Doctoral Thesis

Proposals on Efficient Software Implementation of Pairing-Based Cryptographic Primitives

Author:
Md. Al-Amin Khandaker

Supervisor:
Dr. Yasuyuki Nogami

A thesis submitted in fulfillment of the requirements for the degree of Doctor of Philosophy

in the

Information Security Lab.
Graduate School of Natural Science and Technology

Okayama University

October 24, 2018

Declaration of Authorship

This dissertation and the work presented here for doctoral studies were conducted under the supervision of Professor Yasuyuki Nogami. I, Md. Al-Amin Khandaker, declare that this thesis titled, "Proposals on Efficient Software Implementation of Pairing-Based Cryptographic Primitives" and the work presented in it are my own. I confirm that:

- The work presented in this thesis is the result of original research carried out by myself, in collaboration with others, while enrolled in the Faculty of Engineering of Okayama University as a candidate for the degree of Doctor of Philosophy.
- This work has not been submitted for a degree or any other qualification at this University or any other institution.
- Some of the work presented in this thesis was previously published is listed in "Research Activity" .
- The published work of others cited in this thesis is clearly attributed.
- I have acknowledged all main sources of help to pursue this work.
- In all works all my coauthors contributed equally.
- The experiments and results presented in this thesis and in the articles where I am the first author were conducted by myself.

Signed: _____

Date: _____

"*If we knew what it was we were doing, it would not be called research, would it? "*

Albert Einstein

OKAYAMA UNIVERSITY

Abstract

Faculty of Engineering
Graduate School of Natural Science and Technology

Doctor of Philosophy

Proposals on Efficient Software Implementation of Pairing-Based Cryptographic Primitives

by Md. Al-Amin KHANDAKER

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...

Acknowledgements

This work would not be possible without the unceasing supervison, innumerable counseling and unrelenting persuasion of my Ph.D. advisor Professor Yasuyuki Nogami. I am indebted to *Nogami Sensei* for having me in his lab *(Information Security Lab.)* as a doctoral student and mentoring me on this work. He taught me how to analyze complex problems from different perspectives and express the ideas from pen and papers to a fully publishable article. I enjoyed his insightful comments on the research topics during our discussions. Sometimes his in depth queries bewildered me and influenced my ideas in this thesis. He guided me in different ways to approach a problem and the need to be persistent to accomplish my goal. He made my stay in the lab an more than a workplace.

He also made the MORIKAWA Lab a wonderful workplace and home for the past five years. Furthermore, Prof. Morikawa's role in developing my writing and presentation skills was paramount. Although he was very much strict with me on the research, he is very kind to me in the life.

I am grateful to a large number of people who have directly and indirectly helped me finish this work. First of all, I would like to express my deep gratitude to Professor Yoshitaka Morikawa, my supervisor, who has granted me the chance to start this research, and has given me innumerable advices and unrelenting encouragement. I am also grateful to Associate Professor Yasuyuki Nogami for his continuous support, many insightful comments, and helpful discussions, which inspired many of the ideas in this thesis. He was always there to give advice and helpful comment, to proofread and mark up my papers. I would also like to thank Associate Professor Toru Nakanishi, the members of my thesis committee, for taking time to read my thesis and for their insightful comments and helpful advice. He provided me the basic idea of the research work and guided me through the thesis process. His strong work ethic and passion for science were not only inspiring, but also contagious. He really helped me a lot. I am very grateful to associate professor Nobumoto Yamane who advised some important comments at progress meeting.

I am also grateful to all present and past members of Morikawa Laboratory, Okayama University.

Finally, I would like to dedicate this thesis to my parents Ms. Keiko Sakemi and Mr. Junichi Sakemi, in appreciation of their generous support and continuous encouragement.

The work described in this thesis would not have been possible without the strong scientific, educational, and financial support of professor Yoshitaka Morikawa, associate professor Nobumoto Yamane and assistant professor Yasuyuki Nogami. They are very much responsible for helping me complete the doctoral program. I am especially fortunate that they afforded me a lot of opportunities to attend international conferences.

First, I am greatly indebted to my advisor, Professor Yasuyuki Nogami, for his continuous support, many insightful comments, and helpful discussions, which inspired many of the ideas in this thesis. He was always there to listen and to give advice, to proofread and mark up my papers, and to ask me good questions to help me think through my problems. He taught me how to consider problems and express my ideas. He showed me different ways to approach a research problem and the need to be persistent to accomplish any goal. He also made the MORIKAWA Lab a wonderful workplace and home for the past five years. Furthermore, Prof. Morikawa's role in developing my writing and presentation skills was paramount. Although he was very much strict with me on the research, he is very kind to me in the life.

I would like to thank assistant professor Yasuyuki Nogami for his useful advice and helpful discussion. He spent much time to teach me the finite field, which made it possible for me to do the research on cryptography. He provided me the basic idea of the research work and guided me through the thesis process. His strong work ethic and passion for science were not only inspiring, but also contagious. He really helped me a lot. Without their encouragement and constant guidance, I could not graduate from Okayama University in three years. Thanks a million, Professor Morikawa and assistant professor Nogami.

I am very grateful to associate professor Nobumoto Yamane who advised some important comments at progress meeting

I would also like to thank the members of my thesis committee- Professors Nobuo Funabiki and Toru Nakanishi for taking time to read my thesis and for their insightful comments and helpful advice.

Thanks also to my all friends!

Contents

List of Figures

List of Tables

List of Abbreviations

LAH	**L**ist **A**bbreviations **H**ere
WSF	**W**hat (it) **S**tands **F**or

List of Notations and Symbols

Notation	Description
p	$p > 3$ is an odd prime integer in this thesis.
$x \bmod p$	Modulo operation. the least nonnegative residue of x modulo p.
$\mathbb{F}_p$	Prime field. The field of integers mod p.
$\mathbb{F}_p^*$	The multiplicative group of the field $\mathbb{F}_p$. In other words, $\mathbb{F}_p^* = \{x \mid x \in \mathbb{F}_p \text{ and } x \neq 0\}$.
$\lfloor \cdot \rfloor$	The floor of $\cdot$ is the greatest integer less than or equal to $\cdot$. For example, $\lfloor 1 \rfloor = 1$ and $\lfloor 6.3 \rfloor = 6$.

Dedicated to two ladies I owe most. My mother who brought me to this world. And my wife Shama who sacrificed most during this Ph.D. journey

Research Activities

- Journal Papers (Peer-Reviewed)

1. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "An Improvement of Scalar Multiplication by Skew Frobenius Map with Multi-Scalar Multiplication for KSS Curve." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E100.A, no. 9, Sep. 2017, pp. 1838-1845, 2017. https://doi.org/10.1587/transfun.E100.A.1838
2. **Md. Al-Amin Khandaker**, Taehwan Park, Yasuyuki Nogami, and Howon Kim. "A Comparative Study of Twist Property in KSS Curves of Embedding Degree 16 and 18 from the Implementation Perspective." KIICE Journal of Information and Communication Convergence Engineering, vol. 15, no. 2, Jun. 2017, pp. 93-103, 2017. https://doi.org/10.6109/jicce.2017.15.2.97
3. Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka, and Yasuyuki Nogami, "Efficient Pairing-Based Cryptography on Raspberry Pi." Journal of Communications, vol. 13, no. 2, pp. 88-93, 2018. https://doi.org/10.12720/jcm.13.2.88-93
4. Yuta Hashimoto, **Md. Al-Amin Khandaker**, Yuta Kodera, Taehwan Park, Takuya Kusaka, Howon Kim, Yasuyuki Nogami, "An Implementation of ECC with Twisted Montgomery Curve over 32nd Degree Tower Field on Arduino Uno." International Journal of Networking and Computing (IJNC), vol. 8, no. 2, pp. 341-350, 2018. https://doi.org/10.15803/ijnc.8.2_341
5. Yuta kodera, Takeru miyazaki, **Md. Al-Amin Khandaker**, Md. Arshad ali, Takuya kusaka, Yasuyuki nogami and Satoshi uehara. "Distribution of Digit Patterns in Multi-Value Sequence over the Odd Characteristic Field." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E101.A, no. 9, Sep. 2018, pp. 1525-1536, 2018. https://doi.org/10.1587/transfun.E101.A.1525
6. Shunsuke Ueda, Ken Ikuta, Takuya Kusaka, **Md. Al-Amin Khandaker**, Ali Md. Arshad, Yasuyuki Nogami. "An Extended Generalized Minimum Distance Decoding for Binary Linear Codes on a 4-Level Quantization over an AWGN Channel." IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, vol. E101.A, no. 8, Aug. 2018, pp. 1235-1244, 2018. https://doi.org/10.1587/transfun.E101.A.1235
7. Shoma Kajitani, Yasuyuki Nogami, Shunsuke Miyoshi, Thomas Austin, **Md. Al-Amin Khandaker**, Nasima Begum, Sylvain Duquesne, "Web-based Volunteer Computing for Solving the Elliptic Curve Discrete Logarithm Problem." International Journal of Networking and Computing (IJNC), vol. 6, no. 2, pp. 181-194, 2016. https://doi.org/10.15803/ijnc.6.2_181

- International conferences (Peer-Reviewed)

1. **Md. Al-Amin Khandaker**, Yuki Nanjo, Takuya Kusaka, and Yasuyuki Nogami. "A Comparative Implementation of GLV Technique on KSS-16 Curve." Sixth International Symposium on Computing and Networking (CANDAR), 2018. IEEE. (Acceptance Ratio 28/77 ≈ 36%)
2. **Md. Al-Amin Khandaker**, Yuki Nanjo, Loubna Ghammam, Sylvain Duquesne, Yasuyuki Nogami, and Yuta Kodera. "Efficient optimal ate pairing at 128-bit security level." In: Patra A., Smart N. (eds) Progress in Cryptology (INDOCRYPT), 2017. Lecture Notes in Computer Science, vol 10698. Springer, Cham. https://doi.org/10.1007/978-3-319-71667-1_10.
3. **Md. Al-Amin Khandaker**, Hirotaka Ono, Yasuyuki Nogami, Masaaki Shirase, and Sylvain Duquesne. "An Improvement of Optimal Ate Pairing on KSS Curve with Pseudo 12-Sparse Multiplication." In: Hong S., Park J. (eds) Information Security and Cryptology (ICISC), 2016. Lecture Notes in Computer Science, vol 10157. Springer, Cham. https://doi.org/10.1007/978-3-319-53177-9_11.
4. **Md. Al-Amin Khandaker**, Yasuyuki Nogami, Hwajeong Seo, and Sylvain Duquesne. "Efficient Scalar Multiplication for Ate Based Pairing over KSS Curve of Embedding Degree 18." In: Choi D., Guilley S. (eds) Information Security Applications (WISA), 2016. Lecture Notes in Computer Science, vol 10144. Springer, Cham. https://doi.org/10.1007/978-3-319-56549-1_19.
5. **Md. Al-Amin Khandaker**, and Yasuyuki Nogami. "Isomorphic Mapping for Ate-Based Pairing over KSS Curve of Embedding Degree 18." Fourth International Symposium on Computing and Networking (CANDAR), 2016. IEEE. https://doi.org/10.1109/CANDAR.2016.0113.
6. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "An improvement of scalar multiplication on elliptic curve defined over extension field Fq2." IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2016. IEEE. https://doi.org/10.1109/ICCE-TW.2016.7520894.
7. **Md. Al-Amin Khandaker**, and Yasuyuki Nogami. "Frobenius Map and Skew Frobenius Map for Ate-based Pairing over KSS Curve of Embedding Degree 16 ." 32nd International Technical Conference on Circuits / Systems, Computers and Communications (ITC-CSCC), 2017. IEIE.
8. Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka, and Yasuyuki Nogami. "Consideration of Efficient Pairing Applying Two Construction Methods of Extension Fields." Sixth International Symposium on Computing and Networking (CANDAR), 2018. IEEE.
9. Yuki Nanjo, **Md. Al-Amin Khandaker**, Masaaki Shirase, Takuya Kusaka and Yasuyuki Nogami. "Efficient Ate-Based Pairing over the Attractive Classes of BN Curves." Information Security Applications (WISA), 2018. To appear Lecture Notes in Computer Science. Springer, Cham. (Acceptance Ratio 22/44 = 50%)
10. Yuta Hashimoto, **Md. Al-Amin Khandaker**, Yuta Kodera, Taehwan Park, Takuya Kusaka, Howon Kim and Yasuyuki Nogami. "An ECC Implementation with a Twisted Montgomery Curve over Fq32 on an 8-Bit Microcontroller." Fifth International Symposium on Computing and Networking (CANDAR), 2017. IEEE. https://doi.org/10.1109/CANDAR.2017.90.

11. Taehwan Park, Hwajeong Seo, **Md. Al-Amin Khandaker**, Yasuvuki Nogami, Howon Kim. "Efficient Parallel Simeck Encryption with GPGPU and OpenCL." IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2018. IEEE. https://doi.org/10.1109/ICCE-China.2018.8448768.
12. Yuta Kodera, Takeru Miyazaki, **Md. Al-Amin Khandaker**, Ali Md Arshad, Yasuyuki Nogami, and Satoshi Uehara. "Distribution of bit patterns on multi-value sequence over odd characteristics field." IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2017. IEEE. https://doi.org/10.1109/ICCE-China.2017.7991033
13. Ken Ikuta, Takuya Kusaka, **Md. Al-Amin Khandaker**, Yasuyuki Nogami, and Thomas H. Austin. " Estimation of computational complexity of Pollard's rho method based attack for solving ECDLP over Barreto-Naehrig curves." 32nd International Technical Conference on Circuits / Systems, Computers and Communications (ITC-CSCC), 2017. IEIE.
14. Ken Ikuta, Sho Joichi, Kazuya Kobayashi, **Md. Al-Amin Khandaker**, Takuya Kusaka and Yasuyuki Nogami. "A Study on the Parameter Size of the Montgomery Trick for ECDLP." International Symposium on Information Theory and its Applications (ISITA), 2018. IEICE. (To appear in IEEE Xplore).
15. Ken Ikuta, Sho Joichi, Kazuya Kobayashi, **Md. Al-Amin Khandaker**, Takuya Kusaka and Yasuyuki Nogami. "A Study on the Parameter of the Distinguished Point Method in Pollard's Rho Method for ECDLP." International Symposium on Information Theory and its Applications (ISITA), 2018. IEICE. (To appear in IEEE Xplore).
16. Takuya Kusaka, Sho Joichi, Ken Ikuta, **Md. Al-Amin Khandaker**, Yasuyuki Nogami, Satoshi Uehara, Nariyoshi Yamai and Sylvain Duquesne. "Solving 114-Bit ECDLP for a Barreto-Naehrig Curve." In: Kim H., Kim DC. (eds) Information Security and Cryptology (ICISC), 2017. Lecture Notes in Computer Science, vol 10779. Springer, Cham. https://doi.org/10.1007/978-3-319-78556-1_13.
17. Taehwan Park, Hwajeong Seo, Garam Lee, **Md. Al-Amin Khandaker**, Yasuyuki Nogami, Howon Kim. "Parallel Implementations of SIMON and SPECK, Revisited." In: Kang B., Kim T. (eds) Information Security Applications (WISA), 2017. Lecture Notes in Computer Science, vol 10763. Springer, Cham. https://doi.org/10.1007/978-3-319-93563-8_24. (Acceptance Ratio $27/53 \approx 50\%$)
18. Yuta Kodera, Takuya Kusaka, Takeru Miyazaki, **Md. Al-Amin Khandaker**, Yasuyuki Nogami and Satoshi Uehara. "An Efficient Implementation of Trace Calculation over Finite Field for a Pseudorandom Sequence." Fifth International Symposium on Computing and Networking (CANDAR), 2017. IEEE. https://doi.org/10.1109/CANDAR.2017.86.
19. Akihiro Sanada, Yasuyuki Nogami, Kengo Iokibe, **Md. Al-Amin Khandaker**. "Security analysis of Raspberry Pi against Side-channel attack with RSA cryptography." IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2017. IEEE. https://doi.org/10.1109/ICCE-China.2017.7991108

- Domestic conferences

1. **Md. Al-Amin Khandaker**, Hirotaka Ono, Yuki Nanjo, Takuya Kusaka and Yasuyuki Nogami. "Efficient Optimal-Ate Pairing on BLS-12 Curve Using Pseudo 8-Sparse Multiplication." Computer Security Symposium (CSS), 2017, CD-ROM (3E1-4).
2. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "Efficient Scalar Multiplication by Skew Frobenius Map with Multi-Scalar Multiplication for KSS Curve." Symposium on Cryptography and Information Security (SCIS), 2017, CD-ROM (B1-3).
3. Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka, Yasuyuki Nogami. "A Study on a Construction Method of Degree 18 Extension Field for Efficient Pairing over KSS Curves." Computer Security Symposium (CSS), 2018, CD-ROM (??).
4. Hirotaka Ono, **Md. Al-Amin Khandaker**, Yuki Nanjo, Toshifumi Matsumoto, Takuya Kusaka and Yasuyuki Nogami. "An Implementation and Evaluation of ID-based Authentication on Raspberry Pi with Pairing Library." Symposium on Cryptography and Information Security (SCIS), 2018, CD-ROM (4D2-1).
5. Yuki Nanjo, **Md. Al-Amin Khandaker**, Yuta Kodera and Yasuyuki Nogami. "Implementation method of the pairing over BN curve using two type of extension fields." Symposium on Cryptography and Information Security (SCIS), 2018, CD-ROM (4D2-3).
6. Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka, and Yasuyuki Nogami. "The relation between the efficient sextic twist and constant of the modular polynomial for BN curve." Computer Security Symposium (CSS), 2017, CD-ROM (3E1-3).
7. Norito Jitsui, Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka and Yasuyuki Nogami. " Efficient Elliptic Scalar Multiplication for Pairing-Based Cryptography over BLS48." Symposium on Cryptography and Information Security (SCIS), 2018, CD-ROM (3B4-1).

Chapter 1

ICCE-TW 2016

In elliptic curve cryptography (ECC), a scalar multiplication for rational point is the most time consuming operation. This paper proposes an efficient calculation for a scalar multiplication by applying Frobenious Mapping. Particularly, this paper deals with Barreto-Naehrig curve defined over extension field $\mathbb{F}_{q^2}$, where $q = p^6$ and p is a large prime.

1.1 Introduction

In cryptography research, elliptic curve cryptography (ECC) has gained a wide acceptance due to its smaller key size and greater security. In ECC, scalar multiplication (SM) is carried out at the encryption and decryption phases. SM is the major operation in ECC. Let us denote a scalar and rational point by s and P, respectively. Then, the SM is denoted by $[s]P$. In real cases s is significantly large number less than the order of rational point group. Since SM needs a complicated calculation over the definition field such as prime field, an efficient algorithm for SM is needed. Recently, ECC defined over extension field $\mathbb{F}_{q^2}$ with a large prime number p such as more than 2000 bits is used in some ECC based protocols. On the other hand, pairing based cryptography realizes some innovative application protocol. Pairing based cryptography requires pairing friendly curve which is difficult to generate. Barreto-Naehrig (BN) [4] curve is one of the well known pairing friendly curve[**BN_def**] whose parameters are able to be systematically given. BN curve is mostly used due to its efficiency to realize pairing based cryptography. Thus, this paper proposes an efficient approach for calculating SM on BN curve particularly defined over extension field $\mathbb{F}_{q^2}$, where $q = p^6$ and p is a prime number by using Frobenious Mapping (FM) for the rational points.

1.2 Preliminaries

This section briefly discusses the fundamental arithmetic operations required for elliptic curve cryptography defined over prime field $\mathbb{F}_p$ and its extension field $\mathbb{F}_{q^2}$. In addition, this paper focuses on BN curve defined over $\mathbb{F}_{q^2}$, $q = p^6$.

1.2.1 BN curve over prime field $\mathbb{F}_p$

BN curve is a non super-singular (*ordinary*) pairing friendly elliptic curve of embedding degree 12[**BN_def**]. The equation of BN curve defined over $\mathbb{F}_p$ is given by

$$E : y^2 = x^3 + b, \quad (b \in \mathbb{F}_p). \tag{1.1}$$

where $b \neq 0$. Its characteristic p, Frobenius trace t and order r are given by using an integer variable χ as follows:

$$p(\chi) = 36\chi^4 - 36\chi^3 + 24\chi^2 - 6\chi + 1, \tag{1.2}$$
$$r(\chi) = 36\chi^4 - 36\chi^3 + 18\chi^2 - 6\chi + 1, \tag{1.3}$$
$$t(\chi) = 6\chi^2 + 1. \tag{1.4}$$

From Eq.(1.3) and Eq.(1.4) we find that the bit size of r is two times larger than t. Thus, these parameters generally satisfy $t \ll p \approx r$ and the following relation.

$$r = p + 1 - t. \tag{1.5}$$

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 $\mathcal{O}$. Let us consider two rational points $P = (x_P, y_P)$, $Q = (x_Q, y_Q)$, and their addition $R = P + Q$, where $R = (x_R, y_R)$ and $P, Q, R \in E(\mathbb{F}_p)$. Then, the x and y coordinates of R is calculated as follows.

$$\lambda = \begin{cases} \frac{y_Q - y_P}{x_Q - x_P} & (P \neq Q \text{ and } x_Q \neq x_P), \\ \frac{3x_P^2}{2y_P} & (P = Q \text{ and } y_P \neq 0), \\ \phi & \text{otherwise.} \end{cases} \tag{1.6a}$$

$$(x_R, y_R) = ((\lambda^2 - x_P - x_Q), \\ (x_P - x_R)\lambda - y_P), \text{ if } \lambda \neq 0. \tag{1.6b}$$
$$(x_R, y_R) = \mathcal{O} \quad \text{if } \lambda = 0. \tag{1.6c}$$

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

1.2.2 Elliptic curve over extension field $\mathbb{F}_{q^2}$

At first, let us consider arithmetic operations in $\mathbb{F}_{q^2}$, which is the degree 2 extension field over $\mathbb{F}_q$. In other words extension field $\mathbb{F}_{q^2}$ is the two dimensional vector space over $\mathbb{F}_q$. Let $\{v_0, v_1\}$ be a basis of $\mathbb{F}_{q^2}$, an arbitrary element $\mathbf{x} \in \mathbb{F}_{q^2}$ is represented as

$$\mathbf{x} = x_0 v_0 + x_1 v_1, \quad \text{where } x_i \in \mathbb{F}_q. \tag{1.7}$$

When we implicitly know the basis vectors v_0 and v_1, Eq.(1.7) is simply expressed as

$$\mathbf{x} = (x_0, x_1). \tag{1.8}$$

Addition and subtraction in $\mathbb{F}_{q^2}$

For vectors, addition, subtraction, and multiplication by a scalar in $\mathbb{F}_q$ are carried out by coefficient wise operations over $\mathbb{F}_q$. Let us consider two vectors $\mathbf{x} = (x_0, x_1)$ and

$\mathbf{y} = (y_0, y_1)$. Then,

$$\mathbf{x} \pm \mathbf{y} = (x_0 \pm y_0, x_1 \pm y_1), \tag{1.9}$$
$$k\mathbf{x} = (kx_0, kx_1),\ k \in \mathbb{F}_q. \tag{1.10}$$

Vector multiplication in $\mathbb{F}_{q^2}$

For a vector multiplication, we simply consider a polynomial basis representation. Let $f(x)$ be an irreducible polynomial of degree 2 over $\mathbb{F}_q$. Particularly, an irreducible binomial is efficient for calculations. In order to obtain an irreducible binomial, Legendre Symbol $\left(c/q\right)$ is useful. Consider a non-zero element $c \in \mathbb{F}_q$. If c does not have square roots, $f(x) = x^2 - c$ becomes an irreducible binomial over $\mathbb{F}_q$. In order to judge it, Legendre symbol is generally applied. Then, let its zero be ω, $\omega \in \mathbb{F}_{q^2}$, the set $\{1, \omega\}$ forms a polynomial basis in $\mathbb{F}_{q^2}$. Using this polynomial basis, the multiplication of two arbitrary vectors is performed as follows:

$$\begin{aligned}\mathbf{xy} &= (x_0 + x_1\omega)(y_0 + y_1\omega)\\ &= x_0y_0 + (x_0y_1 + x_1y_0)\omega + x_1y_1\omega^2\\ &= (x_0y_0 + cx_1y_1) + (x_0y_1 + x_1y_0)\omega. \end{aligned}\tag{1.11}$$

In this calculation, we have substituted $\omega^2 - c = 0$, since ω is a zero of the irreducible binomial $f(x) = x^2 - c$.

Vector inversion in $\mathbb{F}_{q^2}$

For calculating the multiplicative inverse vector of a non-zero vector $\mathbf{x} \in \mathbb{F}_{q^2}$, first we calculate the conjugate of $\mathbf{x}$ that is given by Frobenius mapping (FM) $\pi_q(\mathbf{x}) = \mathbf{x}^q$. In detail, $\pi_q(\mathbf{x}) = \mathbf{x}^q$ is the conjugate of $\mathbf{x}$ to each other. Then the inverse $\mathbf{x}^{-1}$ of $\mathbf{x}$ is calculated as follows.

$$\mathbf{x}^{-1} = n(\mathbf{x})^{-1}(\mathbf{x}^q), \tag{1.12}$$

where $\mathbf{x}$, $\mathbf{x}^q$ are the conjugates and $n(\mathbf{x}) \in \mathbb{F}_q^*$ is their product. FM of $\mathbf{x}$, $\pi_q(\mathbf{x}) = (x_0 + x_1\omega)^q$ can be easily calculated using an irreducible binomial as follows:

$$\begin{aligned}(x_0 + x_1\omega)^q &= \sum_{i=0}^{q} \binom{q}{i} x_0^{(q-i)}(x_1\omega)^i\\ &= x_0 + x_1\omega^q\\ &= x_0 + x_1(\omega^2)^{\frac{q-1}{2}}\omega\\ &= x_0 + x_1(c)^{\frac{q-1}{2}}\omega\\ &= x_0 - x_1\omega, \end{aligned}\tag{1.13}$$

where we substituted the modular relation $\omega^q = -\omega$. In other words, the conjugate of $\mathbf{x}$ is given as $x_0 - x_1\omega$. Therefore, the calculation procedure for $n(\mathbf{x}) = \mathbf{x}\pi_q(\mathbf{x})$ is as follows:

$$\begin{aligned}n(\mathbf{x}) &= (x_0 + x_1\omega)(x_0 - x_1\omega)\\ &= x_0^2 - x_1^2\omega^2\\ &= x_0^2 - cx_1^2. \end{aligned}\tag{1.14}$$

Since $n(\mathbf{x})$ is given without ω, it is found that $n(\mathbf{x})$ is a scalar. Finally, the inversion Eq.(1.12) is efficiently calculated.

1.3 Efficient scalar multiplication

In the context of pairing-based cryptography especially on BN curve, three groups $\mathbb{G}_1, \mathbb{G}_2$, and $\mathbb{G}_T$ are considered. Among them, $\mathbb{G}_1, \mathbb{G}_2$ are rational point groups and $\mathbb{G}_T$ is the multiplicative group in the extension field. They have the same order r. Let us consider a rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{q^2})$ as $Q(\mathbf{x}, \mathbf{y}) = (x_0 + x_1\omega, y_0 + y_1\omega)$. In the case of BN curve, it is known that Q satisfies the following relations:

$$\begin{aligned} [p + 1 - t]Q &= O \\ [t - 1]Q &= [p]Q. \end{aligned} \tag{1.15}$$

$$\begin{aligned} [\pi_p - p]Q &= O \\ \pi_p(Q) &= [p]Q. \end{aligned} \tag{1.16}$$

Thus, these relations can accelerate a scalar multiplication in $\mathbb{G}_2$. From Eq.(3.11) $\pi_p(Q) = [p]Q$. Substituting $[p]Q$ in Eq.(3.10) we find $[t-1]Q = \pi_p(Q)$. Next, let us consider SM $[s]Q$, where $0 \le s \le r$. From Eq.(1.3) we know r is the order of BN curve where $[r]Q = O$. Here, the bit size of s is nearly equal to r. As previously said, in BN curve r is two times larger than the bit size of t. It means that s is two times larger than the bit size of $t-1$. Therefore, let us consider $[t-1]$-adic representation of s as $s = s_0 + s_1(t-1)$, where s will be separated into two coefficients s_0 and s_1 whose size will be nearly equal to or less than the size of $[t-1]$. Then SM $[s]Q$ is calculated as follows:

$$\begin{aligned} [s]Q &= [s_0]Q + [s_1(t-1)]Q \\ &= [s_0]Q + s_1\pi_p(Q). \end{aligned} \tag{1.17}$$

Then, applying a multi-scalar multiplication technique, the above calculation will be efficiently carried out.

1.4 Conclusion and future work

In this paper, we have introduced an acceleration of scalar multiplication on Barreto-Naehrig (BN) curve defined over 2 degree extension field $\mathbb{F}_{q^2}$, $q = p^6$. We have showed that $[t-1]$-adic representation of large scalar number along with Frobenius mapping (FM) on rational points accelerates SM operation significantly, where t is the Frobenius trace of BN curve. As a future work, we would like to evaluate its computational time with a large prime characteristic as a practical situation.

Chapter 2

WISA 2016

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.

2.1 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 [**id_based**], broadcast encryption [10] and group signature authentication [9] surge the popularity of pairing based cryptography. In such consequence Ate-based pairings such as Ate [11] and Optimal-ate [27], twisted Ate [20] and χ-Ate [23] 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 $\mathbb{G}_3$ [26] 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) [16] pairing friendly curves of emebdding degree $k = 18$ described in [12]. 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 [7] and curves [5] along with extension field arithmetic [3]. 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 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 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. [**nogami**], 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.

2.2 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.

2.2.1 Elliptic curve [28]

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

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b, \tag{2.1}$$

where $4a^3 + 27b^2 \neq 0$ and $a, b \in \mathbb{F}_p$. Points satisfying Eq.(4.1) 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:

$$(x_n, y_n) \quad = \quad ((\lambda^2 - x_l - x_m), (x_l - x_n)\lambda - y_l), \tag{2.2a}$$

where λ is given as follows:

$$\lambda = \begin{cases} (y_m - y_l)(x_m - x_l)^{-1} & (L \neq M \text{ and } x_m \neq x_l), \\ \\ (3x_l^2 + a)(2y_l)^{-1} & (N = M \text{ and } y_l \neq 0), \end{cases} \tag{2.2b}$$

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,

$$[s]M = \underbrace{M + M + \cdots + M}_{s-1 \quad \text{times additions}}. \tag{2.3}$$

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.

2.2.2 KSS curve

KSS curve is a non super-singular pairing friendly elliptic curve of embedding degree 18 [16]. The equation of KSS curve defined over $\mathbb{F}_{p^{18}}$ is given by

$$E : Y^2 = X^3 + b, \quad (b \in \mathbb{F}_p), \tag{2.4}$$

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:

$$\begin{aligned} p(z) &= (z^8 + 5z^7 + 7z^6 + 37z^5 + 188z^4 + 259z^3 + 343z^2 \\ &\quad +1763z + 2401)/21, && \text{(2.5a)} \\ r(z) &= (z^6 + 37z^3 + 343)/343, && \text{(2.5b)} \\ t(z) &= (z^4 + 16z + 7)/7, && \text{(2.5c)} \end{aligned}$$

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.

$$\#E(\mathbb{F}_{p^{18}}) = p^{18} + 1 - t_{18}, \tag{2.6}$$

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. [25] 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 $E(\mathbb{F}_{p^{18}})$.

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 [14] has been done on constructing Frobenius mapping and utilizing it to calculate scalar multiplication. Nogami et al. [**nogami**] 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.

2.2.3 $\mathbb{F}_{p^{18}}$ 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 [26]. Therefore it is important to construct the field as a tower of extension fields [8] 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, shuch as Bailey et al. [2] 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 [16], 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.

2.3 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.(3.11) relation. Next, a scalar s will be considered for scalar multiplication of $[s]Q$. After that, as Figure 3.3, $(t-1)$-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 3.4, 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 $(t-1)$ as Eq.(4.6c). Next we will pre-compute the Frobenius maps of some rational points defined by detailed procedure. As shown in Eq.(3.20), considering 3 pairs from the coefficients we will apply the mult-scalar multiplication in addition with Frobenious mapping, as shown in Figure 3.5 to calculate scalar multiplication efficiently. Later part of this section will provide the detailed procedure of the proposal.

Figure 3.3 shows $(t-1)$-adic representation of scalar s.

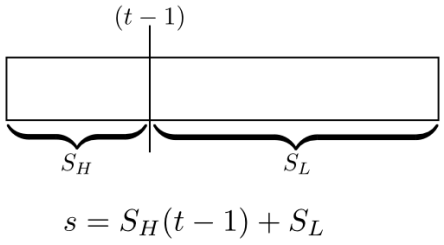


FIGURE 2.1: $(t-1)$ -adic representation of scalar s.

Figure 3.4 shows the final z-adic representation of scalar s.

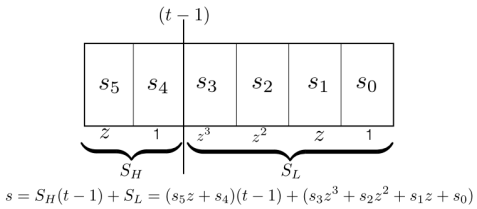


FIGURE 2.2: z-adic and $(t-1)$-adic representation of scalar s.

Figure 3.5 shows, an example of multi-scalar multiplication process, implemented in the experiment.

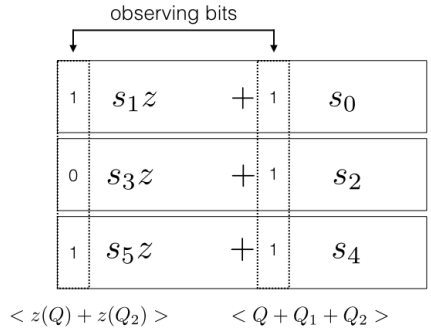


FIGURE 2.3: Multi-scalar multiplication of s with Frobenius mapping.

$\mathbb{G}_1$, $\mathbb{G}_2$ 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 [21], we define $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ as follows:

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

$$\alpha : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3, \tag{2.7}$$

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,

$$\begin{aligned} [p + 1 - t]Q &= \mathcal{O}, \\ [t - 1]Q &= [p]Q. \end{aligned} \tag{2.8}$$

$$\begin{aligned} [\pi_p - p]Q &= \mathcal{O}, \\ \pi_p(Q) &= [p]Q. \end{aligned} \tag{2.9}$$

Thus, these relations can accelerate a scalar multiplication in $\mathbb{G}_2$. Substituting $[p]Q$ in Eq.(3.10) 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.(4.6b), Eq.(4.6b), Eq.(4.6c) of KSS curve.

$$z + 3p - p^4 \equiv 0 \bmod r. \tag{2.10}$$

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.(4.6b) 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:

$$s = S_H(t-1) + S_L, \tag{2.11}$$

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:

$$\begin{aligned} S_H &= s_5 + s_4, \\ S_L &= s_3z^3 + s_2z^2 + s_1z + s_0. \end{aligned}$$

Finally s can be represented as 6 coefficients as follows:

$$\begin{aligned} s &= \sum_{i=0}^{3} s_i z^i + (s_4 + s_5 z)(t-1), \\ s &= (s_0 + s_1 z) + (s_2 + s_3 z)z^2 + (s_4 + s_5 z)(t-1). \end{aligned} \tag{2.12}$$

Reducing the number of ECA and ECD for calculating $[s]Q$.

Let us consider a scalar multiplication of $Q \in \mathbb{G}_2$ in Eq.(3.20) as follows:

$$[s]Q = (s_0 + s_1 z)Q + (s_2 + s_3 z)z^2Q + (s_4 + s_5 z)(t-1)Q. \tag{2.13}$$

Let us denote z^2Q, $(t-1)Q$ of Eq.(3.21) as Q_1 and Q_2 respectively. From Eq.(3.18) and Eq.(3.11) we can derive the Q_1 as follows:

$$\begin{aligned} Q_1 &= z^2Q, \\ &= (9p^2 - 6p^5 + p^8)Q, \\ &= 9\pi^2(Q) - 6\pi^5(Q) + \pi^8(Q). \end{aligned} \tag{2.14}$$

Using the properties of cyclotomic polynomial Eq.(3.22) is simplified as,

$$\begin{aligned} Q_1 &= 8\pi^2(Q) - 5\pi^5(Q), \\ &= \pi^2(8Q) - \pi^5(5Q). \end{aligned} \tag{2.15}$$

And from the Eq.(3.10) and Eq.(3.11), Q_2 is derived as,

$$Q_2 = \pi(Q). \tag{2.16}$$

Substituting Eq.(3.23) and Eq.(3.24) in Eq.(3.21), the following relation is obtained.

$$s[Q] = (s_0 + s_1 z)Q + (s_2 + s_3 z)Q_1 + (s_4 + s_5 z)Q_2. \tag{2.17}$$

Using $z \equiv -3p + p^4 \pmod{r}$ from Eq.(3.18), $z(Q)$ can be pre-computed as follows:

$$z(Q) = \pi(-3Q) + \pi^4(Q). \tag{2.18}$$

Table 3.1 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 the multi-scalar multiplication technique in Eq.(3.25) we can efficiently calculate the scalar multiplication. Figure 3.5 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.

TABLE 2.1: Pre-computed values of rational point for efficient scalar multiplication

$\bullet$	$z(Q)$
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 Figure 3.5, during scalar multiplication in parallel, we are considering Eq.(3.20) 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.

2.4 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 $y^2 = x^3 + 11$.

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

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

Analyzing Table 4.2 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.

Table 2.2: 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 10.11.4	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

*Only single core is used from two cores.

Table 2.3: 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

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

2.5 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.

Chapter 3

IEICE 2016

Improvement of Scalar Multiplication by Skew Frobenius Map with Multi-Scalar Multiplication for KSS Curve

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.

3.1 Introduction

Pairing based cryptography has attracted many researchers since Sakai et al. [**sakai**] and Joux et al. [15] independently proposed a cryptosystem based on elliptic curve pairing. This has encouraged to invent several innovative pairing based cryptographic applications such as broadcast encryption [10] and group signature authentication [9], 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 [11], Optimal-ate [27], twisted Ate [20], χ-Ate [23] and *sub-field twisted* Ate [**devegili**] 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 [16] 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 $\mathbb{G}_3$ [26]. The typical notation of pairing is $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$. In Ate-based pairing, $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ are defined as:

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

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

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) [16] 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 [**nogami**][24] on efficiently computing scalar multiplication defined over Barreto-Naehrig[6] curve along with efficient extension field arithmetic [3]. 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 [24] 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 $z \equiv -3p + p^4 \bmod r$,[1] derived by Aranha et al,[1] and the properties of $\mathbb{G}_2$ rational point, the scalar can be expressed as z-adic representation. Together with skew 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 $\mathbb{F}_{p^k}$.

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

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.

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.

3.2.1 Elliptic curve

An elliptic curve [28] defined over $\mathbb{F}_p$ is generally represented by *affine coordinates* [26] as follows;

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b, \tag{3.1}$$

where $4a^3 + 27b^2 \neq 0$ and $a, b \in \mathbb{F}_p$. A pair of coordinates x and y that satisfy Eq.(4.1) 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 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:

$$x_3 = \lambda^2 - x_1 - x_2, \tag{3.2a}$$
$$y_3 = (x_1 - x_3)\lambda - y_1, \tag{3.2b}$$

where λ is given as follows:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}; & P_1 \neq P_2, \\ \frac{3x_1^2 + a}{2y_1}; & P_1 = P_2, \end{cases} \tag{3.2c}$$

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).

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,

$$[s]P_1 = \sum_{i=0}^{s-1} P_1, \quad 0 \leq s < r, \tag{3.3}$$

When $s = r$, then $[r]P_1 = O$ 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.

3.2.2 KSS curve

In [16], 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:

$$E : Y^2 = X^3 + b, \quad (b \in \mathbb{F}_p), \tag{3.4}$$

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:

$$\begin{aligned} p(z) &= (z^8 + 5z^7 + 7z^6 + 37z^5 + 188z^4 + 259z^3 \\ &\quad +343z^2 + 1763z + 2401)/21, && \text{(3.5a)} \\ r(z) &= (z^6 + 37z^3 + 343)/343, && \text{(3.5b)} \\ t(z) &= (z^4 + 16z + 7)/7, && \text{(3.5c)} \end{aligned}$$

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. [1] and Scott et al. [25] 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 [1] for 192 bit security on KSS curve in the simulation implementation. In the recent work, Kim et al. [17] 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 [17]. However the parameter settings used in this paper in order to show the resemblance of the proposal with the experimental result.

3.2.3 $\mathbb{F}_{p^{18}}$ extension field arithmetic

Pairing based cryptography requires to perform arithmetic operation in extension fields of degree $k \geq 6$[26]. In the previous works of Bailey et al. [2] 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 [16], 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.

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. [24] 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.

3.2.4 Sextic twist of KSS curve

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

$$E : \quad y^2 = x^3 + b, \quad b \in \mathbb{F}_p, \tag{3.6}$$

$$E'_6 : \quad y^2 = x^3 + bu^{-1}, \tag{3.7}$$

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:

$$\psi_6 : \begin{cases} E'_6(\mathbb{F}_{p^e}) \rightarrow E(\mathbb{F}_{p^{6e}}), \\ (x, y) \quad \mapsto (xu^{1/2}, yu^{1/2}). \end{cases} \tag{3.8}$$

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

3.3 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.

Overview of the proposal

Figure 3.1 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 3.1. 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.

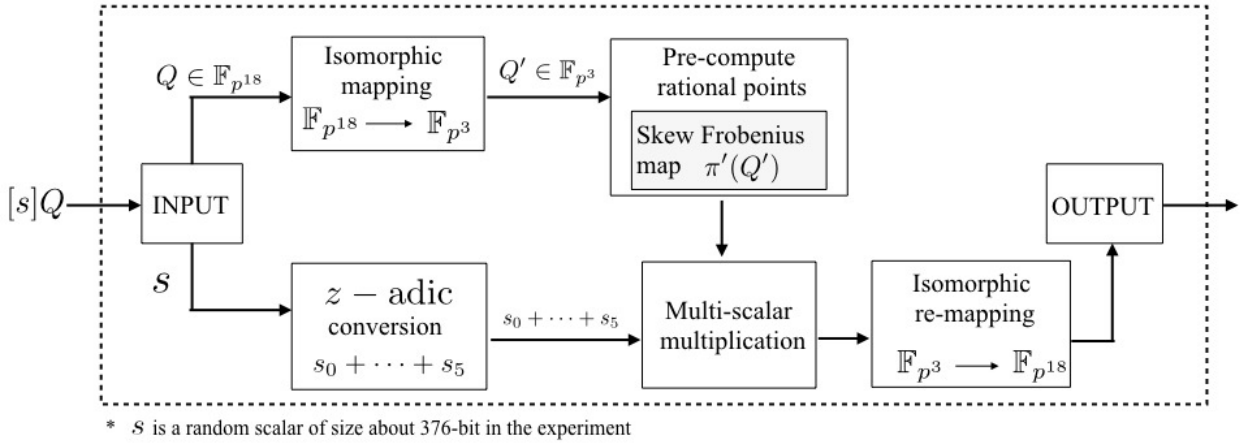


FIGURE 3.1: Overview of the proposed scalar multiplication.

3.3.1 $\mathbb{G}_1$, $\mathbb{G}_2$ 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 [21], we define $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ as follows:

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

$$\alpha : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3, \tag{3.9}$$

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,

$$\begin{aligned} [p+1-t]Q &= O, \\ [t-1]Q &= [p]Q. \end{aligned} \tag{3.10}$$

$$\begin{aligned} [\pi_p - p]Q &= O, \\ \pi_p(Q) &= [p]Q. \end{aligned} \tag{3.11}$$

where $[t-1]Q = \pi_p(Q)$, by substituting $[p]Q$ in Eq.(3.10).

3.3.2 Isomorphic mapping between Q and Q'

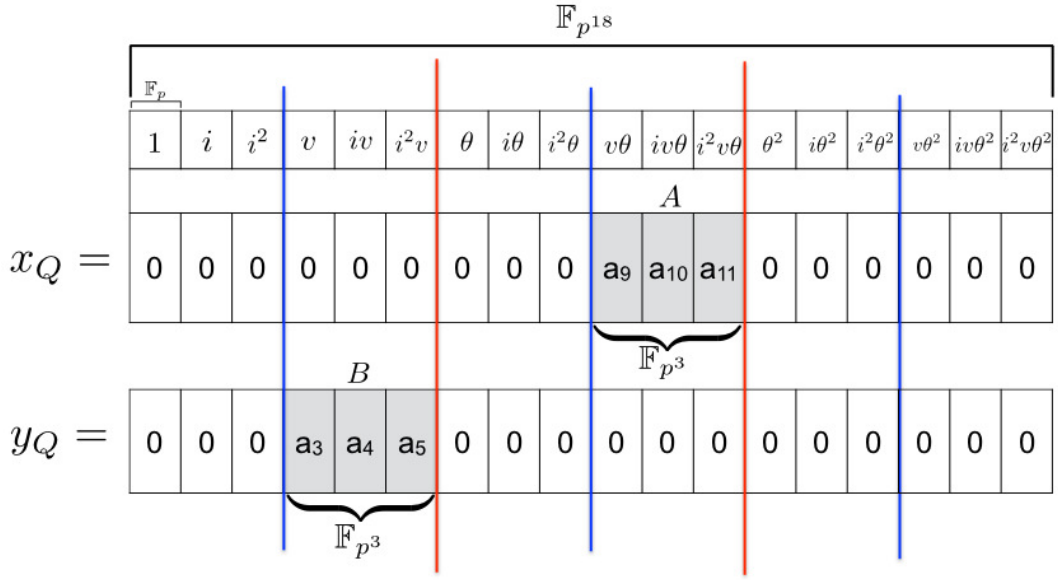
Let us consider E is the KSS curve in base field $\mathbb{F}_{p^3}$ and E' is sextic twist of E given as follows:

$$E : y^2 = x^3 + b, \tag{3.12}$$
$$E' : y^2 = x^3 + bi, \tag{3.13}$$

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 4.2 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



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

FIGURE 3.2: $Q \in \mathbb{F}_{p^{18}}$ and its sextic twisted isomorphic rational point $Q' \in \mathbb{F}_{p^3}$ structure in KSS curve.

belongs to a $\mathbb{F}_{p^3}$ element. The other coefficients are zero. In this paper, considering parameter settings given in Table 5.1 of section 4; Q is given as $Q = (Av\theta, Bv)$, showed in Figure 4.2, 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'.

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

Let's multiply θ^{-6} with both side of Eq.(4.13), where $i = \theta^6$ and $v = \theta^3$.

$$E' : \left(\frac{y}{\theta^3}\right)^2 = \left(\frac{x}{\theta^2}\right)^3 + b. \tag{3.14}$$

Now θ^{-2} and θ^{-3} of Eq.(4.14) can be represented as follows:

$$\theta^{-2} = i^{-1}\theta^4, \tag{3.15a}$$
$$\theta^{-3} = i^{-1}\theta^3. \tag{3.15b}$$

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

$$Q = (A\theta^4, B\theta^3), \quad \text{where } v = \theta^3. \tag{3.16}$$

From Eq.(4.15a) and Eq.(4.15c) $\theta^4 = i\theta^{-2}$ and $\theta^3 = i\theta^{-3}$ is substituted in Eq.(4.16) as follows:

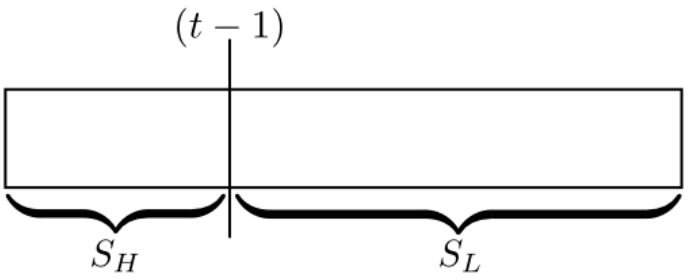
$$Q = (Ai\theta^{-2}, Bi\theta^{-3}), \tag{3.17}$$

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 3.2.3, 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 3.2.3.

3.3.3 z-adic representation of scalar s

In context of KSS curve, properties of Q will be obtained to define the Eq.(3.11) 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 3.3. 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 3.4, 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.(4.6c).

Figure 3.3 shows $(t-1)$-adic representation of scalar s.



$$s = S_H(t-1) + S_L$$

FIGURE 3.3: $(t-1)$ -adic representation of scalar s.

Figure 3.4 shows the z-adic representation of scalar s. In the previous work on optimal-ate pairing, Aranha et al. [1] derived a relation from the parameter setting of KSS curve as follows:

$$z + 3p - p^4 \equiv 0 \bmod r, \tag{3.18}$$

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 $0 \leq s < r$. $[s]Q'$ 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.(4.6b) 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:

$$s = S_H(t-1) + S_L, \tag{3.19}$$

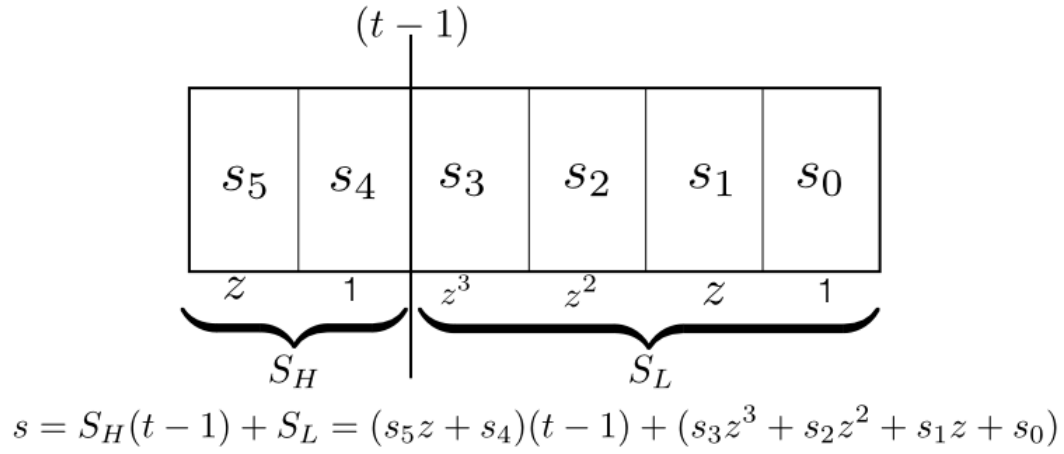


FIGURE 3.4: z-adic and $(t-1)$-adic representation of scalar s.

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:

$$\begin{aligned} S_H &= s_5 + s_4, \\ S_L &= s_3z^3 + s_2z^2 + s_1z + s_0. \end{aligned}$$

Finally s can be represented as 6 coefficients as follows:

$$\begin{aligned} s &= \sum_{i=0}^{3} s_i z^i + (s_4 + s_5 z)(t-1), \\ s &= (s_0 + s_1 z) + (s_2 + s_3 z)z^2 + (s_4 + s_5 z)(t-1). \end{aligned} \tag{3.20}$$

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

Let us consider a scalar multiplication of $Q' \in \mathbb{G}_2'$ in Eq.(3.20) as follows:

$$[s]Q' = (s_0 + s_1 z)Q' + (s_2 + s_3 z)z^2Q' + (s_4 + s_5 z)(t-1)Q'. \tag{3.21}$$

In what follows, z^2Q', $(t-1)Q'$ of Eq.(3.21) is denoted as Q_1' and Q_2' respectively. From Eq.(3.18) and Eq.(3.11) we can derive the Q_1' as follows:

$$\begin{aligned} Q_1' &= z^2Q', \\ &= (9p^2 - 6p^5 + p^8)Q', \\ &= 9\pi'^2(Q') - 6\pi'^5(Q') + \pi'^8(Q'). \end{aligned} \tag{3.22}$$

where $\pi'(Q')$ is called the **skew Frobenius mapping** of rational point $Q' \in E'(\mathbb{F}_{p^3})$. Eq.(3.22) is simplified as follows by utilizing the properties of cyclotomic polynomial.

$$\begin{aligned} Q_1' &= 8\pi'^2(Q') - 5\pi'^5(Q'), \\ &= \pi'^2(8Q') - \pi'^5(5Q'). \end{aligned} \tag{3.23}$$

And from the Eq.(3.10) and Eq.(3.11), Q_2' is derived as,

$$Q_2' = \pi'(Q'). \tag{3.24}$$

Substituting Eq.(3.23) and Eq.(3.24) in Eq.(3.21), the following relation is obtained.

$$s[Q'] = (s_0 + s_1 z)Q' + (s_2 + s_3 z)Q'_1 + (s_4 + s_5 z)Q'_2. \tag{3.25}$$

Using $z \equiv -3p + p^4 \pmod{r}$ from Eq.(3.18), $z(Q')$ can be pre-computed as follows:

$$z(Q') = \pi'(-3Q') + \pi'^4(Q'). \tag{3.26}$$

Table 3.1 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.

TABLE 3.1: 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	$z(Q'_2)$
$Q'_1 + Q'_2$	$z(Q'_1) + z(Q'_2)$
$Q' + Q'_2$	$z(Q') + z(Q'_2)$
$Q' + Q'_1$	$z(Q') + z(Q'_1)$
$Q' + Q'_1 + Q'_2$	$z(Q') + z(Q'_1) + z(Q'_2)$

3.3.4 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:

$$\pi' : (x', y') \mapsto (x'^p, y'^p) \tag{3.27}$$

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:

$$\begin{aligned}
\pi'(x') &= (x')^p (i)^{1-p} (v)^{p-1} (\theta)^{p-1} \\
&= (x')^p (i)^{1-p} (\theta^4)^{p-1} \\
&= (x')^p (i^{-1})^p i (\theta^{p-1})^4 \\
&= (x')^p (i^{-1})^p i (i^{\frac{p-1}{6}})^4 \quad \text{where } \theta^6 = i \\
&= (x')^p (i^{-1})^p i (i^{\frac{p-1}{6}-1} i)^4 \\
&= (x')^p (i^{-1})^p i (i^{3\frac{\frac{p-7}{6}}{3}})^4 i^4 \\
&= (x')^p (i^{-1})^p i (2^{\frac{p-7}{18}})^4 2i \quad \text{where } i^3 = 2 \\
&= (x')^p (i^{-1})^p i (2^{\frac{2p-14}{9}+1}) i \\
&= (x')^p (i^{-1})^p i (2^{\frac{2p-5}{9}}) i,
\end{aligned} \tag{3.28a}$$

$$\begin{aligned}
\pi'(y') &= (y')^p (i)^{1-p} (v)^{p-1} \\
&= (y')^p (i^{-1})^p i (v^{6\frac{p-1}{6}}) \\
&= (y')^p (i^{-1})^p i (i^{3\frac{p-1}{6}}) \\
&= (y')^p (i^{-1})^p i 2^{\frac{p-1}{6}}.
\end{aligned} \tag{3.28b}$$

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

3.3.5 Multi-scalar multiplication

Applying the the multi-scalar multiplication technique in Eq.(3.25) we can efficiently calculate the scalar multiplication in $\mathbb{F}_{p^3}$. Figure 3.5 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.

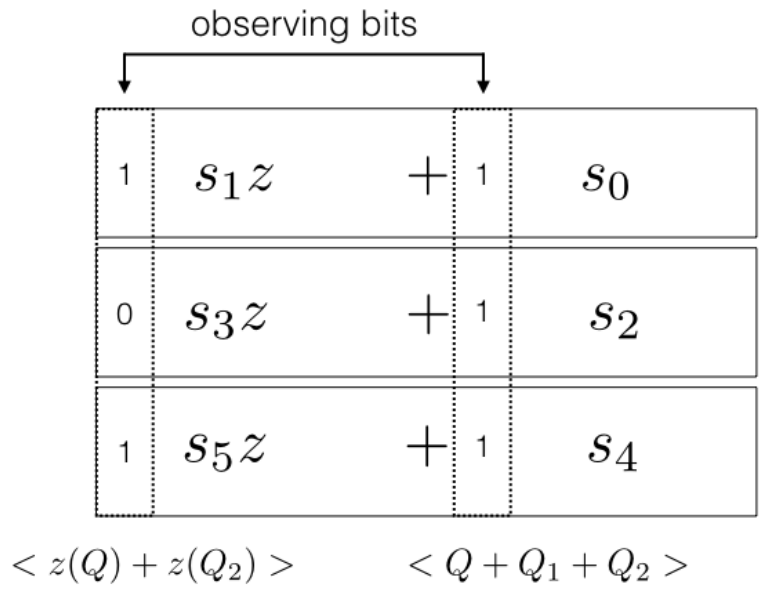


FIGURE 3.5: Multi-scalar multiplication of s with Frobenius mapping.

As shown in Figure 3.5, during scalar multiplication, we are considering 3 pair of coefficients of z-adic representation as shown in Eq.(3.20). 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.

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.(4.15a), Eq.(4.15c) and Eq.(4.14) 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.

3.4 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. [25] to obtain $p = 508 \approx 511$-bit and $r = 376 \approx 384$-bit to simulate in 192-bit security level. Table 5.1 shows the parameter settings considered for the simulation.

TABLE 3.2: 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 4.1 shows the environment, used to experiment and evaluate the proposed method.

TABLE 3.3: 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.

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.

In Table ?? 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

TABLE 3.4: Comparison of average number of ECA and ECD

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

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 3.5: Comparison of execution time in [ms] for scalar multiplication

	Execution time in [ms]			
	With isomorphic mapping		Without isomo	
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 3.5, 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.

3.5 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. [24] 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.

Chapter 4

CANDAR 2016

Pairing based cryptography is considered as the next generation of security for which it attracts many researcher to work on faster and efficient pairing to make it practical. Among the several challenges of efficient pairing; efficient scalar multiplication of rational point defined over extension field of degree $k \geq 12$ is important. However, there exists isomorphic rational point group defined over relatively lower degree extension field. Exploiting such property, this paper has showed a mapping technique between isomorphic rational point groups in the context of Ate-based pairing with Kachisa-Schaefer-Scott (KSS) pairing friendly curve of embedding degree $k = 18$. In the case of KSS curve, there exists sub-field sextic twisted curve that includes sextic twisted isomorphic rational point group defined over $\mathbb{F}_{p^3}$. This paper has showed the mapping procedure from certain $\mathbb{F}_{p^{18}}$ rational point group to its sub-field isomorphic rational point group in $\mathbb{F}_{p^3}$ and vice versa. This paper has also showed that scalar multiplication is about 20 times faster after applying the proposed mapping which in-turns resembles that the impact of this mapping will greatly enhance the pairing operation in KSS curve.

4.1 Introduction

At the advent of this century, Sakai et al. [**sakai**] and Joux et al. [15] independently proposed a cryptosystem based on elliptic curve pairing. Since then, pairing based cryptography has attracted many researchers and it has been considered as the basis of next generation security. Many researchers have proposed several innovative pairing based cryptographic applications such as ID-based encryption [**sakai**], broadcast encryption [10] and group signature authentication [9] that upsurge the popularity of pairing based cryptography. In such outcome, Ate-based pairings such as Ate [11], R-ate [19], Optimal-ate [27], twisted Ate [20] and χ-Ate [23] pairings have gained much attention since they have achieved quite efficient pairing calculation. There is no alternative of efficient and fast pairing calculation for deploying pairing-based cryptographic applications in practical case. This paper focuses on a peripheral technique of Ate-based pairings with Kachisa-Schaefer-Scott (KSS) curve [16].

In general, pairing is a bilinear map from two rational point group $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group $\mathbb{G}_3$ [26], typically denoted by $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$. In the context 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. Pairings are often 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 E of embedded extension field of degree k. This paper has considered Kachisa-Schaefer-Scott (KSS) [16] pairing friendly curves of emebdding degree $k = 18$ described in [12].

In Ate-based pairing with KSS curve, where $k = 18$, pairing computations are done in higher degree extension field $\mathbb{F}_{p^{18}}$. However, KSS curves defined over $\mathbb{F}_{p^{18}}$ have the sextic twisted isomorphism over $\mathbb{F}_{p^3}$. Therefore we can execute computations in the sub-field $\mathbb{F}_{p^3}$. Exploiting such a property, different arithmetic operation of Ate-based pairing can be efficiently performed in $\mathbb{G}_2$. In this paper we have mainly focused on mapping $\mathbb{G}_2$ rational point from extension field $\mathbb{F}_{p^{18}}$ to its sextic twisted sub-field $\mathbb{F}_{p^3}$ and its reverse procedure.

The advantage of such mapping is examined by performing scalar multiplication on $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ rational point, since scalar multiplication is required repeatedly in cryptographic calculation. We have considered sub-field sextic twisted curve of KSS curve, denoted as E'. It includes sextic twisted isomorphic rational point group denoted as $\mathbb{G}_2' \subset E(\mathbb{F}_{p^3})$. 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 $\mathbb{F}_{p^3}$. Then the proposed mapping technique is applied to map rational points of $\mathbb{G}_2$ to its isomorphic $\mathbb{G}_2'$. After that the scalar multiplication in $\mathbb{G}_2'$ performed and the resulted points are re-mapped to $\mathbb{G}_2$ in $\mathbb{F}_{p^{18}}$. The experiment result shows that efficiency of binary scalar multiplication is increased by more than 20 times in sub-field sextic twisted curve than scalar multiplication in $\mathbb{F}_{p^{18}}$ without applying proposed mapping. The mapping and remapping requires one bit wise shifting in $\mathbb{F}_p$, one $\mathbb{F}_{p^3}$ inversion which can be pre-computed and one $\mathbb{F}_p$ multiplication; hence the mapping procedure has no expensive arithmetic operation.

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 II. In section III, this paper describes the isomorphic mapping between the rational point Q and Q' in details. The experimental result is presented in section IV which shows that our scalar multiplication on $\mathbb{G}_2$ point can be accelerated by 20 times by applying the proposed mapping technique in KSS curve. Finally section V draws the conclusion with some outline how this work can be enhanced more as a future work.

4.2 Preliminaries

In this section this paper briefly overviews the fundamentals of elliptic curve operations. Elliptic curve scalar multiplication is reviewed briefly. Pairing friendly curve of embedded degree $k = 18$, i.e., KSS curve and its properties are introduced in combination with its construction procedure by towering.

4.2.1 Elliptic curve

Let $\mathbb{F}_p$ be a prime field and $\mathbb{F}_q$ be its extension field. An elliptic curve [28] defined over $\mathbb{F}_p$ is generally represented by *affine coordinates* [26] as follows;

$$E/\mathbb{F}_p : y^2 = x^3 + ax + b, \tag{4.1}$$

where $4a^3 + 27b^2 \neq 0$ and $a, b \in \mathbb{F}_p$. A pair of coordinates x and y that satisfy Eq.(4.1) are known as *rational points* on the curve.

$E(\mathbb{F}_{q^k})$ denotes an elliptic curve group where the definition field is $\mathbb{F}_{q^k}$ and $\#E(\mathbb{F}_{q^k})$ denotes its order. When the definition field is prime field $\mathbb{F}_p$ then $\#E(\mathbb{F}_p)$ can be represented as,

$$\#E(\mathbb{F}_p) = p + 1 - t, \tag{4.2}$$

where t is called the Frobenius trace of $E(\mathbb{F}_p)$.

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. The set of rational points over $\mathbb{F}_q$, including $\mathcal{O}$ satisfying Eq.(4.1) is denoted by $E(\mathbb{F}_q)$. The order of $E(\mathbb{F}_q)$ is denoted by $\#E(\mathbb{F}_q)$.

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 $P_1, P_2, R \in E(\mathbb{F}_q)$. Then the x and y coordinates of R are calculated as follows:

$$x_3 = \lambda^2 - x_1 - x_2, \tag{4.3a}$$
$$y_3 = (x_1 - x_3)\lambda - y_1, \tag{4.3b}$$

where λ is given as follows:

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1}; & P_1 \neq P_2, \\ \frac{3x_1^2 + a}{2y_1}; & P_1 = P_2, \end{cases} \tag{4.3c}$$

λ is the tangent at the point on the curve and $\mathcal{O}$ is the additive unity in $E(\mathbb{F}_q)$. When $P_1 \neq P_2$ 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).

Let $[s]P_1$ be the scalar multiplication for the rational point P_1 with scalar s as,

$$[s]P_1 = \sum_{i=0}^{s-1} P_1, \quad 0 \leq s < r, \tag{4.4}$$

where r is the order of the target rational point group. If $s = r$, where r is the order of the curve then $[r]P_1 = \mathcal{O}$. When $[s]P_1 = P_2$, if s is unknown, then the solving s from P_1 and P_2 is known as elliptic curve discrete logarithm problem (ECDLP). The security of elliptic curve cryptography depends on the difficulty of solving ECDLP.

The binary method is a widely recognized method for calculating the elliptic curve scalar multiplication. Algorithm 1 shows the binary scalar multiplication algorithm. This algorithm scans the bits of scalar s from most significant bit to least significant bit. When $s[i] = 1$, it will perform ECA and ECD otherwise only ECD will be

calculated. But this method is not resistant to side channel attack [18].

Algorithm 1: Left-to-right binary algorithm for elliptic curve scalar multiplication

Input: P, s

Output: $[s]P$

```
1 T ← 0
2 for i = ⌊log2 s⌋ to 0 do
      T ← T + T
      if s[i] = 1 then
          T ← T + P
3 return T
```

On the other hand Montgomery ladder algorithm is said to be resistant of side channel attack. Algorithm 2 shows the Montgomery ladder algorithm for scalar multiplication. Montgomery ladder has some similarity with binary method except in each iteration it performs ECA and ECD.

Algorithm 2: Montgomery ladder algorithm for elliptic curve scalar multiplication

Input: P, s

Output: $[s]P$

```
1 T0 ← 0, T1 ← P
2 for i = ⌊log2 s⌋ to 0 do
      if s[i] = 1 then
          T0 ← T0 + T1
          T1 ← T1 + T1
      else if s[i] = 0 then
          T1 ← T0 + T1
          T0 ← T0 + T0
3 return T0
```

This paper has considered left-to-right binary scalar multiplication for evaluating the efficiency of the proposed mapping operation. But from the view point of security binary method is vulnarable to side channel attack. Therefore this paper has also experimented with Montgomery ladder [26] for scalar multiplication evaluation.

4.2.2 KSS curve

Kachisa-Schaefer-Scott (KSS) curve [16] is a non super-singular pairing friendly elliptic curve of embedding degree 18, defined over $\mathbb{F}_{p^{18}}$ as follows:

$$E/\mathbb{F}_{p^{18}} : Y^2 = X^3 + b, \quad b \in \mathbb{F}_p, \tag{4.5}$$

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 u as follows:

$$\begin{aligned} p(u) &= (u^8 + 5u^7 + 7u^6 + 37u^5 + 188u^4 + 259u^3 \\ &\quad +343u^2 + 1763u + 2401)/21, \qquad (4.6a) \\ r(u) &= (u^6 + 37u^3 + 343)/343, \qquad (4.6b) \\ t(u) &= (u^4 + 16u + 7)/7, \qquad (4.6c) \end{aligned}$$

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

4.2.3 $\mathbb{F}_{p^{18}}$ extension field arithmetic

In pairing, arithmetic operations are performed in higher degree extension fields, such as $\mathbb{F}_{p^k}$ for moderate value of k [26]. Concequently, such higher extension field needs to be constructed as tower of extension fields [8] to perform arithmetic operation cost effectively.

This paper has represented extension field $\mathbb{F}_{p^{18}}$ as a tower of sub-field to improve arithmetic operations. It has also used irreducible binomials introduced by Bailey et al. [2]. In what follows, this paper considers $3|(p-1)$ and c is a quadratic and cubic non residue in $\mathbb{F}_p$. In context of KSS-curve [16], where $k = 18$, $\mathbb{F}_{p^{18}}$ is constructed as tower field with irreducible binomial as follows:

$$\begin{cases} \mathbb{F}_{p^3} = \mathbb{F}_p[i]/(i^3 - c), \\ \mathbb{F}_{p^6} = \mathbb{F}_{p^3}[v]/(v^2 - i), \\ \mathbb{F}_{p^{18}} = \mathbb{F}_{p^6}[\theta]/(\theta^3 - v), \end{cases} \qquad (4.7)$$

where $c = 2$ is considered to be the best choice for efficient arithmetic. From the above towering construction we can find that $i = v^2 = \theta^6$, where i is the basis element of the base extension field $\mathbb{F}_{p^3}$. In the previous work of Aranha et al. [1], explained the base extension field $\mathbb{F}_{p^3}$ for the *sextic twist* of KSS curve.

4.2.4 $\mathbb{G}_1$, $\mathbb{G}_2$ 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 [21], we define $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ as follows:

$$\begin{aligned} \mathbb{G}_1 &= E(\mathbb{F}_{p^{18}})[r] \cap \mathrm{Ker}(\pi_p - [1]), \\ \mathbb{G}_2 &= E(\mathbb{F}_{p^{18}})[r] \cap \mathrm{Ker}(\pi_p - [p]), \\ \mathbb{G}_3 &= \mathbb{F}^*_{p^{18}}/(\mathbb{F}^*_{p^{18}})^r, \\ & \alpha : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3, \qquad (4.8) \end{aligned}$$

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.

4.2.5 Sextic twist of KSS curve

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

$$\begin{aligned} E: \quad y^2 &= x^3 + b, \quad b \in \mathbb{F}_p, \qquad (4.9) \\ E'_6: \quad y^2 &= x^3 + bz^{-1}, \qquad (4.10) \end{aligned}$$

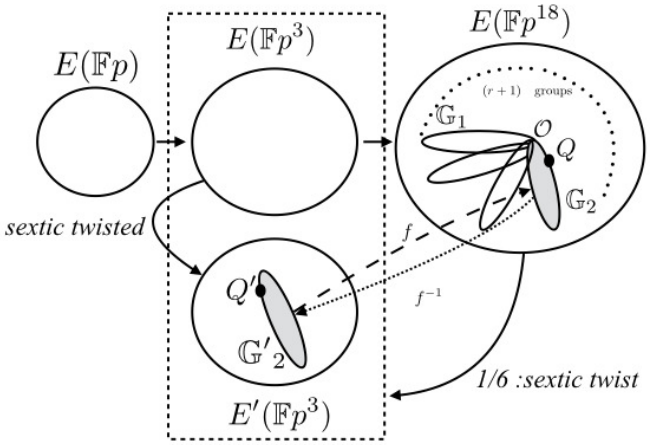


FIGURE 4.1: *sextic twist* in KSS curve.

where z 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:

$$\psi_6 : \begin{cases} E'_6(\mathbb{F}_{p^e}) \rightarrow E(\mathbb{F}_{p^{6e}}), \\ (x,y) \quad \mapsto (xz^{1/2}, yz^{1/2}). \end{cases} \tag{4.11}$$

In context of Ate-based pairing for KSS curve of embedding degree 18, sextic twist is considered to be the most efficient. This papers considers mapping of sextic twisted sub-field isomorphic group of $\mathbb{F}_{p^{18}}$.

4.3 Isomorphic mapping between Q and Q'

This section introduces our proposal of mapping procedure of $\mathbb{G}_2$ rational point group to its sextic twisted isomorphic group $\mathbb{G}'_2$ for Ate-based pairing with KSS curve.

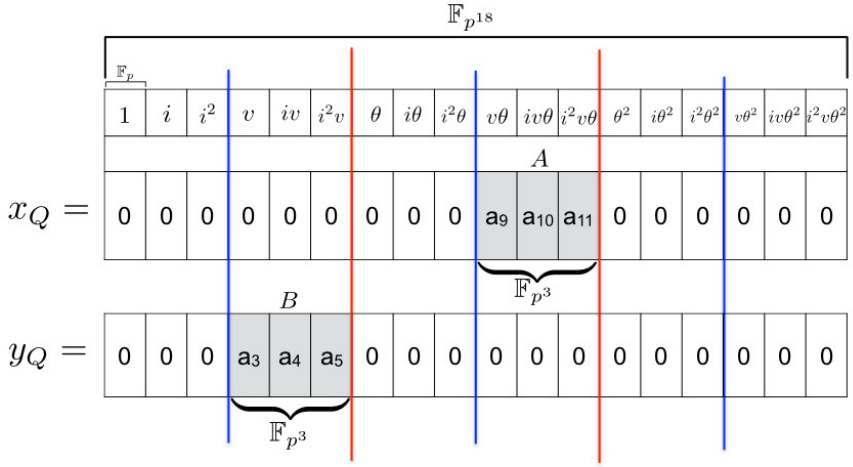
Figure 4.1 shows an overview of sextic twisted curve $E'(\mathbb{F}_{p^3})$ of $E(\mathbb{F}_{p^{18}})$. Let us consider E is the KSS curve in base field $\mathbb{F}_{p^3}$ and E' is sextic twist of E' given as follows:

$$E : y^2 = x^3 + b, \tag{4.12}$$
$$E' : y^2 = x^3 + bi, \tag{4.13}$$

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 $\mathbb{F}_{p^3}$.

In context of KSS curve, let us consider a rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$. Q has a special vector representation with 18 $\mathbb{F}_p$ elements for each x_Q and y_Q coordinates. Figure 4.2 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. The others are zero. However the set of these nonzero elements belongs to $\mathbb{F}_{p^3}$.

This paper considers the mother parameter of KSS curve u = 65-bit and characteristics p = 511-bit. In such consideration, Q is given as $Q = (Av\theta, Bv)$, showed in Figure 4.2, 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.



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

FIGURE 4.2: $Q \in \mathbb{F}_{p^{18}}$ and its sextic twisted isomorphic rational point $Q' \in \mathbb{F}_{p^3}$ structure in KSS curve.

Let us consider the sextic twisted isomorphic sub-field rational point of Q as $Q' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^3})$. Considering x' and y' as the coordinates of Q', we can map the rational point $Q = (Av\theta, Bv)$ to the rational point $Q' = (x', y')$ as follows.

Multiplying both side of Eq.(4.13) with θ^{-6}, where $i = \theta^6$ and $v = \theta^3$.

$$E' : \left(\frac{y}{\theta^3}\right)^2 = \left(\frac{x}{\theta^2}\right)^3 + b. \tag{4.14}$$

θ^{-2} of Eq.(4.14) can be represented as follows:

$$\begin{aligned} \theta^{-2} &= i^{-1} i\theta^{-2}, \\ &= i^{-1}\theta^4, \end{aligned} \tag{4.15a}$$

and multiplying i with both sides.

$$\theta^4 = i\theta^{-2}. \tag{4.15b}$$

Similarly θ^{-3} can be represented as follows:

$$\begin{aligned} \theta^{-3} &= i^{-1} i\theta^{-3} \\ &= i^{-1}\theta^3. \end{aligned} \tag{4.15c}$$

Multiplying i with both sides of Eq.(4.15c) we get θ^3 as,

$$\theta^3 = i\theta^{-3}, \tag{4.15d}$$

Q to Q' mapping

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

$$Q = (A\theta^4, B\theta^3), \quad \text{where } v = \theta^3. \tag{4.16}$$

From Eq.(4.15b) and Eq.(4.15d), we substitute $\theta^4 = i\theta^{-2}$ and $\theta^3 = i\theta^{-3}$ in Eq.(4.16) as follows:

$$Q = (Ai\theta^{-2}, Bi\theta^{-3}), \tag{4.17}$$

where $Ai = x'$ and $Bi = y'$ are the coordinates of $Q' = (x', y') \in \mathbb{F}_{p^3}$. Which implies that we can map $Q \in \mathbb{F}_{p^{18}}$ to $Q' \in \mathbb{F}_{p^3}$ by first selecting the 3 nonzero $\mathbb{F}_p$ coefficients of each coordinates of Q. Then these nonzero $\mathbb{F}_p$ elements form an $\mathbb{F}_{p^3}$ element. After that multiplying the basis element i with that $\mathbb{F}_{p^3}$ element, we get the final $Q' \in \mathbb{F}_{p^3}$. From the structure of $\mathbb{F}_{p^{18}}$, given in Eq.(4.7), 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 Eq.(4.7).

Q' to Q mapping

The reverse mapping $Q' = (x', y') \in \mathbb{F}_{p^3}$ to $Q = (Av\theta, Bv) \in \mathbb{F}_{p^{18}}$ can be obtained as from Eq.(4.15a), Eq.(4.15c) and Eq.(4.14) 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.

4.4 Result Analysis

In order to determine the advantage of the proposal, first we have applied the proposed mapping technique to map rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ to its isomorphic point $Q' \in \mathbb{G}_2' \subset E'(\mathbb{F}_{p^3})$. After that we performed the scalar multiplication of Q'. Then the resulted points are re-mapped to $\mathbb{G}_2$ in $\mathbb{F}_{p^{18}}$. On the other hand we performed scalar multiplication of Q without mapping. In the experiment, 100 scalar numbers of size (about 377-bit) less than order r is generated randomly and then scalar multiplication is calculated for both case. Average value of execution time is considered for comparison. The comparative result is shown in Table 4.2.

In the experiment, mother parameter u is also selected accordingly to find out $\mathbb{G}_2$ rational point Q. In addition p = 511-bit is considered, since Scott et al. [25] 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.

In the experiment, KSS curve over $\mathbb{F}_{p^{18}}$ is given as $y^2 = x^3 + 11$, considering the following parameters

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

Table 4.1 shows the experiment environment, used to evaluate usefulness of the proposed mapping.

Analyzing Table 4.2, we can find that scalar multiplication using the proposed mapping technique is more than 20 times faster than scalar multiplication without

Table 4.1: 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 10.11.4	iOS 9.3.1
Compiler	gcc 4.2.1	gcc 4.2.1
Programming Language	C	Objective-C, C
Library	GNU MP [13]	GNU MP

*Only single core is used from two cores.

Table 4.2: Comparative result of average execution time in [ms] for scalar multiplication

	Average execution time [ms] comparison	
	PC	iPhone 6s
	Execution time	Execution time
Binary method with mapping	5.4×10^1	6.4×10^1
Binary method without mapping	1.1×10^3	1.2×10^3
Montgomery ladder with mapping	6.8×10^1	8.4×10^1
Montgomery ladder without mapping	1.5×10^3	1.6×10^3

the proposed mapping. It this experiment we used binary method and Montgomery ladder for scalar multiplication in both case. In the previous work of Nogami et al. [**nogami**], has showed the procedure to apply Frobenious mapping on twisted elliptic curve for Ate-based pairing. This multiplication can be done more efficiently if skew Frobenius mapping is applied on sextic twisted isomorphic rational point after applying the proposed mapping.

In the experiment we have used two execution environments; such as PC and iPhone with different CPU frequencies. In both environments only one processor core is utilized. The result also shows that the ratio of execution time of PC and iPhone without mapping of both methods is about 0.9. On the other hand the ratio of execution time with mapping of both methods is about 0.8. But the ratio of CPU frequencies of iPhone and PC is about $1.84/2.7 \approx 0.68$. Since PC and iPhone has different processor architectures therefore it's frequency ratio has no relation with the execution time ratio.

The main focus of this experiment is to evaluate the acceleration ratio of scalar multiplication by applying the proposed mapping 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. There are other pairing friendly curves such as BLS-12, BLS-24 [12] where sextic twist is available. We will try to apply the proposed mapping on those curves as our future work.

4.5 Conclusion and future work

In this paper we have proposed mapping procedure of $\mathbb{G}_2$ rational point group to its sextic twisted sub-field isomorphic rational point group $\mathbb{G}_2'$ and its reverse mapping on KSS curve in context of Ate based pairing. We have also presented the advantages

of such mapping by applying binary scalar multiplication and Montgomery ladder on sextic twisted isomorphic rational points in $\mathbb{G}_2'$. Then result of scalar multiplication in $\mathbb{G}_2'$ can accelerate the scalar multiplication in $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ by more than 20 times than scalar multiplication of $\mathbb{G}_2$ rational point directly in $\mathbb{F}_{p^{18}}$. In the previous work of Sakemi et al. [24] has proposed skew Frobenious 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 mapping and the skew Frobenius mapping of $\mathbb{G}_1$ will remarkably accelerate scalar multiplication over KSS curve in the context of pairing based cryptography.

Acknowledgment

This work was partially supported by the Strategic Information and Communications R&D Promotion Programme (SCOPE) of Ministry of Internal Affairs and Communications, Japan.

Chapter 5

ICISC 2016

An Improvement of Optimal Ate Pairing on KSS curve with Pseudo 12-sparse Multiplication

Acceleration of a pairing calculation of an Ate-based pairing such as Optimal Ate pairing depends not only on the optimization of Miller algorithm's loop parameter but also on efficient elliptic curve arithmetic operation and efficient final exponentiation. Some recent works have shown the implementation of Optimal Ate pairing over Kachisa-Schaefer-Scott (KSS) curve of *embedding degree* 18. Pairing over KSS curve is regarded as the basis of next generation security protocols. This paper has proposed a *pseudo 12-sparse multiplication* to accelerate Miller's loop calculation in KSS curve by utilizing the property of rational point groups. In addition, this papers has showed an enhancement of the elliptic curve addition and doubling calculation in Miller's algorithm by applying implicit mapping of its sextic twisted isomorphic group. Moreover this paper has implemented the proposal with recommended security parameter settings for KSS curve at 192 bit security level. The simulation result shows that the proposed *pseudo 12-sparse multiplication* gives more efficient Miller's loop calculation of an Optimal Ate pairing operation along with recommended parameters than pairing calculation without sparse multiplication.

5.1 Introduction

From the very beginning of the cryptosystems that utilizes elliptic curve pairing; proposed independently by Sakai et al. [**sakai**] and Joux [15], has unlocked numerous novel ideas to researchers. Many researchers tried to find out security protocol that exploits pairings to remove the need of certification by a trusted authority. In this consequence, several ingenious pairing based encryption scheme such as ID-based encryption scheme by Boneh and Franklin [**id_based**] and group signature authentication by Nakanishi et al. [22] has come into the focus. In such outcome, Ate-based pairings such as Ate [11], Optimal-ate [27], twisted Ate [20], R-ate [19], and χ-Ate [23] pairings and their applications in cryptosystems have caught much attention since they have achieved quite efficient pairing calculation. But it has always been a challenge for researchers to make pairing calculation more efficient for being used practically as pairing calculation is regarded as quite time consuming operation.

Bilinear pairing operation consist of two predominant parts, named as Miller's loop and final exponentiation. Finding pairing friendly curves [12] and construction of efficient extension field arithmetic are the ground work for any pairing operation. Many research has been conducted for finding pairing friendly curves [**curve_1**, 5] and efficient extension field arithmetic [2] . Some previous work on optimizing the pairing algorithm on pairing friendly curve such Optimal Ate pairing by Matsuda et al. [20] on Barreto-Naehrig (BN) curve [6] is already carried out. The previous work of Mori et al. [21] has showed the *pseudo 8-sparse multiplication* to efficiently

calculate Miller's algorithm defined over BN curve. Apart from it, Aranha et al. [1] has improved Optimal Ate pairing over KSS curve for 192 bit security level by utilizing the relation $t(\chi) - 1 \equiv \chi + 3p(\chi) \bmod r(\chi)$ where $t(\chi)$ is the Frobenius trace of KSS curve, χ is an integer also known as *mother parameter*, $p(\chi)$ is the prime number and $r(\chi)$ is the order of the curve. This paper has exclusively focused on efficiently calculating the Miller's loop of Optimal Ate pairing defined over KSS curve [16] for 192-bit security level by applying *pseudo 12-sparse multiplication* technique along with other optimization approaches. The parameter settings recommended in [1] for 192 bit security on KSS curve is used in the simulation implementation. But in the recent work, Kim et al. [17] has suggested to update the key sizes associated with pairing-based cryptography due to the new development of discrete logarithm problem over finite field. The parameter settings of [1] doesn't end up at the 192 bit security level according to [17]. However the parameter settings of [1] is primarily adapted in this paper in order to show the resemblance of the proposal with the experimental result.

In general, pairing is a bilinear map from two rational point groups $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group $\mathbb{G}_3$ [26]. When KSS pairing-friendly elliptic curve of embedding degree $k = 18$ is chosen for Ate-based pairing, then the bilinear map is denoted by $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$, where $\mathbb{G}_1 \subset E(\mathbb{F}_p)$, $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ and $\mathbb{G}_3 \subset \mathbb{F}^*_{p^{18}}$ and p denotes the characteristic and E is the curve defined over corresponding extension field $\mathbb{F}_{p^k}$. Rational point in $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ has a special vector representation where out of 18 $\mathbb{F}_p$ coefficients 3 continuous $\mathbb{F}_p$ coefficients are non-zero and the others are zero. By utilizing such representation along with the sextic twisted isomorphic sub-field property of $\mathbb{F}_{p^{18}}$, this paper has computed the elliptic curve doubling and elliptic curve addition in the Miller's algorithm as $\mathbb{F}_{p^3}$ arithmetic without any explicit mapping from $\mathbb{F}_{p^{18}}$ to $\mathbb{F}_{p^3}$.

Finally this paper proposes *pseudo 12-sparse multiplication* in affine coordinates for line evaluation in the Miller's algorithm by considering the fact that multiplying or dividing the result of Miller's loop calculation by an arbitrary non-zero $\mathbb{F}_p$ element does not change the result as the following final exponentiation cancels the effect of multiplication or division. Following the division by a non-zero $\mathbb{F}_p$ element, one of the 7 non-zero $\mathbb{F}_p$ coefficients (which is a combination of 1 $\mathbb{F}_p$ and 2 $\mathbb{F}_{p^3}$ coefficients) becomes 1 that yields calculation efficiency. The calculation overhead caused from the division is canceled by isomorphic mapping with a quadratic and cubic residue in $\mathbb{F}_p$. This paper doesn't end up by giving only the theoretic proposal of improvement of Optimal Ate pairing by pseudo 12-sparse multiplication. In order to evaluate the theoretic proposal, this paper shows some experimental results with recommended parameter settings.

5.2 Fundamentals

This section briefly reviews the fundamentals of KSS curve [16], towering extension field with irreducible binomials [2] , sextic twist, pairings and sparse multiplication [21].

5.2.1 KSS curve

Kachisa-Schaefer-Scott(KSS) curve[16] is a non supersingular pairing friendly elliptic curve of embedding degree 18. The equation of KSS curve defined over $\mathbb{F}_{p^{18}}$ is given as follows:

$$E : y^2 = x^3 + b, \quad b \in \mathbb{F}_p \tag{5.1}$$

together with the following parameter settings,

$$p(\chi) = (\chi^8+5\chi^7+7\chi^6+37\chi^5+188\chi^4+259\chi^3+343\chi^2+1763\chi+2401)/21, \quad (5.2\text{-a})$$
$$r(\chi) = (\chi^6+37\chi^3+343)/343, \quad (5.2\text{-b})$$
$$t(\chi) = (\chi^4+16\chi+7)/7, \quad (5.2\text{-c})$$

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

5.2.2 Towering extension field

In extension field arithmetic, higher level computations can be improved by towering. In towering, higher degree extension field is constructed as a polynomial of lower degree extension fields. Since KSS curve is defined over $\mathbb{F}_{p^{18}}$, this paper has represented extension field $\mathbb{F}_{p^{18}}$ as a tower of sub-fields to improve arithmetic operations. In some previous works, such as Bailey et al. [2] explained tower of extension by using irreducible binomials. In what follows, let $(p-1)$ be divisible by 3 and c is a certain quadratic and cubic non residue in $\mathbb{F}_p$. Then for KSS-curve [16], where $k = 18$, $\mathbb{F}_{p^{18}}$ is constructed as tower field with irreducible binomial as follows:

$$\begin{cases} \mathbb{F}_{p^3} & = \mathbb{F}_p[i]/(i^3 - c), \\ \mathbb{F}_{p^6} & = \mathbb{F}_{p^3}[v]/(v^2 - i), \\ \mathbb{F}_{p^{18}} & = \mathbb{F}_{p^6}[\theta]/(\theta^3 - v). \end{cases} \quad (5.3)$$

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

5.2.3 Sextic twist

Let z be a certain quadratic and cubic non residue $z \in \mathbb{F}_{p^3}$. The sextic twisted curve E' of KSS curve E defined in Eq.(5.1) and their isomorphic mapping ψ_6 are given as follows:

$$\begin{aligned} E' &: y^2 = x^3 + bz, \quad b \in \mathbb{F}_p \\ \psi_6 &: E'(\mathbb{F}_{p^3})[r] \longmapsto E(\mathbb{F}_{p^{18}})[r] \cap \mathrm{Ker}(\pi_p - [p]), \\ &\quad (x, y) \longmapsto (z^{-1/3}x, z^{-1/2}y) \end{aligned} \quad (5.4)$$

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

$$\pi_p : (x, y) \longmapsto (x^p, y^p). \quad (5.5)$$

The order of the sextic twisted isomorphic curve $\#E'(\mathbb{F}_{p^3})$ is also divisible by the order of KSS curve E defined over $\mathbb{F}_p$ denoted as r. Extension field arithmetic by utilizing the sextic twisted sub-field curve $E'(\mathbb{F}_{p^3})$ based on the isomorphic twist can improve pairing calculation. In this paper, $E'(\mathbb{F}_{p^3})[r]$ shown in Eq. (5.4) is denoted as $\mathbb{G}'_2$.

Isomorphic mapping between $\mathbf{E}(\mathbb{F}_p)$ and $\hat{E}(\mathbb{F}_p)$

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

$$\begin{aligned} \hat{E} \quad : \quad & y^2 = x^3 + b\hat{z}, \\ & \hat{E}(\mathbb{F}_p)[r] \longmapsto E(\mathbb{F}_p)[r], \\ & (x, y) \longmapsto (\hat{z}^{-1/3}x, \hat{z}^{-1/2}y), \\ & \text{where } \hat{z}, \hat{z}^{-1/2}, \hat{z}^{-1/3} \in \mathbb{F}_p. \end{aligned} \tag{5.6}$$

5.2.4 Pairings

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

Optimal Ate pairing

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

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

$$\alpha : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{F}'_{p^k}/(\mathbb{F}^*_{p^k})^r. \tag{5.7}$$

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

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

$$\alpha(Q, P) = f_{t-1,Q}(P)^{\frac{p^k-1}{r}}, \tag{5.8}$$

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

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

$$(Q, P) = (f_{\chi,Q} \cdot f^p_{3,Q} \cdot l_{[\chi]Q,[3p]Q})^{\frac{p^{18}-1}{r}}, \tag{5.9}$$

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

5.2.5 Sparse multiplication

In the previous work, Mori et al. [21] has substantiated the pseudo 8-sparse multiplication for BN curve. Adapting affine coordinates for representing rational points, we can apply Mori's work in the case of KSS curve. The doubling phase and addition phase in Miller's loop can be carried out efficiently by the following calculations. Let $P = (x_P, y_P)$, $T = (x, y)$ and $Q = (x_2, y_2) \in E'(\mathbb{F}_{p^3})$ be given in affine coordinates, and let $T + Q = (x_3, y_3)$ be the sum of T and Q.

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

$$\begin{aligned} A = \tfrac{1}{2y}, B = 3x^2, C = AB, D = 2x, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, F = C\overline{x}_P, \\ l_{T,T}(P) = y_P + Ev + F\theta = y_P + Ev - Cx_P\theta, \end{aligned} \tag{5.10}$$

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

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

$$\begin{aligned} A = \tfrac{1}{x_2 - x}, B = y_2 - y, C = AB, D = x + x_2, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, F = C\overline{x}_P, \\ l_{T,Q}(P) = y_P + Ev + F\theta = y_P + Ev - Cx_P\theta, \end{aligned} \tag{5.11}$$

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

Analyzing Eq.(5.10) and Eq.(5.11), we get that E and Cx_P are calculated in $\mathbb{F}_{p^3}$. After that, the basis element 1, v and θ identifies the position of y_P, E and Cx_P in $\mathbb{F}_{p^{18}}$ vector representation. Therefore vector representation of $l_{\psi_6(T),\psi_6(T)}(P) \in \mathbb{F}_{p^{18}}$ consists of 18 coefficients. Among them at least 11 coefficients are equal to zero. In the other words, only 7 coefficients $y_P \in \mathbb{F}_p$, $Cx_P \in \mathbb{F}_{p^3}$ and $E \in \mathbb{F}_{p^3}$ are perhaps to be non-zero. $l_{\psi_6(T),\psi_6(Q)}(P) \in \mathbb{F}_{p^{18}}$ also has the same vector structure. Thus, the calculation of multiplying $l_{\psi_6(T),\psi_6(T)}(P) \in \mathbb{F}_{p^{18}}$ or $l_{\psi_6(T),\psi_6(Q)}(P) \in \mathbb{F}_{p^{18}}$ is called sparse multiplication. In the above mentioned instance especially called 11-sparse multiplication. This sparse multiplication accelerates Miller's loop calculation as shown in Alg. 3. This paper comes up with pseudo 12-sparse multiplication.

5.3 Improved Optimal Ate Pairing for KSS curve

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

1. In Eq.(5.10) and Eq.(5.11) among the 7 non-zero coefficients, one of the non-zero coefficients is $y_P \in \mathbb{F}_p$. And y_P remains uniform through Miller's loop calculation. Thereby dividing both sides of those Eq.(5.10) and Eq.(5.11) by y_P, the coefficient becomes 1 which results in a more efficient sparse multiplication by $l_{\psi_6(T),\psi_6(T)}(P)$ or $l_{\psi_6(T),\psi_6(Q)}(P)$. This paper calls it *pseudo 12-sparse multiplication.*

Algorithm 3: Optimal Ate pairing on KSS curve

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

2. Division by y_P in Eq.(5.10) and Eq.(5.11) causes a calculation overhead for the other non-zero coefficients in the Miller's loop. To cancel this additional cost in Miller's loop, the map introduced in Eq.(5.6) is applied.

It is to be noted that this paper doesn't focus on making final exponentiation efficient in Miller's algorithm since many efficient algorithms are available. From Eq.(5.10) and Eq.(5.11) the above mentioned ideas are introduced in details.

5.3.1 Pseudo 12-sparse multiplication

As said before y_P shown in Eq.(5.10) is a non-zero elements in $\mathbb{F}_p$. Thereby, dividing both sides of Eq.(5.10) by y_P we obtain as follows:

$$y_P^{-1} l_{T,T}(P) = 1 + E y_P^{-1} v - C(x_P y_P^{-1})\theta. \tag{5.12}$$

Replacing $l_{T,T}(P)$ by the above $y_P^{-1} l_{T,T}(P)$, the calculation result of the pairing does not change, since *final exponentiation* cancels $y_P^{-1} \in \mathbb{F}_p$. One of the non-zero coefficients becomes 1 after the division by y_P, which results in more efficient vector multiplications in Miller's loop. This paper calls it *pseudo* $12-$*sparse multiplication*. Alg. 4 introduces the detailed calculation procedure of pseudo 12-sparse multiplication.

5.3.2 Line calculation in Miller's loop

The comparison of Eq.(5.10) and Eq.(5.12) shows that the calculation cost of Eq.(5.12) is little bit higher than Eq.(5.10) for $E y_P^{-1}$. The cancellation process of $x_P y_P^{-1}$ terms by utilizing isomorphic mapping is introduced next. The $x_P y_P^{-1}$ and y_P^{-1} terms are pre-computed to reduce execution time complexity. The map introduced in Eq.(5.6) can find a certain isomorphic rational point $\hat{P}(x_{\hat{P}}, y_{\hat{P}}) \in \hat{E}(\mathbb{F}_p)$ such that

$$x_{\hat{P}} y_{\hat{P}}^{-1} = 1. \tag{5.13}$$

Here the twist parameter z of Eq.(5.4) is considered to be $\hat{z} = (x_P y_P^{-1})^6$ of Eq.(5.6), where $\hat{z}$ is a quadratic and cubic residue in $\mathbb{F}_p$ and $\hat{E}$ denotes the KSS curve defined by Eq.(5.6). From the isomorphic mapping Eq.(5.4), such z is obtained by solving the following equation considering the input $P(x_P, y_P)$.

$$z^{1/3} x_P = z^{1/2} y_P, \tag{5.14}$$

Algorithm 4: Pseudo 12-sparse multiplication

Input: $a, b \in \mathbb{F}_{p^{18}}$
$a = (a_0 + a_1\theta + a_2\theta^2) + (a_3 + a_4\theta + a_5\theta^2)v,\ b = 1 + b_1\theta + b_3 v$
where $a_i, b_j, c_i \in \mathbb{F}_{p^3} (i = 0, \cdots, 5, j = 1, 3)$
Output: $c = ab = (c_0 + c_1\theta + c_2\theta^2) + (c_3 + c_4\theta + c_5\theta^2)v \in \mathbb{F}_{p^{18}}$

$c_1 \leftarrow a_0 \times b_1, c_5 \leftarrow a_2 \times b_3, t_0 \leftarrow a_0 + a_2, S_0 \leftarrow b_1 + b_3$
$c_3 \leftarrow t_0 \times S_0 - (c_1 + c_5)$
$c_2 \leftarrow a_1 \times b_1, c_6 \leftarrow a_3 \times b_3, t_0 \leftarrow a_1 + a_3$
$c_4 \leftarrow t_0 \times S_0 - (c_2 + c_6)$
$c_5 \leftarrow c_5 + a_4 \times b_1, c_6 \leftarrow c_6 + a_5 \times b_1$
$c_7 \leftarrow a_4 \times b_3, c_8 \leftarrow a_5 \times b_3$
$c_0 \leftarrow c_6 \times i$
$c_1 \leftarrow c_1 + c_7 \times i$
$c_2 \leftarrow c_2 + c_8 \times i$
$c \leftarrow c + a$
return $c = (c_0 + c_1\theta + c_2\theta^2) + (c_3 + c_4\theta + c_5\theta^2)v$

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

$$\hat{P}(x_{\hat{P}}, y_{\hat{P}}) = (x_P^3 y_P^{-2}, x_P^3 y_P^{-2}). \tag{5.15}$$

As the x and y coordinates of $\hat{P}$ are the same, $x_{\hat{P}} y_{\hat{P}}^{-1} = 1$. Therefore, corresponding to the map introduced in Eq.(5.6), first mapping not only P to $\hat{P}$ shown above but also Q to $\hat{Q}$ shown below.

$$\hat{Q}(x_{\hat{Q}}, y_{\hat{Q}}) = (x_P^2 y_P^{-2} x_Q, x_P^3 y_P^{-3} y_Q). \tag{5.16}$$

When we define a new variable $L = (x_P^{-3} y_P^2) = y_{\hat{P}}^{-1}$, the line evaluations, Eq.(5.10) and Eq.(5.11) become the following calculations. In what follows, let $\hat{P} = (x_{\hat{P}}, y_{\hat{P}}) \in E(\mathbb{F}_p)$, $T = (x, y)$ and $Q = (x_2, y_2) \in E'(\mathbb{F}_{p^3})$ be given in affine coordinates and let $T + Q = (x_3, y_3)$ be the sum of T and Q.

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

$$\begin{aligned} A = \tfrac{1}{2y}, B = 3x^2, C = AB, D = 2x, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, \\ \hat{l}_{T,T}(P) = y_P^{-1} l_{T,T}(P) = 1 + ELv - C\theta, \end{aligned} \tag{5.17}$$

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

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

$$\begin{aligned} A = \tfrac{1}{x_2 - x}, B = y_2 - y, C = AB, D = x + x_2, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, \\ \hat{l}_{T,Q}(P) = y_P^{-1} l_{T,Q}(P) = 1 + ELv - C\theta, \end{aligned} \tag{5.18}$$

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

As we compare the above equation with to Eq.(5.10) and Eq.(5.11), the third term of the right-hand side becomes simple since $x_{\hat{P}} y_{\hat{P}}^{-1} = 1$.

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

5.4 Cost evaluation and experimental result

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

5.4.1 Parameter settings and computational environment

In the experimental simulation, this paper has considered the 192 bit security level for KSS curve. Table 5.1 shows the parameters settings suggested in [1] for 192 bit security over KSS curve. However this parameter settings does not necessarily comply with the recent suggestion of key size by Kim et al. [17] for 192 bit security level. The sole purpose to use this parameter settings in this paper is to compare the literature with the experimental result.

TABLE 5.1: Parameters

Security level	χ	$p(\chi)$ [bit]	c Eq.(5.3)	b Eq.(5.1)
192-bit	$-2^{64} - 2^{51} + 2^{46} + 2^{12}$	508	2	2

To evaluate the operational cost and to compare the execution time of the proposal based on the recommended parameter settings, the following computational environment is considered. Table 5.2 shows the computational environment.

TABLE 5.2: Computing environment

CPU	Core i5 6600
Memory	8.00GB
OS	Ubuntu 16.04 LTS
Library	GMP 6.1.0 [13]
Compiler	gcc 5.4.0
Programming language	C

5.4.2 Cost evaluation

Let us consider m, s, a and i to denote the times of multiplication, squaring, addition and inversion $\in \mathbb{F}_p$. Similarly, $\tilde{m}, \tilde{s}, \tilde{a}$ and $\tilde{i}$ denote the number of multiplication, squaring, addition and inversion $\in \mathbb{F}_{p^3}$ and $\hat{m}, \hat{s}, \hat{a}$ and $\hat{i}$ to denote the count of multiplication, squaring, addition and inversion $\in \mathbb{F}_{p^{18}}$ respectively. Table 5.3 and Table 5.4 show the calculation costs with respect to operation count.

Table 5.3: Operation count of line evaluation

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

Table 5.4: Operation count of multiplication

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

By analyzing the Table 5.4 we can find that 11-sparse multiplication requires 18 more multiplication in $\mathbb{F}_p$ than pseudo 12-sparse multiplication.

5.4.3 Experimental result

Table 5.5 shows the calculation times of Optimal Ate pairing respectively. In this execution time count, the time required for final exponentiation is excluded. The results (time count) are the averages of 10000 iterations on PC respectively. According to the experimental results, pseudo 12-sparse contributes to a few percent acceleration of 11-sparse.

Table 5.5: Calculation time of Optimal Ate pairing at the 192-bit security level

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

5.5 Conclusion and future works

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

Acknowledgment

This work is partially supported by the Strategic Information and Communications R&D Promotion Programme (SCOPE) of Ministry of Internal Affairs and Communications, Japan.

Appendix A

Frequently Asked Questions

A.1 How do I change the colors of links?

The color of links can be changed to your liking using:

`\hypersetup{urlcolor=red}`, or

`\hypersetup{citecolor=green}`, or

`\hypersetup{allcolor=blue}`.

If you want to completely hide the links, you can use:

`\hypersetup{allcolors=.}`, or even better:

`\hypersetup{hidelinks}`.

If you want to have obvious links in the PDF but not the printed text, use:

`\hypersetup{colorlinks=false}`.

Bibliography

[1] Diego F. Aranha et al. “Implementing Pairings at the 192-Bit Security Level”. In: *PAIRING 2012*. Ed. by Michel Abdalla and Tanja Lange. Vol. 7708. LNCS. Springer, Heidelberg, May 2013, pp. 177–195. DOI: 10.1007/978-3-642-36334-4_11.

[2] Daniel V. Bailey and Christof Paar. “Efficient Arithmetic in Finite Field Extensions with Application in Elliptic Curve Cryptography”. In: *Journal of Cryptology* 14.3 (June 2001), pp. 153–176. DOI: 10.1007/s001450010012.

[3] Daniel V Bailey and Christof Paar. “Optimal extension fields for fast arithmetic in public-key algorithms”. In: *Advances in Cryptology—CRYPTO'98*. Springer. 1998, pp. 472–485.

[4] Paulo S. L. M. Barreto and Michael Naehrig. “Pairing-Friendly Elliptic Curves of Prime Order”. In: *SAC 2005*. Ed. by Bart Preneel and Stafford Tavares. Vol. 3897. LNCS. Springer, Heidelberg, Aug. 2006, pp. 319–331. DOI: 10.1007/11693383_22.

[5] Paulo SLM Barreto, Ben Lynn, and Michael Scott. “Constructing elliptic curves with prescribed embedding degrees”. In: *Security in Communication Networks*. Springer, 2002, pp. 257–267.

[6] Paulo SLM Barreto and Michael Naehrig. “Pairing-friendly elliptic curves of prime order”. In: *International Workshop on Selected Areas in Cryptography, SAC 2005*. Springer. 2005, pp. 319–331.

[7] Paulo SLM Barreto et al. “Efficient algorithms for pairing-based cryptosystems”. In: *Advances in cryptology—CRYPTO 2002*. Springer, 2002, pp. 354–369.

[8] Naomi Benger and Michael Scott. “Constructing tower extensions of finite fields for implementation of pairing-based cryptography”. In: *Arithmetic of finite fields*. Springer, 2010, pp. 180–195.

[9] Dan Boneh, Xavier Boyen, and Hovav Shacham. “Short group signatures”. In: *Advances in Cryptology–CRYPTO 2004*. Springer. 2004, pp. 41–55.

[10] Dan Boneh, Craig Gentry, and Brent Waters. “Collusion resistant broadcast encryption with short ciphertexts and private keys”. In: *Advances in Cryptology–CRYPTO 2005*. Springer. 2005, pp. 258–275.

[11] Henri Cohen et al. *Handbook of elliptic and hyperelliptic curve cryptography*. CRC press, 2005.

[12] David Freeman, Michael Scott, and Edlyn Teske. “A taxonomy of pairing-friendly elliptic curves”. In: *Journal of cryptology* 23.2 (2010), pp. 224–280.

[13] Torbjörn Granlund and the GMP development team. *GNU MP: The GNU Multiple Precision Arithmetic Library*. 6.1.0. http://gmplib.org. 2015.

[14] Tsutomu Iijima et al. “Construction of Frobenius maps of twists elliptic curves and its application to elliptic scalar multiplication”. In: *Proc. of SCIS*. 2002, pp. 699–702.

[15] Antoine Joux. “A one round protocol for tripartite Diffie–Hellman”. In: *International Algorithmic Number Theory Symposium*. Springer. 2000, pp. 385–393.

[16] Ezekiel Kachisa, Edward Schaefer, and Michael Scott. “Constructing Brezing-Weng Pairing-Friendly Elliptic Curves Using Elements in the Cyclotomic Field”. In: *Pairing-Based Cryptography–Pairing 2008* (2008), pp. 126–135.

[17] Taechan Kim and Razvan Barbulescu. “Extended tower number field sieve: A new complexity for the medium prime case”. In: *Advances in Cryptology - CRYPTO 2016 - Proceedings, Part I*. Springer. 2016, pp. 543–571.

[18] Paul C Kocher. “Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems”. In: *Annual International Cryptology Conference*. Springer. 1996, pp. 104–113.

[19] Eunjeong Lee, Hyang-Sook Lee, and Cheol-Min Park. “Efficient and generalized pairing computation on abelian varieties”. In: *IEEE Transactions on Information Theory* 55.4 (2009), pp. 1793–1803.

[20] Seiichi Matsuda et al. “Optimised versions of the ate and twisted ate pairings”. In: *Cryptography and Coding*. Springer, 2007, pp. 302–312.

[21] Yuki Mori et al. “Pseudo 8–Sparse Multiplication for Efficient Ate–Based Pairing on Barreto–Naehrig Curve”. In: *Pairing-Based Cryptography–Pairing 2013*. Springer, 2013, pp. 186–198.

[22] Toru Nakanishi and Nobuo Funabiki. “Verifier-local revocation group signature schemes with backward unlinkability from bilinear maps”. In: *Advances in Cryptology-ASIACRYPT 2005*. Springer, 2005, pp. 533–548.

[23] Yasuyuki Nogami et al. “Integer variable χ–based ate pairing”. In: *International Conference on Pairing-Based Cryptography*. Springer. 2008, pp. 178–191.

[24] Yumi Sakemi et al. “Skew frobenius map and efficient scalar multiplication for pairing–based cryptography”. In: *International Conference on Cryptology and Network Security*. Springer. 2008, pp. 226–239.

[25] Michael Scott. “On the efficient implementation of pairing-based protocols”. In: *Cryptography and Coding*. Springer, 2011, pp. 296–308.

[26] Joseph H Silverman, Gary Cornell, and M Artin. *Arithmetic geometry*. Springer, 1986.

[27] Frederik Vercauteren. “Optimal pairings”. In: *Information Theory, IEEE Transactions on* 56.1 (2010), pp. 455–461.

[28] Lawrence C Washington. *Elliptic curves: number theory and cryptography*. CRC press, 2008.

Biography

Md. Al-Amin Khandaker was born on September 11, 1990, in a beautiful village of Bangladesh. He completed his high school in 2007 and in 2008, admitted to Jahangirnagar University, Bangladesh. In 2012, he graduated majoring in Computer Science and Engineering. After that, he joined in a Holland-based off-shore software development company in Dhaka. In 2015 he awarded Japan Govt. Scholarship (MEXT) to pursue Doctor's course in the field of cryptography in Okayama University under the supervision of Professor Yasuyuki NOGAMI. His main fields of research are optimization and efficient implementation techniques for the elliptic curve, pairing-based cryptography and it's application for IoT security. He is a graduate student member of IEEE.