Journal of information and communication convergence engineering
http://jicce.org

J. Inf. Commun. Converg. Eng. 15(2): 97-103, Jun. 2017 Regular paper

A Comparative Study of Twist Property in KSS Curves of Embedding Degree 16 and 18 from the Implementation Perspective

Md. Al-Amin Khandaker[1], **Taehwan Park**[2], **Yasuyuki Nogami**[1*], **and Howon Kim**[2], ***Member, KIICE***

[1]Department of Information and Communication Systems, Okayama University, Okayama 700-8530, Japan
[2]Department of Electrical and Computer, Pusan National University, Busan 46241, Korea

Abstract

Implementation of faster pairing calculation is the basis of efficient pairing-based cryptographic protocol implementation. Generally, pairing is a costly operation carried out over the extension field of degree $\boldsymbol{k \geq 12}$. But the twist property of the pairing friendly curve allows us to calculate pairing over the sub-field twisted curve, where the extension degree becomes $\boldsymbol{k/d}$ and twist degree $\boldsymbol{d = 2, 3, 4, 6}$. The calculation cost is reduced substantially by twisting but it makes the discrete logarithm problem easier if the curve parameters are not carefully chosen. Therefore, this paper considers the most recent parameters setting presented by Barbulescu and Duquesne [1] for pairing-based cryptography; that are secure enough for 128-bit security level; to explicitly show the *quartic twist* $(\boldsymbol{d = 4})$ and *sextic twist* $(\boldsymbol{d = 6})$ mapping between the isomorphic rational point groups for KSS (Kachisa-Schaefer-Scott) curve of embedding degree $\boldsymbol{k = 16}$ and $\boldsymbol{k = 18}$, receptively. This paper also evaluates the performance enhancement of the obtained twisted mapping by comparing the elliptic curve scalar multiplications.

Index Terms: Isomorphic mapping, KSS curve, Pairing-based cryptography, Quartic twist, Sextic twist

I. INTRODUCTION

Development of optimized implementation of the underlying mathematical operations in cryptographic techniques is an integral part of information security. Among the public key cryptographic techniques, pairing-based cryptography is comparatively a new branch of cryptographic research which generally deals with a specific algorithm with some certain characteristics. In general, pairing is a bilinear map from two additive rational point groups $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group $\mathbb{G}_3$ [2], typically denoted by $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$. In practice, pairing is realized by the elliptic curves defined over the extension field.

Implementation of a pairing requires special elliptic curve usually known *pairing-friendly* curves. This paper considers a well-studied non-supersingular pairing-friendly curve named Kachisa-Schaefer-Scott (KSS) curve [3] of the embedding degree $k \geq 16$. It means pairing needs to be calculated in extension field of degree $k \geq 16$. Thanks to the isomorphic twist property of the KSS curve which allows to calculate the pairing and the related operations in lower degree extension field that makes calculation more efficient. This paper focuses on the explicit derivation and implementation of this twist property for KSS curve of embedding degree $k = 16$ and $k = 18$ named KSS16 and KSS18, respectively throughout this paper.

Received 05 June 2017, **Revised** 08 June 2017, **Accepted** 13 June 2017
*__Corresponding Author__ Yasuyuki Nogami (E-mail: yasuyuki.nogami@okayama-u.ac.jp, Tel: +81-86-251-8127)
Department of Information and Communication Systems, Okayama University, Okayama 700-8530, Japan.

Open Access http://doi.org/10.6109/jicce.2017.15.2.97 print ISSN: 2234-8255 online ISSN: 2234-8883

The advantage of the derived isomorphic twisted mapping is examined by performing elliptic curve scalar multiplication on $\mathbb{G}_2 \subset E(\mathbb{F}_{p^k})$ rational point, since scalar multiplication is required repeatedly in cryptographic calculation. Three well-known scalar multiplication algorithms are considered for the comprehensive experimental implementation named as binary method, Montgomery ladder and sliding-window method.

The experimental result in Section IV shows that a scalar multiplication of rational point in $\mathbb{G}_2$ point is accelerated by 10 to 20 times by applying the mapping technique given in Section III for both KSS16 and KSS18 curve. The result also shows that the *sextic twist* of KSS18 is faster than the *quartic twist* of the KSS16 curve (In CRYPTO'16, Kim and Barbulescu [4] proposed a new ECDLP attack which requires to update pairing-friendly curve parameters. Therefore, this paper uses the most recent parameters proposed by Barbulescu and Duquesne [1]).

II. BACKGROUND

The background studies required for the system model is briefly discussed in this section.

A. Elliptic Curve [5]

Let E be the elliptic curve defined over the prime field $\mathbb{F}_p$ as follows:

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

where $4a^3 + 27b^2 \neq 0$ and $a, b \in \mathbb{F}_p$. Points satisfying Eq. (1) including the *point at infinity* $\mathcal{O}$ are known as rational points on the curve, forms an additive Abelian group denoted by $E(\mathbb{F}_p)$. The total number of points on E is denoted as $\#E(\mathbb{F}_p)$. When the definition field is the k^{th} degree extension field $\mathbb{F}_{p^k}$, rational points on the curve E also forms an additive Abelian group denoted as $E\left(\mathbb{F}_{p^k}\right)$.

1) Point Addition

Let's 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 are obtained as follows:

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

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

Here λ is the tangent at the point on the curve and $\mathcal{O}$ is 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).

Let r be the *order* of the target rational point group and $s$be the scalar such that $0 \leq s < r$. Scalar multiplication of rational point M, denoted as $[s]M$ can be calculated by $(s-1)$-times additions of M as,

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

If $s = r$, where r is the order of the curve then $[r]M = \mathcal{O}$. When $[s]M = N$ and 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.

This paper has considered left-to-right binary scalar multiplication for evaluating the efficiency of the given mapping operation. From the view point of security, binary method is vulnerable to side channel attack [6]. Therefore, this paper has also experimented with Montgomery ladder [7] and sliding-window method [8] for scalar multiplication evaluation.

B. Kachisa-Schaefer-Scott (KSS) Curve

In [3], the authors proposed a family of non-super-singular Brezing-Weng pairing-friendly elliptic curves of embedding degree$k = \{16, 18, 32, 26, 40\}$, using elements in the cyclotomic field. Like other pairing-friendly curves, *characteristic* p, *Frobenius trace* t and *order* r of these curves are given systematically by an integer variable known as mother parameter. As mentioned earlier this paper considers KSS16 and KSS18 curve as follows:

KSS18	KSS16
$E/\mathbb{F}_{p^{18}}: Y^2 = X^3 + b,\ b \in \mathbb{F}_p$ and $b \neq 0$.	$E/\mathbb{F}_{p^{16}}: Y^2 = X^3 + aX,\ a \in \mathbb{F}_p$ and $a \neq 0$.

Here $X, Y \in \mathbb{F}_{p^{18}}$ in KSS18 and $X, Y \in \mathbb{F}_{p^{16}}$ in KSS16 curve respectively. The curves are parametrized by an integer variable u as follows:

KSS18	$p(u) = (u^8 + 5u^7 + 7u^6 + 37u^5 + 188u^4 + 259u^3 + 343u^2 + 1763u + 2401)\ /\ 21$
	$r(u) = (u^6 + 37u^3 + 343)\ /\ 343$
	$t(u) = (u^4 + 16u + 7)\ /\ 7$
KSS16	$p(u) = (u^{10} + 2u^9 + 5u^8 + 48u^6 + 152u^5 + 240u^4 + 625u^2 + 34 + 2398u + 3125)\ /\ 980$
	$r(u) = (u^8 + 48u^4 + 625)/61550$
	$t(u) = (2u^5 + 41u + 35)\ /\ 35$

Table 1. Vector representation of $Q = (x_Q, y_Q) \in \mathbb{F}_{p^{18}}$

	1	i	i^2	v	iv	i^2v	θ	$i\theta$	$i^2\theta$	$v\theta$	$iv\theta$	$i^2v\,\theta$	θ^2	$i\theta^2$	$i^2\,\theta^2$	$v\theta^2$	$iv\theta^2$	$i^2v\theta^2$
x_Q	0	0	0	0	0	0	0	0	0	0	0	0	a_{12}	a_{13}	a_{14}	0	0	0
y_Q	0	0	0	a_3	a_4	a_5	0	0	0	0	0	0	0	0	0	0	0	0

The necessary condition for u in KSS18 is $u \equiv 14 (\mathrm{mod}\, 42)$ and whereas for KSS16 curve it is $u \equiv 25 \text{ or } 45 (\mathrm{mod}\, 70)$.

C. Extension Field Arithmetic

In [9], the authors have explained optimal extension field towering by using irreducible binomials. Since this paper uses two curves of different extension degree, therefore, the towering process of $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{16}}$ are represented as follows:

KSS18 towering	KSS16 towering
$\mathbb{F}_{p^3} = \mathbb{F}_p[i]/(i^3 - c)$, $\mathbb{F}_{p^6} = \mathbb{F}_{p^3}[v]/(v^2 - i)$, $\mathbb{F}_{p^{18}} = \mathbb{F}_{p^6}[\theta]/(\theta^3 - v)$,	$\mathbb{F}_{p^2} = \mathbb{F}_p[\alpha]/(\alpha^2 - z)$, $\mathbb{F}_{p^4} = \mathbb{F}_{p^2}[\beta]/(\beta^2 - \alpha)$, $\mathbb{F}_{p^8} = \mathbb{F}_{p^4}[\gamma]/(\gamma^2 - \beta)$, $\mathbb{F}_{p^{16}} = \mathbb{F}_{p^8}[\omega]/(\omega^2 - \gamma)$.

Here the necessary condition of KSS18 towering is $3|(p-1)$, where p is the characteristics of KSS18 curve and c is the cubic non-residue. For KSS16 curve, $4|(p-1)$ and z is the quadratic non-residue. For both towering, $c = 2$ and $z = 2$ will be best choice for efficient calculation since multiplication by 2 can be done by 1 bit left shifting operation.

D. $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_3$ Groups

In the context of pairing-based cryptography, especially on KSS curves, two additive rational point groups $\mathbb{G}_1$, $\mathbb{G}_2$ and a multiplicative group $\mathbb{G}_3$ of order r are considered. From [10], $\mathbb{G}_1$,$\mathbb{G}_2$ and $\mathbb{G}_3$ are defined as follows:

$$\begin{aligned} \mathbb{G}_1 &= E(\mathbb{F}_p)[r] \cap \mathrm{Ker}(\pi_p - [1]), \\ \mathbb{G}_2 &= E(\mathbb{F}_{p^k})[r] \cap \mathrm{Ker}(\pi_p - [p]), \qquad (4a) \\ \mathbb{G}_3 &= \mathbb{F}^*_{p^k}/(\mathbb{F}^*_{p^k})^r, \end{aligned}$$

$$\xi : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3\,, \qquad (4b)$$

where π_p is the Frobenius mapping and ξ denotes Ate pairing. In the case of KSS curves, the above $\mathbb{G}_1$ is just $E(\mathbb{F}_p)$. In what follows, rest of this paper considers $P \in \mathbb{G}_1 \subset E(\mathbb{F}_p)$ and $Q \in \mathbb{G}_2$, where $\mathbb{G}_2$ is a subset of $E(\mathbb{F}_{p^{16}})$ and $E(\mathbb{F}_{p^{18}})$ for KSS16 and KSS18 curves respectively.

E. Twist on KSS Curves

There exists a twisted curve with a group of rational points of order r which are isomorphic to the group where rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^k})$ belongs to. This subfield isomorphic rational point group includes a twisted isomorphic point of Q, typically denoted as $Q' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^{k/d}})$, where k is the embedding degree and d is the twist degree. Since points on the twisted curve are defined over a smaller field than $\mathbb{F}_{p^k}$, therefore ECA and ECD becomes faster. However, when required in the pairing calculation, such as for line evaluation they can be quickly mapped to a point over $\mathbb{F}_{p^k}$. Defining such mapping and re-mapping techniques is the focus of this paper. Since the pairing-friendly KSS16 curve has CM discriminant of $D = 1$ and $4|k$, therefore quartic twist is available. For sextic twist, the curve should have $D = 3$ and $6|k$, which exists in KSS18.

III. SYSTEM MODEL AND METHODS

This section introduces the target mapping procedure of $\mathbb{G}_2$ rational point group to its twisted (quartic and sextic) isomorphic group $\mathbb{G}'_2$ for Ate-based pairing over the considered KSS curves.

A. Sextic Twisted Mapping of KSS18

Let E be the KSS18 curve in the base field $\mathbb{F}_{p^3}$ as follows:

$$E : y^2 = x^3 + b, \qquad (5)$$

where $b \in \mathbb{F}_p$; $x, y, \in \mathbb{F}_{p^3}$. In the context of KSS18 curve, let us consider a rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$. This Q has a special vector representation with 18 $\mathbb{F}_p$ coefficients for each x_Q and y_Q coordinate. Table 1 shows the structure of the coefficients of $Q \in \mathbb{F}_{p^{18}}$. Among the 18 coefficients, there are 3 continuous nonzero $\mathbb{F}_p$ coefficients. The other coefficients are zero. However, the set of these nonzero coefficients belongs to a $\mathbb{F}_{p^3}$ element.

Table 2. Vector representation of $Q = (x_Q, y_Q) \in \mathbb{F}_{p^{16}}$

	1	α	β	$\alpha\beta$	γ	$\alpha\gamma$	$\beta\gamma$	$\alpha\beta\gamma$	ω	$\alpha\omega$	$\beta\omega$	$\alpha\beta\omega$	$\gamma\omega$	$\alpha\gamma\omega$	$\beta\gamma\omega$	$\alpha\beta\gamma\omega$
x_Q	0	0	0	0	n_4	n_5	n_6	n_7	0	0	0	0	0	0	0	0
y_Q	0	0	0	0	0	0	0	0	0	0	0	0	n_{12}	n_{13}	n_{14}	n_{15}

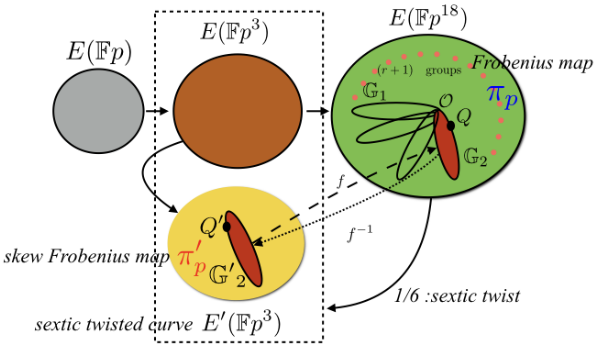


Fig. 1. Sextic twist of KSS18 curve.

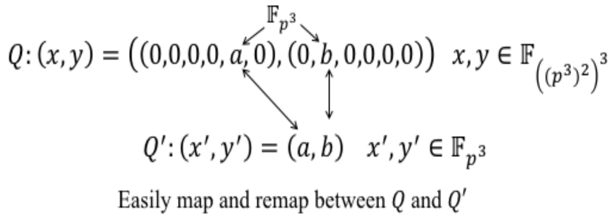

$\mathbb{F}_{p^3}$
$Q: (x, y) = ((0,0,0,0,a,0),(0,b,0,0,0,0))$ $x, y \in \mathbb{F}_{((p^3)^2)^3}$
$Q': (x', y') = (a, b)$ $x', y' \in \mathbb{F}_{p^3}$
Easily map and remap between Q and Q'

Fig. 2. Mapping and remapping of Q and Q'.

This paper considers parameter given in [1] for KSS18 curve. In such consideration, Q is given as $Q = (x'\theta^2, y'v)$, showed in Table 1, where $x' = (a_{12} + a_{13}i + a_{14}i^2)$, $y' = (a_3 + a_4 i + a_5 i^2) \in \mathbb{F}_{p^3}$, where v and θ are the basis elements of $\mathbb{F}_{p^6}$ and $\mathbb{F}_{p^{18}}$ respectively. Here x' and y' are the coordinates of Q' and $Q' = (x', y') \in \mathbb{G}'_2 \subset E'$ is the sextic twisted isomorphic subfield rational point of Q shown in Fig. 1.

Now from Eq. (5), let us find the twisted curve E' shown in Fig. 1 as follows:

$$\begin{aligned} (y'v)^2 &= (x'\theta^2)^3 + b, \\ {y'}^2\theta^6 &= {x'}^3\theta^6 + b, \\ {y'}^2 i &= {x'}^3 i + b, \end{aligned}$$

multiplying i^{-1} in both sides.

$$ {y'}^2 = {x'}^3 + b\, i^{-1}, \tag{6}$$

where $\theta^6 = v^2 = i$. The twisted curve of E' is obtained as $y^2 = x^3 + bi^{-1}$, where i is the basis element in $\mathbb{F}_{p^3}$ and i^{-1} is the quadratic and cubic non-residue over $\mathbb{F}_{p^3}$.

The mapping from $Q \in \mathbb{F}_{p^{18}}$ to $Q' \in \mathbb{F}_{p^3}$ can be easily achieved by selecting the 3 nonzero $\mathbb{F}_p$ coefficients of each coordinate of Q and placing them in $Q' = (x', y') \in \mathbb{F}_{p^3}$ respectively. No arithmetic operation is required for this mapping operation.

The reverse mapping, that is mapping from $Q' = (x', y') \in \mathbb{F}_{p^3}$ to $Q = (x'\theta^2, y'v) \in \mathbb{F}_{p^{18}}$ can also be obtained easily by just placing the x' and y' in the correct basis position in $Q = (x'\theta, y'v)$. It this case it also needs no extra arithmetic operation. Fig. 2 shows the scenario.

B. Quartic Twisted Mapping of KSS16

For quartic twisted mapping at first it is required to obtain certain rational point Q of subgroup order r in $E(\mathbb{F}_{p^{16}})$. Let us consider the rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{16}})$ and its quartic twisted rational point $Q' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^4})$. Rational point Q has a special vector representation given in Table 2. From Table 2, co-ordinate of $Q = (x_Q, y_Q) \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{16}})$is obtained as $Q = (x_Q, y_Q) = (\gamma x_{Q'}, \omega\gamma y_{Q'})$ where $x_{Q'}$, $y_{Q'}$ are the co-ordinates of the rational point Q' in the twisted curve. Now let's find the twisted curve of KSS16 in $\mathbb{F}_{p^4}$ as follows:

$$\begin{aligned} (\omega\gamma y_{Q'})^2 &= (\gamma x_{Q'})^3 + a(\gamma x_{Q'}), \\ \gamma\beta y_{Q'}^2 &= \gamma\beta\, x_{Q'}^3 + a\gamma x_{Q'}, \\ y_{Q'}^2 &= x_{Q'}^3 + a\beta^{-1} x_{Q'}, \end{aligned} \tag{7}$$

multiplying $(\gamma\beta)^{-1}$ both sides.

The twisted curve of E' is obtained as $y^2 = x^3 + a\beta^{-1}x$ where β is the basis element in $\mathbb{F}_{p^4}$. There is a tricky part that needs attention when calculating the ECD in $E'(\mathbb{F}_{p^4})$ presented in the following equation.

$$\lambda = (3x_{Q'}^2 + \boldsymbol{a})(2\, y_{Q'})^{-1}, \tag{8}$$

where $\boldsymbol{a} \in \mathbb{F}_{p^4}$, since $\boldsymbol{a} = a\beta^{-1}$ and $\beta \in \mathbb{F}_{p^4}$. The calculation of $\boldsymbol{a} = a\beta^{-1}$ is given as follows:

$$\begin{aligned} a\beta^{-1} &= (a + 0\alpha + 0\beta + 0\alpha\beta)\beta^{-1}, \\ &= z^{-1}a\alpha\beta, \end{aligned} \tag{9}$$

where $\alpha^2 = z$. Now let's denote the quartic mapping as follows:

$$Q = (x_Q, y_Q) = (\gamma x_{Q'}, \omega\gamma y_{Q'}\ ) \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{16}})$$

$$\mapsto \quad Q' = (x_{Q'}, y_{Q'}) \in \mathbb{G}_{2'} \subset E'(\mathbb{F}_{p^4}).$$

It means for quartic twisted mapping it requires no calculation except selecting the coefficient and placing them in correct basis position same as KSS18 curve.

IV. RESULT ANALYSIS

The focus of this paper is to derive twisted mapping and obtain experimental results to show the effectiveness of the isomorphic mapping over KSS16 and KSS18 curves. To determine the effectiveness, this paper has implemented 3 well-known elliptic curve scalar multiplication methods named as the binary (BIN) method, Montgomery ladder (ML) method, and sliding-window (SW) method using the derived mapping and without mapping.

For the experiment first the authors have applied the mapping technique shown in Section III to map rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^k})$ to its isomorphic twisted point $Q' \in \mathbb{G}_2' \subset E'(\mathbb{F}_{p^{k/d}})$ in both KSS curves. After that the scalar multiplication of Q' is calculated. Then the resulted points are re-mapped to $\mathbb{G}_2 \subset E(\mathbb{F}_{p^k})$. Let's define this strategy as *with mapping*. On the other hand, scalar multiplication of Q without mapping is also calculated which is denoted as *w/o mapping*.

In the experiment, the authors have considered most recent parameters of their knowledge till date given by Barbulescu and Duquesne [1]. These parameters are said to be secure enough against the recent development of ECDLP attack by Kim and Barbulescu [4].

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	OS X 10.12.3	iOS 10.2.1
Compiler	gcc 4.2.1	gcc 4.2.1
Programming language	C	Objective-C, C
Library [11]	GNU MP 6.1.1	GNU MP 6.1.1

Table 4. Parameters used in the experiment

	KSS18	KSS16
Mother parameter	$u = 2^{44} + 2^{22} - 2^9 + 2$	$u = -2^{34} + 2^{27} - 2^{23} + 2^{20} - 2^{11} + 1$
Obtained curve	$y^2 = x^3 + 3$	$y^2 = x^3 + x$
Order r size	256-bit	263-bit

Table 3 shows the experiment environment. Table 4 shows the parameters used in the experiment. The comparative results are shown in Figs. 3 and 4. In the experiment 100 random scalars $0 < s \leq r$ is generated and the average is execution time is obtained in millisecond. Analyzing Figs. 3 and 4, we can find that scalar multiplication on the sextic twisted KSS18 curve using the given mapping is more than 20 times faster than without the mapping. In the case of quartic twisted KSS16 curve, scalar multiplication becomes at most 10 times faster after applying the given mapping than no mapping. Another important difference is, sextic twisted mapped rational points take less time in both environments since it has one less coefficient than quartic twisted KSS16 curve points and the random numbers size for in KSS18 curve is smaller than KSS16 case.

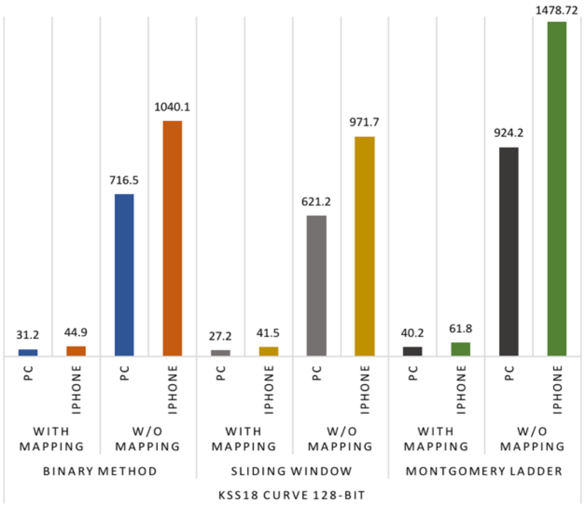


Fig. 3. Comparative result of BIN, SW and ML scalar multiplication methods with and w/o mapping in KSS18 curve.

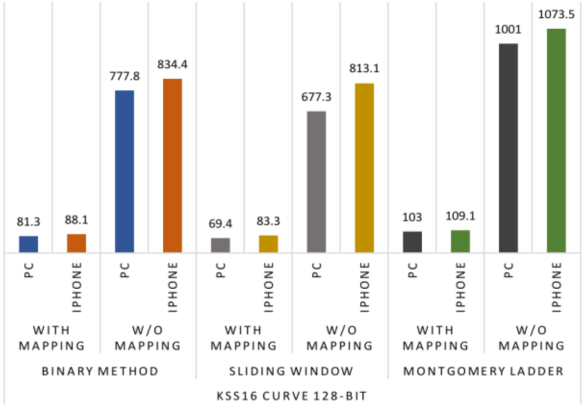


Fig. 4. Comparative result of BIN, SW and ML scalar multiplication methods with and w/o mapping in KSS16 curve.

In the experiment, execution environments, such as PC and iPhone, have different CPU clock frequencies. In both environments, single processor core is utilized. The ratio of CPU frequencies of iPhone and PC is about $1.84 / 2.7 \approx 0.68$. In KSS18 curve, the execution time [PC: iPhone] ratio without mapping for is around 0.62 to 0.66, which is close to CPU frequency ratio. On the other hand, with mapping case for KSS18 curve, the ratio is also around 0.6. For KSS16 curve, the ratio with no mapping case is more than 0.8 and for mapping case it is around 0.7 to 0.9. Since PC and iPhone has different processor architectures therefore it's frequency ratio has modest relation with the execution time ratio. The ratio may also be effected by the other processes, running in certain environment during the experiment time.

V. DISCUSSION AND CONCLUSION

This paper explicitly shows the isomorphic mapping procedure of $\mathbb{G}_2$ rational point group to its sextic and quartic twisted sub-field isomorphic rational point group $\mathbb{G}_2'$ and its reverse mapping for KSS18 and KSS16 curves in the context of Ate-based pairing. The authors have evaluated the effectiveness of such mapping by implementing 3 different scalar multiplication methods on twisted rational points in $\mathbb{G}_2'$. The result of scalar multiplication in $\mathbb{G}_2'$ accelerates the scalar multiplication in $\mathbb{G}_2$ by 10 to 20 times than scalar multiplication of $\mathbb{G}_2$ rational point directly in $E(\mathbb{F}_{p^{16}})$ and $E(\mathbb{F}_{p^{18}})$. The authors would like to make pairing based protocol and apply this technique as a future work.

ACKNOWLEDGMENTS

This work was partially supported by the Strategic Information and Communications R&D Promotion Programme (SCOPE) of Ministry of Internal Affairs and Communications, Japan and the Energy Technology Development Program of the Korea Institute of Energy Technology Evaluation and Planning (KETEP), granted financial resource from the Ministry of Trade, Industry & Energy, Republic of Korea (No. 20152000000170).

REFERENCES

[1] R. Barbulescu and S. Duquesne, "Updating key size estimations for pairings," Cryptology ePrint Archive, 2017 [Internet], Available: http://ia.cr/2017/334.

[2] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren, *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Boca Raton, FL: CRC Press, 2005.

[3] E. Kachisa, E. Schaefer, and M. Scott, "Constructing Brezing-Weng pairing-friendly elliptic curves using elements in the cyclotomic field," in *Pairing-Based Cryptography-Pairing 2008, Lecture Notes in Computer Science*, vol. 5209, pp. 126–135, 2008.

[4] T. Kim and R. Barbulescu, "Extended tower number field sieve: a new complexity for the medium prime case," in *Advances in Cryptology–CRYPTO 2016*, *Lecture Notes in Computer Science*, vol. 9814, pp. 543–571, 2016.

[5] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography*. Boca Raton, FL: CRC press, 2008.

[6] P. C. Kocher, "Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems," in *Advances in Cryptology–CRYPTO'96, Lecture Notes in Computer Science*, vol. 1109, pp. 104–113, 1996.

[7] P. L. Montgomery, "Speeding the pollard and elliptic curve methods of factorization," *Journal of Mathematics of Computation*, vol. 48, no. 177, pp. 243–264, 1987.

[8] C. K. Koc, "High-radix and bit recoding techniques for modular exponentiation," *International Journal of Computer Mathematics*, vol. 40, no. 3-4, pp. 139–156, 1991.

[9] D. V. Bailey and C. Paar, "Efficient arithmetic in finite field extensions with application in elliptic curve cryptography," *Journal of Cryptology*, vol. 14, no. 3, pp. 153–176, 2001.

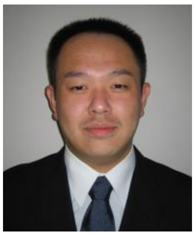
[10] Y. Mori, S. Akagi, Y. Nogami, and M. Shirase, "Pseudo 8–sparse multiplication for efficient ate– based pairing on Barreto–Naehrig curve," in *Pairing-Based Cryptography-Pairing 2013*, *Lecture Notes in Computer Science*, vol. 8365, pp. 186–198, 2013.

[11] The GNU Multiple Precision Arithmetic Library 6.1.1 edition, 2016 [Internet], Available: http://gmplib.or.

Md. Al-Amin Khandaker
graduated from Jahangirnagar University in 2011. He is now pursuing his Ph.D. in the field of finite field theory and cryptography in Okayama University under the supervision of Professor Dr. Nogami. His research interest includes efficient implementation of pairing based cryptography and IoT security. He is a student member of IEEE.

http://doi.org/10.6109/jicce.2017.15.2.97

Taehwan Park
received his B.S.E.E. from Pusan National University, Busan, Korea, in 2013. He is currently pursuing the combined M.S. and Ph.D. course in Computer Engineering at Pusan National University. His research interests include IoT device security, information security, elliptic curve cryptography, and post quantum cryptography.



Yasuyuki Nogami
graduated from Shinshu University in 1994 and received the Ph.D. degree in 1999 from Shinshu University. He is now a 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.

Howon Kim
received his B.S.E.E. from Kyungpook National University, Daegu, Korea, in 1993, and his M.S. and Ph.D. in Electronic and Electrical Engineering from Pohang University of Science and Technology (POSTECH), Pohang, Korea, in 1995 and 1999, respectively. From July 2003 to June 2004, he studied with the COSY group at the Ruhr-University of Bochum, Germany. He was a senior member of the technical staff at the Electronics and Telecommunications Research Institute (ETRI), Daejeon, Republic of Korea. He is currently working as a professor with the Department of Computer Engineering, School of Computer Science and Engineering, Pusan National University, Busan, Korea. His research interests include RFID technology, sensor networks, information security, and computer architecture. Currently, his main research focus is on the Internet of Things (IoT) technology and the related security issues, mobile RFID technology, and sensor networks, public key cryptosystems, post quantum cryptography, and their security issues. He is a member of the IEEE and the International Association for Cryptologic Research (IACR).