Efficient Scalar Multiplication for Ate Based Pairing over KSS Curve of Embedding Degree 18

Md. Al-Amin Khandaker[1](✉), Yasuyuki Nogami[1], Hwajeong Seo[2], and Sylvain Duquesne[3]

[1] Graduate School of Natural Science and Technology,
Okayama University, Okayama, Japan
khandaker@s.okayama-u.ac.jp, yasuyuki.nogami@okayama-u.ac.jp
[2] Pusan National University, Busan, South Korea
hwajeong@pusan.ac.kr
[3] Université Rennes I, Rennes, France
sylvain.duquesne@univ-rennes1.fr

Abstract. Efficiency of the next generation pairing based security protocols rely not only on the faster pairing calculation but also on efficient scalar multiplication on higher degree rational points. In this paper we proposed a scalar multiplication technique in the context of Ate based pairing with Kachisa-Schaefer-Scott (KSS) pairing friendly curves with embedding degree $k = 18$ at the 192-bit security level. From the systematically obtained characteristics p, order r and Frobenious trace t of KSS curve, which is given by certain integer z also known as mother parameter, we exploit the relation $\#E(\mathbb{F}_p) = p+1-t \bmod r$ by applying Frobenius mapping with rational point to enhance the scalar multiplication. In addition we proposed z-adic representation of scalar s. In combination of Frobenious mapping with multi-scalar multiplication technique we efficiently calculate scalar multiplication by s. Our proposed method can achieve 3 times or more than 3 times faster scalar multiplication compared to binary scalar multiplication, sliding-window and non-adjacent form method.

Keywords: KSS curve · Frobenius mapping · Scalar multiplication

1 Introduction

The intractability of Elliptic Curve Discrete Logarithm Problem (ECDLP) spurs on many innovative pairing based cryptographic protocols. Pairing based cryptography is considered to be the basis of next generation security. Recently a number of unique and innovative pairing based cryptographic applications such as identity based encryption scheme [17], broadcast encryption [8] and group signature authentication [7] surge the popularity of pairing based cryptography. In such consequence Ate-based pairings such as Ate [9] and Optimal-ate [20],

D. Choi and S. Guilley (Eds.): WISA 2016, LNCS 10144, pp. 221–232, 2017.
DOI: 10.1007/978-3-319-56549-1_19

twisted Ate [13] and χ-Ate [15] pairings has gained much attention. To make such cryptographic applications practical, these pairings need to be computed efficiently and fast. This paper focuses on such Ate-based pairings.

Pairing is a bilinear map from two rational point $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group $\mathbb{G}_3$ [19] typically denoted by $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$. In the case of Ate-based pairing, $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ are defined as follows:

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

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

where α denotes Ate pairing. In general, pairings are only found in certain extension field $\mathbb{F}_{p^k}$, where p is the prime number, also know as characteristics and the minimum extension degree k is called *embedding* degree. The rational points $E(\mathbb{F}_{p^k})$ are defined over a certain pairing friendly curve of embedded extension field of degree k. Security level of pairing based cryptography depends on the sizes of both r and p^k, where r generally denotes the largest prime number that divides the order $\#E(\mathbb{F}_p)$. The next generation security of pairing-based cryptography needs $\log_2 r \approx 256$ bits and $\log_2 p^k \approx 3000$ to 5000 bits. Therefore taking care of $\rho = (\log_2 p)/(\log_2 r)$, k needs to be 12 to 20. This paper has considered Kachisa-Schaefer-Scott (KSS) [12] pairing friendly curves of embedding degree $k = 18$ described in [10]. Pairing on KSS curve is considered to be the basis of next generation security as it conforms 192-bit security level. Making the pairing practical over KSS curve depends on several factors such as efficient pairing algorithm, efficient extension field arithmetic and efficiently performing scalar multiplication. Many researches have conducted on efficient pairing algorithms [4] and curves [5] along with extension field arithmetic [2]. This paper focuses on efficiently performing scalar multiplication in $\mathbb{G}_2$ by scalar s, since scalar multiplication is required repeatedly in cryptographic calculation. Scalar multiplication is also considered to be the one of the most time consuming operation in cryptographic scene. Moreover in asymmetric pairing such as Ate-based pairing, scalar multiplication in $\mathbb{G}_2$ 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 many researches for efficient scalar multiplication in $\mathbb{G}_1$.

Scalar multiplication by s means $(s - 1)$ times elliptic additions of a given rational point on the elliptic curve. This elliptic addition is not as simple as addition of extension field, but it requires 3 multiplications plus an inversion of the extension field. General approaches 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 $\mathbb{F}_{p^k}$. Frobenious map $\pi : (x, y) \mapsto (x^p, y^p)$ is the p-th power of the rational point (x, y) defined over $\mathbb{F}_{p^k}$. In this paper we also exploited the Frobenious trace t, $t = p + 1 - \#E(\mathbb{F}_p)$ defined over KSS curve. In the previous work on optimal-ate pairing, Aranha et al. [1] derived an important relation: $z \equiv -3p + p^4 \bmod r$, where z is the mother parameter of KSS curve and z is about six times smaller than the size of order r. We have utilized this relation to construct z-adic representation of scalar s which is introduced in Sect. 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 at least 3 times or more than 3 times faster than 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.

As shown in the previous work of scalar multiplication on sextic twisted BN curve by Nogami et al. [16], we can consider sub-field sextic twisted curve in the case of KSS curve of embedding degree 18. Let us denote the sub-field sextic twisted curve by E'. It will include sextic twisted isomorphic rational point group denoted as $\mathbb{G}_2'$. In KSS curve, $\mathbb{G}_2$ is defined over $\mathbb{F}_{p^{18}}$ whereas its sub-field isomorphic group $\mathbb{G}_2'$ is defined over $\mathbb{F}_{p^3}$. Important feature of this sextic twisted isomorphic group is, all the scalar multiplication in $\mathbb{G}_2$ is mapped with $\mathbb{G}_2'$ and it can be efficiently carried out by applying skew Frobenious map. Then, the resulted points can be re-mapped to $\mathbb{G}_2$ in $\mathbb{F}_{p^{18}}$. This above mentioned skew Frobenious mapping in sextic twisted isomorphic group will calculate more faster scalar multiplication. However, the main focus of this paper is presenting the process of splitting the scalar into z-adic representation and applying Frobenius map in combination with multi-scalar multiplication technique.

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 [21]

Let $\mathbb{F}_p$ be a prime field. Elliptic curve over $\mathbb{F}_p$ is defined as,

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

where $4a^3 + 27b^2 \neq 0$ and $a, b \in \mathbb{F}_p$. Points satisfying Eq. (1) are known as rational points on the curve.

Point Addition. Let $E(\mathbb{F}_p)$ be the set of all rational points on the curve defined over $\mathbb{F}_p$ and it includes the point at infinity denoted by $\mathcal{O}$. The order of $E(\mathbb{F}_p)$ is denoted by $\#E(\mathbb{F}_p)$ where $E(\mathbb{F}_p)$ forms an additive group for the elliptic addition. Let us consider two rational points $L = (x_l, y_l)$, $M = (x_m, y_m)$, and their addition $N = L + M$, where $N = (x_n, y_n)$ and $L, M, N \in E(\mathbb{F}_p)$. Then, the x and y coordinates of N is calculated as follows:

$$(x_n, y_n) = ((\lambda^2 - x_l - x_m), (x_l - x_n)\lambda - y_l), \tag{2a}$$

where λ is given as follows:

$$\lambda = \begin{cases} (y_m - y_l)(x_m - x_l)^{-1} & (L \neq M \text{ and } x_m \neq x_l), \\ \\ (3x_l^2 + a)(2y_l)^{-1} & (N = M \text{ and } y_l \neq 0), \end{cases} \tag{2b}$$

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

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

$$[s]M = \underbrace{M + M + \cdots + M}_{s-1 \quad \text{times additions}} . \tag{3}$$

If $s = r$, where r is the order of the curve then $[r]M = \mathcal{O}$. When $[s]M = N$, if s is unknown, then the solving s from M and N is known as elliptic curve discrete logarithm problem (ECDLP). The security of elliptic curve cryptography lies on the difficulty of solving ECDLP.

2.2 KSS Curve

KSS curve is a non super-singular pairing friendly elliptic curve of embedding degree 18 [12]. The equation of KSS curve defined over $\mathbb{F}_{p^{18}}$ is given by

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

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:

$$\begin{aligned} p(z) &= (z^8 + 5z^7 + 7z^6 + 37z^5 + 188z^4 + 259z^3 + 343z^2 \\ &\quad +1763z + 2401)/21, && \text{(5a)} \\ r(z) &= (z^6 + 37z^3 + 343)/343, && \text{(5b)} \\ t(z) &= (z^4 + 16z + 7)/7, && \text{(5c)} \end{aligned}$$

where z is such that $z \equiv 14 \pmod{42}$ and the co-factor is $\rho = (\log_2 p / \log_2 r)$ is about 4/3. The order of rational points $\#E(\mathbb{F}_{p^{18}})$ on KSS curve can be obtained by the following relation.

$$\#E(\mathbb{F}_{p^{18}}) = p^{18} + 1 - t_{18}, \tag{6}$$

where $t_{18} = \alpha^{18} + \beta^{18}$ and α, β are complex numbers such that $\alpha + \beta = t$ and $\alpha\beta = p$. Since Aranha et al. [1] and Scott et al. [18] has proposed 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 considered $p = 511$-bit.

Frobenius Mapping of Rational Point in $\boldsymbol{E}(\mathbb{F}_{p^{18}})$. Let (x, y) be the rational point in $E(\mathbb{F}_{p^{18}})$. Frobenious map $\pi_p : (x, y) \mapsto (x^p, y^p)$ is the p-th power of the rational point defined over $\mathbb{F}_{p^{18}}$. Some previous work [11] has been done on constructing Frobenius mapping and utilizing it to calculate scalar multiplication. Nogami et al. [16] showed efficient scalar multiplication in the context of Ate-based pairing in BN curve of embedding degree $k = 12$. This paper has exploited Frobenius mapping for efficient scalar multiplication for the case of KSS curve.

2.3 $\mathbb{F}_{p^{18}}$ Extension Field Arithmetic

In context of pairing, it is required to perform arithmetic in higher extension fields, such as $\mathbb{F}_{p^k}$ for moderate value of k [19]. Therefore it is important to construct the field as a tower of extension fields [6] to perform arithmetic operation efficiently. Higher level computations can be calculated as a function of lower level computations. Because of that an efficient implementation of lower level arithmetic results in the good performance of arithmetic in higher degree fields.

In this paper extension field $\mathbb{F}_{p^{18}}$ is represented as a tower of sub field to improve arithmetic operations. In some previous works, such as Bailey et al. [3] explained tower of extension by using irreducible binomials. In what follows, let $(p-1)$ is divisible by 3 and θ is a quadratic and cubic non residue in $\mathbb{F}_p$. Then for case of KSS-curve [12], where $k = 18$, $\mathbb{F}_{p^{18}}$ is constructed as tower field with irreducible binomial as follows:

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

According to previous work such as Aranha et al. [1], the base extension field is $\mathbb{F}_{p^3}$ for the *sextic twist* of KSS curve.

3 Efficient Scalar Multiplication

In this section we will introduce our proposal for efficient scalar multiplication in $\mathbb{G}_2$ rational point for Ate-based pairing on KSS curve. Before going to detailed procedure, an overview about how the proposed method will calculate scalar multiplication efficiently of $\mathbb{G}_2$ rational point is given.

Overview. At first $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ groups will be defined. Then a rational point $Q \in \mathbb{G}_2$ will be considered. In context of KSS curve, properties of Q will be obtained to define the Eq. (9) relation. Next, a scalar s will be considered for scalar multiplication of $[s]Q$. After that, as Fig. 1, $(t-1)$-adic representation of s will be considered, where s will be divided into two smaller parts S_H, S_L. The lower bits of s, represented as S_L, will be nearly equal to the size of $(t-1)$ while 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 2, 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 $(t-1)$ as Eq. (5c). Next we will pre-compute the Frobenius maps of some rational points defined by detailed procedure. As shown in Eq. (12), considering 3 pairs from the coefficients we will apply the mult-scalar multiplication in addition with Frobenious mapping, as shown in Fig. 3 to calculate scalar multiplication efficiently. Later part of this section will provide the detailed procedure of the proposal.

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

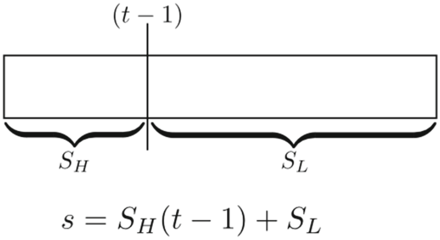

Fig. 1. $(t-1)$ -adic representation of scalar s.

Figure 2 shows the final z-adic representation of scalar s.

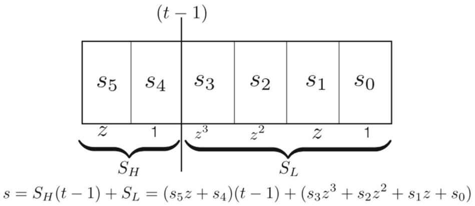
$(t-1)$
s_5
s_4
s_3
s_2
s_1
s_0
z
1
z^3
z^2
z
1
S_H
S_L
$s = S_H(t-1) + S_L = (s_5z + s_4)(t-1) + (s_3z^3 + s_2z^2 + s_1z + s_0)$

Fig. 2. z-adic and $(t-1)$-adic representation of scalar s.

Figure 3 shows, an example of multi-scalar multiplication process, implemented in the experiment.

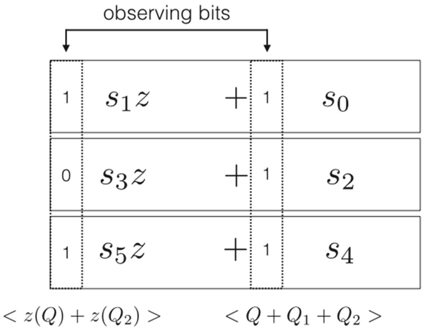

Fig. 3. Multi-scalar multiplication of s with Frobenius mapping.

$\mathbb{G}_1$, $\mathbb{G}_2$ 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 [14], we define $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ as follows:

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

$$\alpha : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3, \tag{7}$$

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.

Let us consider a rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$. In the case of KSS curve, it is known that Q satisfies the following relations,

$$\begin{aligned}\left[p+1-t\right]Q &= \mathcal{O},\\ \left[t-1\right]Q &= \left[p\right]Q.\end{aligned} \tag{8}$$

$$\begin{aligned}[\pi_p - p]Q &= \mathcal{O},\\ \pi_p(Q) &= [p]Q.\end{aligned} \tag{9}$$

Thus, these relations can accelerate a scalar multiplication in $\mathbb{G}_2$. Substituting $[p]Q$ in Eq. (8) we find $[t-1]Q = \pi_p(Q)$.

***z*-adic representation of scalar *s*.** From the previous work on optimal-ate pairing, Aranha et al. [1] derived the following relation from parameters Eq. (5a), (5b) and (5c) of KSS curve.

$$z + 3p - p^4 \equiv 0 \bmod r. \tag{10}$$

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

Let us consider scalar multiplication $[s]Q$, where $0 \leq s < r$. From Eq. (5b) we know r is the order of KSS curve where $[r]Q = \mathcal{O}$. 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:

$$s = S_H(t-1) + S_L, \tag{11}$$

where s will be separated into two coefficients S_H and S_L. Size of S_L will be nearly equal to the size of $(t-1)$ and S_H will be about half of $(t-1)$. Now we consider z-adic representation of S_H and S_L as follows:

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

Finally s can be represented as 6 coefficients as follows:

$$\begin{aligned} s &= \sum_{i=0}^{3} s_i z^i + (s_4 + s_5 z)(t-1), \\ s &= (s_0 + s_1 z) + (s_2 + s_3 z)z^2 + (s_4 + s_5 z)(t-1). \end{aligned} \tag{12}$$

Reducing the Number of ECA and ECD for Calculating $[\boldsymbol{s}]\boldsymbol{Q}$. Let us consider a scalar multiplication of $Q \in \mathbb{G}_2$ in Eq. (12) as follows:

$$[s]Q = (s_0 + s_1 z)Q + (s_2 + s_3 z)z^2 Q + (s_4 + s_5 z)(t-1)Q. \tag{13}$$

Let us denote $z^2 Q$, $(t-1)Q$ of Eq. (13) as Q_1 and Q_2 respectively. From Eqs. (9) and (10) we can derive the Q_1 as follows:

$$\begin{aligned} Q_1 &= z^2 Q, \\ &= (9p^2 - 6p^5 + p^8)Q, \\ &= 9\pi^2(Q) - 6\pi^5(Q) + \pi^8(Q). \end{aligned} \tag{14}$$

Using the properties of cyclotomic polynomial Eq. (14) is simplified as,

$$\begin{aligned} Q_1 &= 8\pi^2(Q) - 5\pi^5(Q), \\ &= \pi^2(8Q) - \pi^5(5Q). \end{aligned} \tag{15}$$

And from the Eqs. (8) and (9), Q_2 is derived as,

$$Q_2 = \pi(Q). \tag{16}$$

Substituting Eqs. (15) and (16) in Eq. (13), the following relation is obtained.

$$s[Q] = (s_0 + s_1 z)Q + (s_2 + s_3 z)Q_1 + (s_4 + s_5 z)Q_2. \tag{17}$$

Using $z \equiv -3p + p^4 \pmod{r}$ from Eq. (10), $z(Q)$ can be pre-computed as follows:

$$z(Q) = \pi(-3Q) + \pi^4(Q). \tag{18}$$

Table 1 shows all the pre-computed values of rational points for the proposed method. In this paper pre-computed rational points are denoted such as $< Q + Q_2 >$. Finally applying the multi-scalar multiplication technique in Eq. (17) we can efficiently calculate the scalar multiplication. Figure 3 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.

Table 1. Pre-computed values of rational point for efficient scalar multiplication

	$z(Q)$
Q_1	$z(Q_1)$
Q_2	$z(Q_2)$
$Q_1 + Q_2$	$z(Q_1) + z(Q_2)$
$Q + Q_2$	$z(Q) + z(Q_2)$
$Q + Q_1$	$z(Q) + z(Q_1)$
$Q + Q_1 + Q_2$	$z(Q) + z(Q_1) + z(Q_2)$

As shown in Fig. 3, during scalar multiplication in parallel, we are considering Eq. (12) like 3 pair of coefficients of z-adic representation. If we consider 6-coefficients for parallelization, we will need to calculate $2^6 \times 2$ pre-computed points. The chance of appearing each pre-computed point in parallel calculation will be only once which will make the pre-calculated points redundant.

4 Experimental Result Evaluation

In order to demonstrate the efficiency of the proposal, this section shows some 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.

In the experiment the following parameters are considered for the KSS curve $y^2 = x^3 + 11$.

$$\begin{aligned} z &= 65\text{-bit}, \\ p &= 511\text{-bit}, \\ r &= 378\text{-bit}, \\ t &= 255\text{-bit}. \end{aligned}$$

The mother parameter z is also selected accordingly to find out $\mathbb{G}_2$ rational point Q.

500 scalar numbers of size (about 377-bit) less than order r is generated randomly in the experiment. Then average number of ECA and ECD for the proposed method and the three other methods is calculated for a scalar multiplication. 13 pre-computed ECA is taken into account while the average is calculated for the proposed method. In case of sliding-window method window size 4-bit is considered. Therefore 14 pre-computed ECA is required. In addition, average execution time of the proposed method and the three other methods is also compared.

Table 2 shows the environment, used to experiment and evaluate the proposed method.

Table 2. Computational environment

	PC	iPhone6s
CPU[a]	2.7 GHz Intel Core i5	Apple A9 Dual-core 1.84 GHz
Memory	16 GB	2 GB
OS	Mac OS X 10.11.4	iOS 9.3.1
Compiler	gcc 4.2.1	gcc 4.2.1
Programming Language	C	Objective-C, C
Library	GNU MP 6.1.0	GNU MP 6.1.0

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

Analyzing Table 3 we can find that our proposed method requires more than 5 times less ECD than binary method, sliding-window method and NAF method. The number of ECA is also reduced in the proposed method by about 30% than binary method.

In this experiment, execution time may seems slower than other efficient algorithm such as Montgomery reduction. But the main purpose of this execution time comparison is to compare the ratio of the execution time of the proposed method with other well studied methods. The result shows that proposed method is at least 3 times faster than the other methods. Other acceleration techniques

Table 3. Comparative result of average number of ECA and ECD and execution time in [ms] for scalar multiplication

	Average ECA, ECD and execution time [ms] comparison			
	PC		PC	iPhone 6s
Methods	#ECA	#ECD	Execution time	Execution time
Binary	187	376	1.15×10^3	1.3×10^3
Sliding-window	103	376	1.14×10^3	1.10×10^3
NAF	126	377	1.03×10^3	1.13×10^3
Proposed	124	64	3.36×10^2	3.76×10^2

such as Montgomery reduction, Montgomery trick and efficient coordinates can be applied to this proposed method to enhance its execution time.

5 Conclusion and Future Work

In this paper we have proposed an efficient method to calculate elliptic curve scalar multiplication using Frobenious mapping over KSS curve in context of pairing based cryptography. We have also applied $(t-1)$-adic and z-adic representation on the scalar and have applied multi-scalar multiplication technique to calculate scalar multiplication in parallel. We have evaluated and analyzed the improvement by implementing a simulation for large size of scalar in 192-bit security level. The experimented result shows that our proposed method is at least 3 times efficient in context of execution time and takes 5 times less number of elliptic curve doubling than binary method, sliding-window method and non-adjacent form method. As a future work we would like to enhance its computation time by applying not only Montgomery reduction but also skew Frobenius map in sub-field isomorphic rational point group technique and test the effect of the improvement in some pairing application for practical case.

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., 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.: Optimal extension fields for fast arithmetic in public-key algorithms. In: Krawczyk, H. (ed.) CRYPTO 1998. LNCS, vol. 1462, pp. 472–485. Springer, Heidelberg (1998). doi:10.1007/BFb0055748
3. Bailey, D.V., Paar, C.: Efficient arithmetic in finite field extensions with application in elliptic curve cryptography. J. Cryptology **14**(3), 153–176 (2001). http://dx.doi.org/10.1007/s001450010012
4. Barreto, P.S.L.M., Kim, H.Y., Lynn, B., Scott, M.: Efficient algorithms for pairing-based cryptosystems. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 354–369. Springer, Heidelberg (2002). doi:10.1007/3-540-45708-9_23
5. 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
6. Benger, N., Scott, M.: Constructing Tower extensions of finite fields for implementation of pairing-based cryptography. In: Hasan, M.A., Helleseth, T. (eds.) WAIFI 2010. LNCS, vol. 6087, pp. 180–195. Springer, Heidelberg (2010). doi:10.1007/978-3-642-13797-6_13
7. Boneh, D., Boyen, X., Shacham, H.: Short group signatures. In: Franklin, M. (ed.) CRYPTO 2004. LNCS, vol. 3152, pp. 41–55. Springer, Heidelberg (2004). doi:10.1007/978-3-540-28628-8_3

8. Boneh, D., Gentry, C., Waters, B.: Collusion resistant broadcast encryption with short ciphertexts and private keys. In: Shoup, V. (ed.) CRYPTO 2005. LNCS, vol. 3621, pp. 258–275. Springer, Heidelberg (2005). doi:10.1007/11535218_16
9. 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)
10. Freeman, D., Scott, M., Teske, E.: A taxonomy of pairing-friendly elliptic curves. J. Cryptology **23**(2), 224–280 (2010)
11. Iijima, T., Matsuo, K., Chao, J., Tsujii, S.: Construction of frobenius maps of twists elliptic curves and its application to elliptic scalar multiplication. In: Proceedings of SCIS, pp. 699–702 (2002)
12. 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
13. 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
14. 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, Cham (2014). doi:10.1007/978-3-319-04873-4_11
15. 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, 1–3 September 2008, pp. 178–191 (2008). http://dx.doi.org/10.1007/978-3-540-85538-5_13
16. Nogami, Y., Sakemi, Y., Okimoto, T., Nekado, K., Akane, M., Morikawa, Y.: Scalar multiplication using frobenius expansion over twisted elliptic curve for ate pairing based cryptography. IEICE Trans. **92**-A(1), 182–189 (2009). http://search.ieice.org/bin/summary.php?id=e92-a_1_182&category=A&year=2009&lang=E&abst=
17. Sakai, R., Kasahara, M.: Id based cryptosystems with pairing on elliptic curve. IACR Cryptology ePrint Archive 2003, 54 (2003)
18. Scott, M.: On the efficient implementation of pairing-based protocols. In: Chen, L. (ed.) IMACC 2011. LNCS, vol. 7089, pp. 296–308. Springer, Heidelberg (2011). doi:10.1007/978-3-642-25516-8_18
19. Silverman, J.H., Cornell, G., Artin, M.: Arithmetic Geometry. Springer, Heidelberg (1986)
20. Vercauteren, F.: Optimal pairings. IEEE Trans. Inf. Theory **56**(1), 455–461 (2010)
21. Washington, L.C.: Elliptic Curves: Number Theory and Cryptography. CRC Press, Boca Raton (2008)