)
\end{aligned}
$$

where $[t-1]Q = \pi_p(Q)$, by substituting $[p]Q$ in Eq. (10).

3.2 Isomorphic mapping between Q and Q'

Let us consider E is the KSS curve in base field $\mathbb{F}_{p^3}$ and E' is sextic twist of E given as follows:

$$
\begin{aligned}
E : y^2 &= x^3 + b, \qquad (12)\\
E' : y^2 &= x^3 + bi, \qquad (13)
\end{aligned}
$$

where $b \in \mathbb{F}_p$; $x, y, i \in \mathbb{F}_{p^3}$ and basis element i is the quadratic and cubic non residue in $\mathbb{F}_{p^3}$.

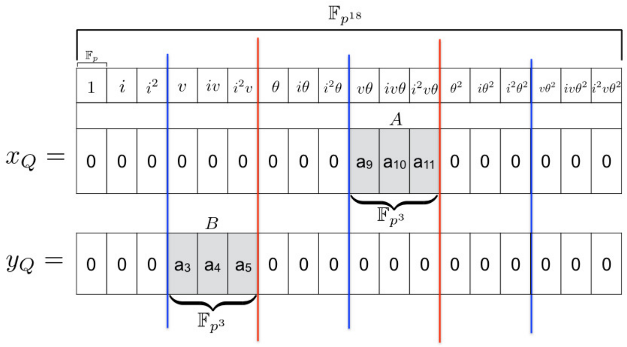
Rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ has a special vector representation with 18 $\mathbb{F}_p$ elements for each x_Q and y_Q coordinates. Figure 2 shows the structure of the coefficients of $Q \in \mathbb{F}_{p^{18}}$ and its sextic twisted isomorphic rational point $Q' \in \mathbb{F}_{p^3}$ in KSS curve. Among 18 elements, there are 3 continuous nonzero $\mathbb{F}_p$ elements which belongs to a $\mathbb{F}_{p^3}$ element. The other coefficients are zero. In this paper, considering parameter settings given in Table 2 of section 4; Q is given as $Q = (Av\theta, Bv)$, showed in Figure 2, where $A, B \in \mathbb{F}_{p^3}$ and v and θ are the basis elements of $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^{18}}$ respectively.

Let us consider the sextic twisted isomorphic sub-field rational point of Q as $Q' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^3})$ and x' and y' as the coordinates of Q'.

3.2.1 Mapping $Q = (Av\theta, Bv)$ to the rational point $Q' = (x', y')$

Let's multiply θ^{-6} with both side of Eq. (13), where $i = \theta^6$ and $v = \theta^3$.

$$
E' : \left(\frac{y}{\theta^3}\right)^2 = \left(\frac{x}{\theta^2}\right)^3 + b. \qquad (14)
$$



$$
\begin{aligned}
&a_j \in \mathbb{F}_p, \quad \text{where} \quad a_j = (0, 1, \cdots, 17)\\
&Q = (x_Q, y_Q) = (Av\theta, Bv) \in \mathbb{F}_{p^{18}}\\
&Q' = (x'_Q, y'_Q) = (Ai, Bi) \in \mathbb{F}_{p^3}
\end{aligned}
$$

Fig. 2 $Q \in \mathbb{F}_{p^{18}}$ and its sextic twisted isomorphic rational point $Q' \in \mathbb{F}_{p^3}$ structure in KSS curve.

Now θ^{-2} and θ^{-3} of Eq. (14) can be represented as follows:

$$
\begin{aligned}
\theta^{-2} &= i^{-1}\theta^4, \qquad (15a)\\
\theta^{-3} &= i^{-1}\theta^3. \qquad (15b)
\end{aligned}
$$

Let us represent $Q = (Av\theta, Bv)$ as follows:

$$
Q = (A\theta^4, B\theta^3), \quad \text{where } v = \theta^3. \qquad (16)
$$

From Eq. (15a) and Eq. (15b) $\theta^4 = i\theta^{-2}$ and $\theta^3 = i\theta^{-3}$ is substituted in Eq. (16) as follows:

$$
Q = (Ai\theta^{-2}, Bi\theta^{-3}), \qquad (17)
$$

where $Ai = x'$ and $Bi = y'$ are the coordinates of $Q' = (x', y') \in \mathbb{F}_{p^3}$. From the structure of $\mathbb{F}_{p^{18}}$, given in 2.3, this mapping has required no expensive arithmetic operation. Multiplication by the basis element i in $\mathbb{F}_{p^3}$ can be done by 1 bit wise left shifting since $c = 2$ is considered for towering in 2.3.

3.3 z-adic representation of scalar s

In context of KSS curve, properties of Q will be obtained to define the Eq. (11) relation. Next, a random scalar s will be considered for scalar multiplication of $[s]Q$. Then $(t-1)$-adic representation of s will be considered as Figure 3. Here s will be divided into two smaller coefficients S_H, S_L where S_L denotes lower bits of s, will be nearly equal to the size of $(t-1)$. On the other hand the higher order bits S_H will be the half of the size of $(t-1)$. Next, z-adic representation of S_H and S_L will be considered. Figure 4, shows the z-adic representation from where we find that scalar s is divided into 6 coefficients of z, where the size of z is about $1/4$ of that of $(t-1)$ according to Eq. (5c).

Figure 3 shows $(t-1)$-adic representation of scalar s.

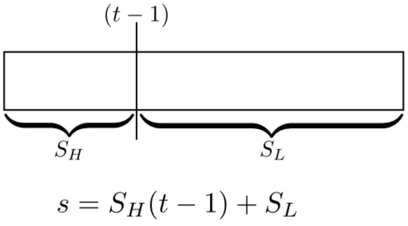


Fig. 3 $(t-1)$ -adic representation of scalar s.

Figure 4 shows the z-adic representation of scalar s. In the previous work on optimal-ate pairing, Aranha et al. [17] derived a relation from the parameter setting of KSS curve as follows:

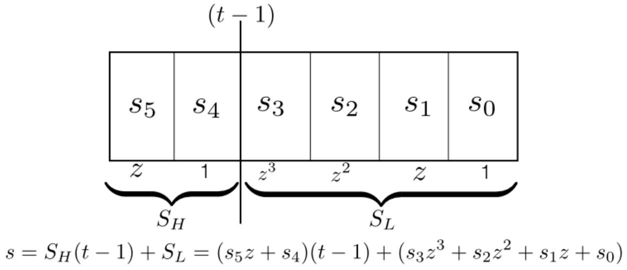

$(t-1)$
s_5
s_4
s_3
s_2
s_1
s_0
z
1
z^3
z^2
z
1
S_H
S_L
$s = S_H(t-1) + S_L = (s_5 z + s_4)(t-1) + (s_3 z^3 + s_2 z^2 + s_1 z + s_0)$

Fig. 4 z-adic and $(t-1)$-adic representation of scalar s.

$$z + 3p - p^4 \equiv 0 \bmod r, \tag{18}$$

where z is the *mother parameter* of KSS curve which is about six times smaller than order r.

Since Q is mapped to its ismorphic sextic twisted rational point Q', therefore we can consider scalar multiplication $[s]Q'$ where $0 \le s < r$. $[s]Q'$ will be calculated in $\mathbb{F}_{p^3}$ and eventually the result will be mapped to $\mathbb{F}_{p^{18}}$ to get the final result. From Eq. (5b) we know r is the order of KSS curve where $[r]Q = O$. Here, the bit size of s is nearly equal to r. In KSS curve t is $4/6$ times of r. Therefore, let us first consider $(t-1)$-adic representation of s as follows:

$$s = S_H(t-1) + S_L, \tag{19}$$

where s will be separated into two coefficients S_H and S_L. S_L will be nearly equal to the size of $(t-1)$ and S_H will be about half of $(t-1)$. In what follows, z-adic representation of S_H and S_L is given as:

$$\begin{aligned} S_H &= s_5 + s_4, \\ S_L &= s_3 z^3 + s_2 z^2 + s_1 z + s_0. \end{aligned}$$

Finally s can be represented as 6 coefficients as follows:

$$\begin{aligned} s &= \sum_{i=0}^{3} s_i z^i + (s_4 + s_5 z)(t-1), \\ s &= (s_0 + s_1 z) + (s_2 + s_3 z)z^2 + (s_4 + s_5 z)(t-1). \end{aligned} \tag{20}$$

3.3.1 Reducing number of Elliptic Curve Doubling (ECD) in $[s]Q'$.

Let us consider a scalar multiplication of $Q' \in \mathbb{G}_2'$ in Eq. (20) as follows:

$$[s]Q' = (s_0 + s_1 z)Q' + (s_2 + s_3 z)z^2 Q' + (s_4 + s_5 z)(t-1)Q'. \tag{21}$$

In what follows, $z^2 Q'$, $(t-1)Q'$ of Eq. (21) is denoted as Q_1' and Q_2' respectively. From Eq. (18) and Eq. (11) we can derive the Q_1' as follows:

$$\begin{aligned} Q_1' &= z^2 Q', \\ &= (9p^2 - 6p^5 + p^8)Q', \\ &= 9\pi'^2(Q') - 6\pi'^5(Q') + \pi'^8(Q'). \end{aligned} \tag{22}$$

where $\pi'(Q')$ is called the **skew Frobenius mapping** of rational point $Q' \in E'(\mathbb{F}_{p^3})$. Eq. (22) is simplified as follows by utilizing the properties of cyclotomic polynomial.

$$\begin{aligned} Q_1' &= 8\pi'^2(Q') - 5\pi'^5(Q'), \\ &= \pi'^2(8Q') - \pi'^5(5Q'). \end{aligned} \tag{23}$$

And from the Eq. (10) and Eq. (11), Q_2' is derived as,

$$Q_2' = \pi'(Q'). \tag{24}$$

Substituting Eq. (23) and Eq. (24) in Eq. (21), the following relation is obtained.

$$s[Q'] = (s_0 + s_1 z)Q' + (s_2 + s_3 z)Q_1' + (s_4 + s_5 z)Q_2'. \tag{25}$$

Using $z \equiv -3p + p^4 \pmod r$ from Eq. (18), $z(Q')$ can be pre-computed as follows:

$$z(Q') = \pi'(-3Q') + \pi'^4(Q'). \tag{26}$$

Table 1 13 pre-computed values of rational points

Pre-computed rational points	Skew Frobenius mapped rational points
	$z(Q')$
Q'_1	$z(Q'_1)$
Q'_2	$z(Q'_2)$
$Q'_1 + Q'_2$	$z(Q'_1) + z(Q'_2)$
$Q' + Q'_2$	$z(Q') + z(Q'_2)$
$Q' + Q'_1$	$z(Q') + z(Q'_1)$
$Q' + Q'_1 + Q'_2$	$z(Q') + z(Q'_1) + z(Q'_2)$

Table 1 shows all the pre-computed values of rational points defined over $\mathbb{F}_{p^3}$ for the proposed method. Pre-computed rational points are denoted inside angular bracket such as $< Q' + Q'_2 >$ in this paper.

3.4 Skew Frobenius map

Similar to Frobenius mapping, skew Frobenius map is the p-th power over the sextic twisted isomorphic rational points such as $Q' = (x', y')$ as follows:

$$\pi' : (x', y') \mapsto (x'^p, y'^p) \tag{27}$$

The detailed procedure to obtain the skew Frobenius map of $Q' = (x', y') \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^3})$ is given bellow:

$$\begin{aligned}
\pi'(x') &= (x')^p(i)^{1-p}(v)^{p-1}(\theta)^{p-1} \\
&= (x')^p(i)^{1-p}(\theta^4)^{p-1} \\
&= (x')^p(i^{-1})^p i(\theta^{p-1})^4 \\
&= (x')^p(i^{-1})^p i(i^{\frac{p-1}{6}})^4 \quad \text{where } \theta^6 = i \\
&= (x')^p(i^{-1})^p i(i^{\frac{p-1}{6}-1}i)^4 \\
&= (x')^p(i^{-1})^p i(i^{3\frac{\frac{p-7}{6}}{3}})^4 i^4 \\
&= (x')^p(i^{-1})^p i(2^{\frac{p-7}{18}})^4 2i \quad \text{where } i^3 = 2 \\
&= (x')^p(i^{-1})^p i(2^{\frac{2p-14}{9}+1})i \\
&= (x')^p(i^{-1})^p i(2^{\frac{2p-5}{9}})i,
\end{aligned} \tag{28a}$$

$$\begin{aligned}
\pi'(y') &= (y')^p(i)^{1-p}(v)^{p-1} \\
&= (y')^p(i^{-1})^p i(v^{6\frac{p-1}{6}}) \\
&= (y')^p(i^{-1})^p i(i^{3\frac{p-1}{6}}) \\
&= (y')^p(i^{-1})^p i2^{\frac{p-1}{6}}.
\end{aligned} \tag{28b}$$

Here $(i^{-1})^p i$, $(2^{\frac{2p-5}{9}})i$ and $2^{\frac{p-1}{6}}$ can be pre-computed.

3.5 Multi-scalar multiplication

Applying the the multi-scalar multiplication technique in Eq. (25) we can efficiently calculate the scalar multiplication in $\mathbb{F}_{p^3}$. Figure 5 shows an example of this multiplication. Suppose in an arbitrary index, from left to right, bit pattern of s_1, s_3, s_5 is 101 and at the same index s_0, s_2, s_4 is 111. Therefore we apply the pre-computed points $< z(Q') + z(Q'_2) >$ and $< Q' + Q'_1 + Q'_2 >$ as ECA in parallel. Then we perform ECD and move to the right next bit index to repeat the process until maximum length z-adic coefficient becomes zero.

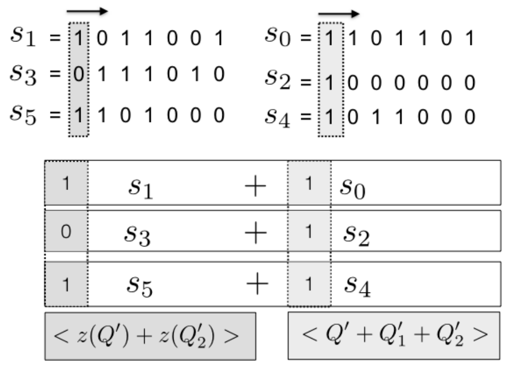


Fig. 5 Multi-scalar multiplication of s with Frobenius mapping.

As shown in Figure 5, during scalar multiplication, we are considering 3 pair of coefficients of z-adic representation as shown in Eq. (20). If we consider 6-coefficients for parallelization, it will require $2^6 \times 2$ pre-computed points. The chance of appearing each pre-computed point in the calculation will be only once that will cause redundancy.

3.5.1 Re-mapping rational points from $E'(\mathbb{F}_{p^3})$ to $E(\mathbb{F}_{p^{18}})$

After the multi-scalar multiplication, we need to remap the result to $\mathbb{F}_{p^{18}}$. For example let us consider re-mapping of $Q' = (x', y') \in E'(\mathbb{F}_{p^3})$ to $Q = (Av\theta, Bv) \in E(\mathbb{F}_{p^{18}})$. From Eq. (15a), Eq. (15b) and Eq. (14) it can be obtained as follows:

$$\begin{aligned}
xi^{-1}\theta^4 &= Av\theta, \\
yi^{-1}\theta^3 &= Bv,
\end{aligned}$$

which resembles that $Q = (Av\theta, Bv)$. Therefore it means that multiplying i^{-1} with the Q' coordinates and placing the resulted coefficients in the corresponding position of the coefficients in Q, will map Q' to Q. This mapping costs one $\mathbb{F}_{p^3}$ inversion of i which can be pre-computed and one $\mathbb{F}_p$ multiplication.

4. Simulation result evaluation

This section shows experimental result with the calculation cost. In the experiment we have compared the proposed method with three well studied method of scalar multiplication named binary method, sliding-window method and non-adjacent form (NAF) method. The mother parameter z is selected according to the suggestion of Scott et al. [19] to obtain $p = 508 \approx 511$-bit and $r = 376 \approx 384$-bit to simulate in 192-bit security level. Table 2 shows the parameter settings considered for the simulation.

Table 2 Parameter settings used in the experiment

Defined KSS curve	$y^2 = x^3 + 11$
Mother parameter z	65-bit
Characteristics $p(z)$	511-bit
Order $r(z)$	376-bit
Frobenius trace $t(z)$	255-bit
Persuadable security level	192-bit

Table 3 Computational Environment

	PC	iPhone6s
CPU [*]	2.7 GHz Intel Core i5	Apple A9 Dual-core 1.84 GHz
Memory	16 GB	2 GB
OS	Mac OS X 10.11.6	iOS 10.0
Compiler	gcc 4.2.1	gcc 4.2.1
Programming Language	C	Objective-C, C
Library	GMP 6.1.0	GMP 6.1.0

[*] Only single core is used from two cores.

Table 3 shows the environment, used to experiment and evaluate the proposed method.

In the experiment 100 random scalar numbers of size less than order r (378-bit) is generated. 13 ECA counted for pre-computed rational points is taken into account while the average is calculated for the proposed method. Window size of 4-bit is considered for sliding-window method. Therefore 14 pre-computed ECA is required. In addition, average execution time of the proposed method and the three other methods is also compared along with the operation count.

In what follows, "***With isomorphic mapping***" refers that skew Frobenius mapping technique is applied for Binary, Sliding-window and NAF methods. Therefore the scalar multiplication is calculated in $\mathbb{F}_{p^3}$ extension field. And for Proposed method it is skew Frobenius mapping with multi-scalar multiplication. On the other hand "***Without isomorphic mapping***" denotes that Frobenius map is not applied for any of the methods. In this case, all the scalar multiplication is calculated in $\mathbb{F}_{p^{18}}$ extension field.

Table 4 Comparison of average number of ECA and ECD

	Count of average number of ECA, ECD	
Methods	#ECA	#ECD
Binary	186	375
Sliding-window	102	376
NAF	127	377
Proposed	123	64

In Table 4 the operations of the *Proposed* method are counted in $\mathbb{F}_{p^3}$. On the other hand for Binary, Sliding-window and NAF method, the operations are counted in $\mathbb{F}_{p^{18}}$. The table clearly shows that in the *Proposed* method requires about 6 times less ECD than any other methods. The number of ECA is also reduced in the *Proposed* method by about 30% than binary method and almost same number of ECA of NAF.

Table 5 Comparison of execution time in [ms] for scalar multiplication

	Execution time in [ms]			
	With isomorphic mapping		Without isomorphic mapping	
Methods	PC	iPhone6s	PC	iPhone6s
Binary	5.4×10^1	8.4×10^1	1.2×10^3	1.8×10^3
Sliding-window	4.8×10^1	7.5×10^1	1.0×10^3	1.6×10^3
NAF	5.3×10^1	7.7×10^1	1.6×10^3	1.7×10^3
Proposed	1.6×10^1	2.4×10^1	-	-
Multi-scalar (only)	-	-	3.4×10^2	5.5×10^2

Analyzing Table 5, we can find that when isomorphic mapping and skew Frobenius mapping is not adapted for Binary, Sliding-window and NAF, then the scalar multiplication of proposed method is more than 60 times faster than other methods. However when isomorphic mapping is applied for the other methods then our proposed technique is more than 3 times faster. Another important comparison shows that when only multi-scalar multiplication is applied then our proposed methods is about 20 times faster. In every scenario our proposed method is faster than the other commonly used approaches.

The main focus of this experiment is to evaluate the acceleration ratio of scalar multiplication by applying the proposed approach on $\mathbb{G}_2$ rational point group of KSS curve of embedding degree 18. The experiment does not focus on efficiently implementing scalar multiplication for certain environment.

5. Conclusion and future work

In this paper we have proposed an efficient method to calculate elliptic curve scalar multiplication using skew Frobenius mapping over KSS curve in context of pairing based cryptography. The simulation result shows that multi-scalar multiplication after applying skew Frobenius mapping in $\mathbb{G}'_2$ can accelerate the scalar multiplication in $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ by more than 60 times than scalar multiplication of $\mathbb{G}_2$ rational point directly in $\mathbb{F}_{p^{18}}$. In the previous work of Sakemi et al. [14] has proposed skew Frobenius map for $\mathbb{G}_1$ rational point defined over BN curve. As a future work we would like to apply such approach on $\mathbb{G}_1$ rational point defined over KSS curve. Together with the proposed method, the skew Frobenius mapping of $\mathbb{G}_1$ will remarkably accelerate scalar multiplication over KSS curve in the context of pairing based cryptography.

References

[1] R. Sakai and M. Kasahara, "Id based cryptosystems with pairing on elliptic curve.," IACR Cryptology ePrint Archive, vol.2003, p.54, 2003.

[2] A. Joux, “A one round protocol for tripartite diffie–hellman,” International Algorithmic Number Theory Symposium, pp.385–393, Springer, 2000.

[3] D. Boneh, C. Gentry, and B. Waters, “Collusion resistant broadcast encryption with short ciphertexts and private keys,” Advances in Cryptology–CRYPTO 2005, pp.258–275, Springer, 2005.

[4] D. Boneh, X. Boyen, and H. Shacham, “Short group signatures,” Advances in Cryptology–CRYPTO 2004, pp.41–55, Springer, 2004.

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

[6] F. Vercauteren, “Optimal pairings,” Information Theory, IEEE Transactions on, vol.56, no.1, pp.455–461, 2010.

[7] S. Matsuda, N. Kanayama, F. Hess, and E. Okamoto, “Optimised versions of the ate and twisted ate pairings,” in Cryptography and Coding, pp.302–312, Springer, 2007.

[8] Y. Nogami, M. Akane, Y. Sakemi, H. Katou, and Y. Morikawa, “Integer variable chi-based ate pairing,” Pairing-Based Cryptography - Pairing 2008, Second International Conference, Egham, UK, September 1-3, 2008. Proceedings, pp.178–191, 2008.

[9] A.J. Devegili, M. Scott, and R. Dahab, “Implementing cryptographic pairings over barreto-naehrig curves,” International Conference on Pairing-Based Cryptography, pp.197–207, Springer, 2007.

[10] E. Kachisa, E. Schaefer, and M. Scott, “Constructing brezing-weng pairing-friendly elliptic curves using elements in the cyclotomic field,” Pairing-Based Cryptography–Pairing 2008, pp.126–135, 2008.

[11] J.H. Silverman, G. Cornell, and M. Artin, Arithmetic geometry, Springer, 1986.

[12] D. Freeman, M. Scott, and E. Teske, “A taxonomy of pairing-friendly elliptic curves,” Journal of cryptology, vol.23, no.2, pp.224–280, 2010.

[13] Y. Nogami, Y. Sakemi, T. Okimoto, K. Nekado, M. Akane, and Y. Morikawa, “Scalar multiplication using frobenius expansion over twisted elliptic curve for ate pairing based cryptography,” IEICE Transactions, vol.92-A, no.1, pp.182–189, 2009.

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

[15] P.S.L.M. Barreto and M. Naehrig, “Pairing-friendly elliptic curves of prime order,” Selected Areas in Cryptography, 12th International Workshop, SAC 2005, Kingston, ON, Canada, August 11-12, 2005, Revised Selected Papers, pp.319–331, 2005.

[16] D.V. Bailey and C. Paar, “Optimal extension fields for fast arithmetic in public-key algorithms,” Advances in Cryptology-CRYPTO’98, pp.472–485, Springer, 1998.

[17] D.F. Aranha, L. Fuentes-Castañeda, E. Knapp, A. Menezes, and F. Rodríguez-Henríquez, “Implementing pairings at the 192-bit security level,” in Pairing-Based Cryptography–Pairing 2012, pp.177–195, Springer, 2012.

[18] L.C. Washington, Elliptic curves: number theory and cryptography, CRC press, 2008.

[19] M. Scott, “On the efficient implementation of pairing-based protocols,” in Cryptography and Coding, pp.296–308, Springer, 2011.

[20] T. Kim and R. Barbulescu, “Extended tower number field sieve: A new complexity for medium prime case,” tech. rep., IACR Cryptology ePrint Archive, 2015: 1027, 2015.

[21] D.V. Bailey and C. Paar, “Efficient arithmetic in finite field extensions with application in elliptic curve cryptography,” J. Cryptology, vol.14, no.3, pp.153–176, 2001.

[22] Y. Mori, S. Akagi, Y. Nogami, and M. Shirase, “Pseudo 8–sparse multiplication for efficient ate–based pairing on barreto–naehrig curve,” in Pairing-Based Cryptography–Pairing 2013, pp.186–198, Springer, 2013.

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.

Md. Al-Amin Khandaker graduated from Jahangirnagar University in 2011. He is now pursuing his PhD in the field of Finite Field Theory andits application in cryptography in Okayama University under the supervision of Dr. Yasuyuki NOGAMI. His main fields of research are pairing based cryptography and its applications. He is a student member of IEEE.

Yasuyuki NOGAMI graduated from Shinshu University in 1994 and received the PhD degree in 1999 from Shinshu University. He is now an associate professor of Okayama University. His main fields of research are finite field theory and its applications such as recent public key cryptographies. He is now studying about elliptic curve cryptography, pairing-based cryptography, Lattice-based cryptography, pseudo random number generator, Advanced Encryption Standard, and homomorphic encryptions. Recently, he is a member of security research group in Okayama university and particularly focusing on IoT security from the viewpoints of software and hardware implementations. He is a member of IEICE and IEEE.