Efficient Software Implementation of Pairing-Based Cryptographic Primitives for High-level Security for IoT

March, 2019

Md. Al-Amin KHANDAKER

Graduate School of
Natural Science and Technology
(Doctor's Course)

OKAYAMA UNIVERSITY

DOCTORAL THESIS

Efficient Software Implementation of Pairing-Based Cryptographic Primitives for High-level Security for IoT

Author:
Md. Al-Amin KHANDAKER

Supervisor:
Yasuyuki NOGAMI

Co-supervisors:
Nobuo FUNABIKI
Satoshi DENNO

A dissertation submitted to
OKAYAMA UNIVERSITY
in fulfillment of the requirements for the degree of
Doctor of Philosophy in Engineering
in the
Faculty of Engineering
Graduate School of Natural Science and Technology

December 9, 2018

To Whom It May Concern

We hereby certify that this is a typical copy of the original Doctoral dissertation of

Md. Al-Amin Khandaker

Thesis Title:

Efficient Software Implementation of Pairing-Based Cryptographic Primitives for High-level Security for IoT

Seal of Supervisor *Official Seal*

Professor Yasuyuki Nogami

Graduate School of Natural Science and Technology

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, "Efficient Software Implementation of Pairing-Based Cryptographic Primitives for High-level Security for IoT" 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 at Okayama University as a candidate for the degree of Doctor of Philosophy in Engineering.
- This work has not been submitted for a degree or any other qualification at this University or any other institution.
- Some of the previously published works presented in this dissertation listed in "Research Activities".
- The published work of others cited in this thesis is clearly attributed. Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help to pursue this work.
- My coauthors contribution is acknowledged in all works.
- The experiments and results presented in this thesis and in the articles where I am the first author were conducted by the myself.

Signed: Md. Al-Amin KHANDAKER Student number: 51427351

Date: December 9, 2018

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

Albert Einstein

Abstract

Md. Al-Amin KHANDAKER

Efficient Software Implementation of Pairing-Based Cryptographic Primitives for High-level Security for IoT

Pairing-based cryptography over the elliptic curves is a relative new paradigm in public key cryptography(PKC). In general, pairing calculation involves certain elliptic curve named pairing-friendly curve defined over finite extension of prime field. It is typically defined as bilinear map from rational points of two additive groups to a multiplicative group. Two mathematical tool named as Miller's algorithm and final exponentiation is mostly involved in pairing calculation. However, most protocols also requires two more operation in pairing groups named scalar multiplication and exponentiation in multiplicative group. The above mentioned mathematical tools are the major bottleneck for the efficiency of pairing-based protocols.

Since, the inception at the advent of this century pairing-based cryptography brings monumental amount of research. The results of this vast amount of research brought some novel cryptographic application which was not possible before pairing-based cryptography. However, computation speed of pairing was very slow to consider them as a practical option. Years of research from the mathematicians, cryptographers and computer scientists improves the efficiency of pairing.

The security of pairing-based cryptography is not only rely on the intractability of elliptic curve discrete logarithm problem (ECDLP) of additive elliptic curve group but also discrete logarithm problem (DLP) on multiplicative group. It is known that key size in cryptography based of ECDLP requires fewer bits than cryptography based on DLP. Therefore, it is a crucial to maintain a balance in parameter sizes for both additive and multiplicative groups in pairing-based cryptography. In CRYPTO 2016, Kim and Barbulescu showed a more efficient version of number field sieve algorithm to solve DLP. This new attack makes all previous parameter settings to update.

This thesis presents several improvement technics for pairing-based cryptography over two ordinary pairing-friendly curves named KSS-16 and KSS-18. The motivation behind to work on these curves is, they not widely studied in literature compared to other pairing-friendly curves. After the extNFS algorithm, the security level of widely used pairing-friendly curves were challenged. The technics can also be applied on the ordinary pairing-friendly

curves. We also present several improvements in extension field arithmetic operation. We implement the proposed improvements in for experimental purpose. All the sources are bundled in an installable library.

Acknowledgements

The last 3 and a half year was one of the best time of my life that I will cherish forever. I'm immensely blessed throughout this period for which I have many people to thank. I'm grateful to many people who have directly and indirectly helped me finish this work.

This work would not be possible without the unceasing supervision, innumerable counselling 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. His presence and off-work discussion make the lab more than a workplace.

I'm also very grateful for to my doctoral course co-supervisors Professor Nobuo Funabiki (*Distributed Systems Design Lab.*) and Professor Satoshi Denno (*Multimedia Radio Systems Lab.*) for having their time to read my thesis draft. Their insightful comments and helpful advice helped to shape the thesis into this state. I must recall my experience of taking the "Theory of Distributed Algorithm" course taught by Professor Nobuo Funabiki. His strong passion for algorithmic problem solving during the lectures was not only inspiring but also contagious.

I reminisce my encounters with Professor Satoshi Denno during my days at *Secure Wireless System lab*. He provided me with the deep-seated idea of the research works and Japan life. His questions and suggestions for the time of half yearly progress meetings were very intuitive.

I am very grateful to Associate Professor Nobumoto Yamane (*Information Transmission Lab.*) for provided important comments at progress meetings.

I would like to express my gratitude to Senior Assistant Professor Takuya Kusaka (*Information Security Lab.*) for the in-depth discussion of scientific topics. His strong work ethic and passion for research helped us to publish some of the remarkable collaborative works. He was always there to help while any difficulty arose from attending a conference to publishing a paper.

I express my gratitude to Senior Assistant Professor Hiroto Kagotani of (*Information System Design Lab.*) for employing me as a research assistant for

a quarter. Since the Information System Design Lab and Information Security Lab. share space, we had encountered more often and share of research discussions. His comments during the progress report were enlightening.

I am also grateful to Assistant Professor Kengo Iokibe (*Optical and Electromagnetic Waves Lab.*) for the collaborative work we had on side-channel analysis of raspberry pi.

I would like to express my deep gratitude of Professor Sylvain Duquesne of Univ Rennes, France for having me at IRMAR as a short-term researcher and allowing me to present my work in front of some brightest audiences. Professor Duquesne's in-depth reviews on my works were not only helpful towards to final acceptability but also intriguing.

My sincere gratitude to post-doctoral fellow Dr. Loubna Ghammam at Normandie University, France for her persistent guidance. Our collaboration with Professor Duquesne and Dr. Loubna helps me to work on the diverse area of mathematical aspects of cryptography.

I am also thankful to Professor Howon Kim of Pusan National University, South Korea and his Ph.D. student Taehwan Park for a great research collaboration on IoT security.

My gratitude to one of the great IoT security expert Professor Hwajeong Seo of Hansung University, South Korea for being a co-author in my first major conference paper.

Thanks to MEXT, Japan for the scholarship which fulfilled my dream to pursue the doctoral study in Japan. I sincerely acknowledge all the funds that afforded me to join several international conferences and conduct research activities.

I am also grateful to all administrative officer of the Faculty of Engineering who directly or indirectly made an impact in my doctoral course studies. My special thanks to Ms. Yumiko Kurooka for her kind support in administrative works.

Special thanks also to my seniors, juniors, and friends in the laboratory for creating a great work atmosphere and their generous support. Thanks to pairing team members of my lab who are one of brightest minds I've worked with.

I can not thank enough to my wife for her sacrifices and generous supports to my bread and butter. I would like to take the opportunity to appreciate my parents Ms. Nasima Akter and Mr. Md. Ali-Azzam Khandaker for their understanding, and encouragements.

So far so general we all are standing on the shoulders of the giants for our works. My profound gratitude to all great cryptographer, cryptographic engineers and researchers whose works keep inspiring students like me. I'm indebted to all my research collaborator, co-authors and reviewers for making my doctoral voyage engaging.

Contents

List of Figures

List of Tables

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 the people I owe most. To my parents who brought me to this world and to my wife who sacrificed the most during my Ph.D. journey.

Research Activities

Peer-Reviewed Journal Papers (First author)

1. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "An Improvement of Scalar Multiplication by Skew Frobenius Map with Multi-Scalar Multiplication for KSS Curve". In: *IEICE Transactions* 100-A.9 (2017), pp. 1838-1845. DOI: 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". In: *J. Inform. and Commun. Convergence Engineering* 15.2 (2017), pp. 97-103. DOI: 10.6109/jicce.2017.15.2.97.

Peer-Reviewed International Conference Papers (First author)

LNCS Proceedings:

3. **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: *INDOCRYPT 2017*. Ed. by Arpita Patra and Nigel P. Smart. Vol. 10698. LNCS. Springer, Heidelberg, Dec. 2017, pp. 186–205. DOI: 10.1007/978-3-319-71667-1_10.

4. **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: *ICISC 2016*. Ed. by Seokhie Hong and Jong Hwan Park. Vol. 10157. LNCS. Springer, Heidelberg, 2017, pp. 208–219. DOI: 10.1007/978-3-319-53177-9_11.

5. **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: *WISA 2016*. Ed. by Dooho Choi and Sylvain Guilley. Vol. 10144. LNCS. Springer, Heidelberg, Aug. 2016, pp. 221–232. DOI: 10.1007/978-3-319-56549-1_19.

IEEE Xplore indexed:

6. **Md. Al-Amin Khandaker**, Yuki Nanjo, Takuya Kusaka, and Yasuyuki Nogami. "A Comparative Implementation of GLV Technique on KSS-16 Curve." In: *Sixth International Symposium on Computing and Networking, CANDAR 2018*, Gifu, Japan, November 27-30, 2016. 2018, pp. ?–?. DOI: ?. (Acceptance Ratio 28/77 ≈ 36%)

7. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "Isomorphic Mapping for Ate-Based Pairing over KSS Curve of Embedding Degree 18". In: *Fourth International Symposium on Computing and Networking, CANDAR 2016*, Hiroshima, Japan, November 22-25, 2016. 2016, pp. 629–634. DOI: 10. 1109/CANDAR.2016.0113.

8. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "A consideration of towering scheme for efficient arithmetic operation over extension field of degree 18". In: *19th International Conference on Computer and Information Technology (ICCIT) 2016*. Dec. 2016, pp. 276–281. DOI: 10.1109/ICCITECHN.2016. 7860209.: .

9. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "An improvement of scalar multiplication on elliptic curve defined over extension field Fq2". In: *IEEE International Conference on Consumer Electronics-Taiwan (ICCE- TW). 2016*, Nantou, Taiwan, May 27-29, 2016. 2016, pp. 1–2. DOI: 10.1109/ICCE-TW.2016.7520894.

IEICE/IEIE sponsored:

10. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "Frobenius Map and Skew Frobenius Map for Ate-based Pairing over KSS Curve of Embedding Degree 16 ". In: *International Technical Conference on Circuits / Systems, Computers and Communications (ITC-CSCC), 2017*, Busan, Korea, Jul. 2-5, 2017. IEIE.

Peer-Reviewed Journal Papers (Co-author)

11. Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka, and Yasuyuki Nogami. "Efficient Pairing-Based Cryptography on Raspberry Pi". In: *Journal of Communications (JCM)* 13.2 (2018), pp. 88–93. DOI: 10.12720/jcm.13.2.88-93.

12. Yuta Hashimoto, **Md. Al-Amin Khandaker**, Yuta Kodera, Taehwan Park, Takuya Kusaka, Howon Kim, and Yasuyuki Nogami. "An Implementation of ECC with Twisted Montgomery Curve over 32nd Degree Tower Field on Arduino Uno". In: *International Journal of Networking and Computing (IJNC)* 8.2 (2018), pp. 341–350. DOI: 10.15803/ijnc.8.2_341.

13. Yuta Kodera, Takeru Miyazaki, **Md. Al-Amin Khandaker**, Ali Md. Arshad, Takuya Kusaka, Yasuyuki Nogami, and Satoshi Uehara. "Distribution of Digit Patterns in Multi-Value Sequence over the Odd Characteristic Field". In: *IEICE Transactions* 101-A.9 (2018), pp. 1525–1536. DOI: 10.1587/transfun.E101.A.1525.

14. Shunsuke Ueda, Ken Ikuta, Takuya Kusaka, **Md. Al-Amin Khandaker**, Ali Md. Arshad, and Yasuyuki Nogami. "An Extended Generalized Minimum Distance Decoding for Binary Linear Codes on a 4-Level Quantization over an AWGN Channel". In: *IEICE Transactions* 101-A.8 (2018), pp. 1235–1244. DOI: 10.1587/transfun.E101.A.1235.

15. Shoma Kajitani, Yasuyuki Nogami, Shunsuke Miyoshi, Thomas Austin, **Md. Al-Amin Khandaker**, Nasima Begum, and Sylvain Duquesne. "Web-based Volunteer Computing for Solving the Elliptic Curve Discrete Logarithm Problem". In: *International Journal of Networking and Computing (IJNC)* 6.2 (2016), pp. 181–194. DOI: 10.15803/ijnc.6.2_181.

Peer-Reviewed International Conference Papers (Co-author)

LNCS Proceedings:

16. Yuki Nanjo, **Md. Al-Amin Khandaker**, Masaaki Shirase, Takuya Kusaka, and Yasuyuki Nogami. "Efficient Ate-Based Pairing over the Attractive Classes of BN Curves". In: *WISA 2018*. To appear LNCS. Springer, Heidelberg, Aug. 2018. pp. ?–?. DOI: ?. (Acceptance Ratio 22/44 = 50%)

17. 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: *ICISC 2017*. Ed. by Howon Kim and Dong-Chan Kim. Vol. 10779. LNCS. Springer, Heidelberg, Oct. 2017, pp. 231–244. DOI: 10.1007/978-3-319-78556-1_13.

18. Taehwan Park, Hwajeong Seo, Garam Lee, **Md. Al-Amin Khandaker**, Yasuyuki Nogami, and Howon Kim. "Parallel Implementations of SIMON and SPECK, Revisited". In: *WISA 2017*. Ed. by Brent ByungHoon Kang and Taesoo Kim. Vol. 10763. LNCS. Springer, Heidelberg, Aug. 2017, pp. 283–294. DOI: 10.1007/978-3-319-93563-8_24.

IEEE Xplore indexed:

19. Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka, and Yasuyuki Nogami. "Consideration of Efficient Pairing Applying Two Construction Methods of Extension Fields." In: *Sixth International Symposium*

on Computing and Networking, CANDAR 2018, Gifu, Japan, November 27-30, 2016. 2018, pp. ?–?. DOI: ?.

20. 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". In: *Fifth International Symposium on Computing and Networking, CANDAR 2017*, Aomori, Japan, November 19-22, 2017. 2017, pp. 445–450. DOI: 10.1109/CANDAR.2017.90.

21. 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". In: *Fifth International Symposium on Computing and Networking, CANDAR 2017*, Aomori, Japan, November 19-22, 2017. 2017, pp. 451–455. DOI: 10.1109/CANDAR.2017.86.

22. Taehwan Park, Hwajeong Seo, **Md. Al-Amin Khandaker**, Yasuvuki Nogami, and Howon Kim. "Efficient Parallel Simeck Encryption with GPGPU and OpenCL". In: *IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). 2018*, Taichung, Taiwan, May 19-21, 2018. 2018, pp. 1–2. DOI: 10.1109/ICCE-China.2018.8448768.

23. 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". In: *IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). 2017*, Taipei, Taiwan, June 12-14, 2017. 2017, pp. 137-138. DOI: 10.1109/ICCE-China.2017.7991033.

24. Akihiro Sanada, Yasuyuki Nogami, Kengo Iokibe, **Md. Al-Amin Khandaker**. "Security analysis of Raspberry Pi against Side-channel attack with RSA cryptography."In: *IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW). 2017*, Taipei, Taiwan, June 12-14, 2017. 2017, pp. 287 - 288. DOI: 10.1109/ICCE-China.2017.7991108.

IEICE/IEIE sponsored:

25. 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". In: *International Symposium on Information Theory and its Applications (ISITA), 2018*. IEICE. (To appear in IEEE Xplore).

26. 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". In: *International Symposium on Information Theory and its Applications (ISITA), 2018*. IEICE. (To appear in IEEE Xplore).

27. 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". In: *32nd International Technical Conference on Circuits / Systems, Computers and Communications (ITC-CSCC), 2017*. IEIE.

Domestic conferences (First author)

28. **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". In: *Computer Security Symposium (CSS), 2017*, CD-ROM (3E1-4).

29. **Md. Al-Amin Khandaker** and Yasuyuki Nogami. "Efficient Scalar Multiplication by Skew Frobenius Map with Multi-Scalar Multiplication for KSS Curve". In: *Symposium on Cryptography and Information Security (SCIS), 2017*, CD-ROM (B1-3).

Domestic conferences (Co-author)

30. 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". In: *Computer Security Symposium (CSS), 2018*, CD-ROM (??).

31. 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". In: *Symposium on Cryptography and Information Security (SCIS), 2018*, CD-ROM (4D2-1).

32. 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". In: *Symposium on Cryptography and Information Security (SCIS), 2018*, CD-ROM (4D2-3).

33. 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". In: *Computer Security Symposium (CSS), 2017*, CD-ROM (3E1-3).

34. Norito Jitsui, Yuki Nanjo, **Md. Al-Amin Khandaker**, Takuya Kusaka and Yasuyuki Nogami. "Efficient Elliptic Scalar Multiplication for Pairing-Based Cryptography over BLS48". In: *Symposium on Cryptography and Information Security (SCIS), 2018*, CD-ROM (3B4-1).

Chapter 1

Improved Optimal-Ate Pairing for KSS-18 Curve

1.1 Introduction

1.1.1 Background and Motivation

From the very beginning of the cryptosystems that utilizes elliptic curve pairing; proposed independently by Sakai et al. [SK03] and Joux [Jou04], 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 [BF01] and group signature authentication by Nakanishi et al. [NF05] have come into the focus. In such outcome, Ate-based pairings such as Ate [Coh+05], Optimal-ate [Ver10], twisted Ate [Mat+07], R-ate [LLP09], and u-Ate [Nog+08] 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.

1.1.2 General Notation

As aforementioned, pairing is a bilinear map from two rational point groups $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group $\mathbb{G}_3$ [SCA86]. Bilinear pairing operation consist of two predominant parts, named as Miller's algorithm and final exponentiation. In the case of Ate-based pairing using KSS-18 pairing-friendly elliptic curve of embedding degree $k = 18$, the bilinear map is denoted by $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$, The groups $\mathbb{G}_1 \subset E(\mathbb{F}_p)$, $\mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ and $\mathbb{G}_3 \subset \mathbb{F}^*_{p^{18}}$ and p denotes the characteristic of $\mathbb{F}_p$. The elliptic curve E is defined over the extension field $\mathbb{F}_{p^{18}}$. The 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, continuously 3 of them are non-zero and the others are zero. By utilizing such representation along with the sextic twist and isomorphic mapping in subfield of $\mathbb{F}_{p^{18}}$, this chapter 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 $\mathbb{F}_{p^3}$.

1.1.3 Contribution Outline

This chapter 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 chapter does not end 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 chapter shows some experimental results with recommended parameter settings.

1.1.4 Related Works

Finding pairing friendly curves [FST06] 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 [BLS03; DEM05] and efficient extension field arithmetic [BP01]. Some previous work on optimizing the pairing algorithm on pairing friendly curve such Optimal-Ate pairing by Matsuda et al. [Mat+07] on Barreto-Naehrig (BN) curve [BN06] is already carried out. The previous work of Mori et al. [Mor+14] has showed the *pseudo 8-sparse multiplication* to efficiently calculate Miller's algorithm defined over BN curve. Apart from it, Aranha et al. [Ara+13] has improved Optimal-Ate pairing over KSS-18 curve for 192 bit security level by utilizing the relation $t(u) - 1 \equiv u + 3p(u) \bmod r(u)$ where $t(u)$ is the Frobenius trace of KSS-18 curve, u is an integer also known as *mother parameter*, $p(u)$ is the prime number and $r(u)$ is the order of the curve. This chapter has exclusively focused on efficiently calculating the Miller's loop of Optimal-Ate pairing defined over KSS-18 curve [KSS07] for 192-bit security level by applying *pseudo 12-sparse multiplication* technique along with other optimization approaches. The parameter settings recommended in [Ara+13] for 192 bit security on KSS-18 curve is used in the simulation implementation. But in the recent work, Kim et al. [KB16] has suggested to update the key sizes associated with pairing-based cryptography due to the development new algorithm to solve discrete logarithm problem over finite field. The parameter settings of [Ara+13] does not end up at the 192 bit security level according to [KB16]. However the parameter settings of [Ara+13] is primarily adapted in this chapter in order to show the resemblance of the proposal with the experimental result.

1.2 Fundamentals

This section briefly reviews the fundamentals of towering extension field with irreducible binomials [BP01], sextic twist, pairings and sparse multiplication [Mor+14] with respect to KSS-18 curve [KSS07].

1.2.1 KSS Curve

Kachisa-Schaefer-Scott (KSS) curve [KSS07] is a non supersingular pairing friendly elliptic curve of embedding degrees $k = \{16, 18, 32, 36, 40\}$. This chapter considers KSS curve of embedding degree $k = 18$, in short KSS-18 curve. The equation of KSS-18 curve defined over $\mathbb{F}_{p^{18}}$ is given as follows:

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

together with the following parameter settings,

$$p(u) = (u^8+5u^7+7u^6+37u^5+188u^4+259u^3+343u^2+1763u+2401)/21, \tag{1.2-a}$$
$$r(u) = (u^6+37u^3+343)/343, \tag{1.2-b}$$
$$t(u) = (u^4+16u+7)/7, \tag{1.2-c}$$

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 u, such that $u \equiv 14 \pmod{42}$.

1.2.2 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-18 curve is defined over $\mathbb{F}_{p^{18}}$, this chapter 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. [BP01] 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-18-curve [KSS07], where $k = 18$, $\mathbb{F}_{p^{18}}$ is constructed as tower field with irreducible binomial as follows:

$$\begin{cases} \mathbb{F}_{p^3} &= \mathbb{F}_p[i]/(i^3 - c), \\ \mathbb{F}_{p^6} &= \mathbb{F}_{p^3}[v]/(v^2 - i), \\ \mathbb{F}_{p^{18}} &= \mathbb{F}_{p^6}[\theta]/(\theta^3 - v). \end{cases} \tag{1.3}$$

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

1.2.3 Sextic Twist of KSS-18 Curve

Let z be a certain quadratic and cubic non residue in $\mathbb{F}_{p^3}$. The sextic twisted curve E' of KSS-18 curve E (Eq.(1.1)) and their isomorphic mapping ψ_6 are

given as follows:

$$\begin{aligned} E' &: y^2 = x^3 + bz, \quad b \in \mathbb{F}_p \\ \psi_6 &: E'(\mathbb{F}_{p^3})[r] \longmapsto E(\mathbb{F}_{p^{18}})[r] \cap \mathrm{Ker}(\pi_p - [p]), \\ &\quad (x, y) \longmapsto (z^{-1/3}x, z^{-1/2}y) \end{aligned} \tag{1.4}$$

where Ker(·) denotes the kernel of the mapping. Frobenius mapping π_p for rational point is given as

$$\pi_p : (x, y) \longmapsto (x^p, y^p). \tag{1.5}$$

The order of the sextic twisted isomorphic curve $\#E'(\mathbb{F}_{p^3})$ is also divisible by the order of KSS-18 curve E defined over $\mathbb{F}_p$ denoted as r. Extension field arithmetic by utilizing the sextic twisted subfield curve $E'(\mathbb{F}_{p^3})$ based on the isomorphic twist can improve pairing calculation. In this chapter, $E'(\mathbb{F}_{p^3})[r]$ shown in Eq. (1.4) is denoted as $\mathbb{G}_2'$.

1.2.4 Isomorphic Mapping between $E(\mathbb{F}_p)$ 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:

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

where

$$\hat{z}, \hat{z}^{-1/2}, \hat{z}^{-1/3} \in \mathbb{F}_p$$

.

1.2.5 Pairing over KSS-18 Curve

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-18 curve of embedding degree $k = 18$ is described as follows.

1.2.5.1 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:

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

$$\alpha : \mathbb{G}_2 \times \mathbb{G}_1 \longrightarrow \mathbb{F}'_{p^k}/(\mathbb{F}^*_{p^k})^r. \tag{1.6}$$

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

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

$$\alpha(Q, P) = f_{t-1,Q}(P)^{\frac{p^k-1}{r}}, \tag{1.7}$$

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 chapter. Several works [STO06; Sco+09] have been already done for efficient final exponentiation.

1.2.5.2 Optimal-Ate Pairing

The previous work of Aranha et al. [Ara+13] has mentioned about the relation $t(u) - 1 \equiv u + 3p(u) \bmod r(u)$ for Optimal-Ate pairing. Exploiting the relation, Optimal-Ate pairing on the KSS-18 curve is defined by the following representation.

$$(Q, P) = (f_{u,Q} \cdot f_{3,Q}^{p} \cdot l_{[u]Q,[3p]Q})^{\frac{p^{18}-1}{r}}, \tag{1.8}$$

where u is the mother parameter. The calculation procedure of Optimal-Ate pairing is shown in **Algorithm**. 1. In what follows, the calculation steps from 1 to 5 shown in **Algorithm**. 1 is identified as Miller's loop. 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 chapter.

1.2.6 Sparse multiplication

In the previous work, Mori et al. [Mor+14] 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-18 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.

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

$$\begin{aligned} A = \tfrac{1}{2y}, B = 3x^2, C = AB, D = 2x, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, F = C\overline{x}_P, \\ l_{T,T}(P) = y_P + Ev + F\theta = y_P + Ev - Cx_P\theta, \end{aligned} \tag{1.9}$$

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

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

$$\begin{aligned} A = \tfrac{1}{x_2 - x}, B = y_2 - y, C = AB, D = x + x_2, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, F = C\overline{x}_P, \\ l_{T,Q}(P) = y_P + Ev + F\theta = y_P + Ev - Cx_P\theta, \end{aligned} \tag{1.10}$$

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.(1.9) and Eq.(1.10), we get that E and Cx_P are calculated in $\mathbb{F}_{p^3}$. After that, the basis element 1, v and θ identifies the position of y_P, E and Cx_P in $\mathbb{F}_{p^{18}}$ vector representation. Therefore vector representation of $l_{\psi_6(T),\psi_6(T)}(P) \in \mathbb{F}_{p^{18}}$ consists of 18 coefficients. Among them at least 11 coefficients are equal to zero. In the other words, only 7 coefficients $y_P \in \mathbb{F}_p$, $Cx_P \in \mathbb{F}_{p^3}$ and $E \in \mathbb{F}_{p^3}$ are perhaps to be non-zero. $l_{\psi_6(T),\psi_6(Q)}(P) \in \mathbb{F}_{p^{18}}$ also has the same vector structure. Thus, the calculation of multiplying $l_{\psi_6(T),\psi_6(T)}(P) \in \mathbb{F}_{p^{18}}$ or $l_{\psi_6(T),\psi_6(Q)}(P) \in \mathbb{F}_{p^{18}}$ is called sparse multiplication. In the above mentioned instance especially called 11-sparse multiplication. This sparse multiplication accelerates Miller's loop calculation as shown in **Algorithm**.1. This chapter comes up with pseudo 12-sparse multiplication.

Algorithm 1: Optimal-Ate pairing on KSS-18 curve

Input: $u, P \in \mathbb{G}_1, Q \in \mathbb{G}'_2$
Output: (Q, P)

$f \leftarrow 1, T \leftarrow Q$
for $i = \lfloor \log_2(u) \rfloor$ **downto** 1 **do**
    $f \leftarrow f^2 \cdot l_{T,T}(P), T \leftarrow [2]T$
    if $u[i] = 1$ **then**
        $f \leftarrow f \cdot l_{T,Q}(P), T \leftarrow T + Q$
$f_1 \leftarrow f_{3,Q}^p, f \leftarrow f \cdot f_1$
$Q_1 \leftarrow [u]Q, Q_2 \leftarrow [3p]Q$
$f \leftarrow f \cdot l_{Q_1,Q_2}(P)$
$f \leftarrow f^{\frac{p^{18}-1}{r}}$
return f

1.3 Improved Optimal-Ate Pairing for KSS-18 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-18 curve. The following two ideas are proposed in order to efficiently apply 12-sparse multiplication on Optimal-Ate pairing on KSS-18 curve.

1. In Eq.(1.9) and Eq.(1.10) 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.(1.9) and Eq.(1.10) 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 chapter calls it *pseudo 12-sparse multiplication*.
2. Division by y_P in Eq.(1.9) and Eq.(1.10) 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.(1.2.4) is applied.

It is to be noted that this chapter doesn't focus on making final exponentiation efficient in Miller's algorithm since many efficient algorithms are available. From Eq.(1.9) and Eq.(1.10) the above mentioned ideas are introduced in details.

1.3.1 Pseudo 12-sparse Multiplication

As said before y_P shown in Eq.(1.9) is a non-zero elements in $\mathbb{F}_p$. Thereby, dividing both sides of Eq.(1.9) by y_P we obtain as follows:

$$y_P^{-1} l_{T,T}(P) = 1 + E y_P^{-1} v - C(x_P y_P^{-1})\theta. \tag{1.11}$$

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 chapter calls it $pseudo\ 12-sparse\ multiplication$. **Algorithm**. 2 introduces the detailed calculation procedure of pseudo 12-sparse multiplication.

Algorithm 2: Pseudo 12-sparse multiplication

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

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

1.3.2 Line Calculation in Miller's Loop

The comparison of Eq.(1.9) and Eq.(1.11) shows that the calculation cost of Eq.(1.11) is little bit higher than Eq.(1.9) for Ey_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.(1.2.4) can find a certain isomorphic rational point $\hat{P}(x_{\hat{P}}, y_{\hat{P}}) \in \hat{E}(\mathbb{F}_p)$ such that

$$x_{\hat{P}} y_{\hat{P}}^{-1} = 1. \tag{1.12}$$

Here the twist parameter z of Eq.(1.4) is considered to be $\hat{z} = (x_P y_P^{-1})^6$ of Eq.(1.2.4), where $\hat{z}$ is a quadratic and cubic residue in $\mathbb{F}_p$ and $\hat{E}$ denotes the KSS-18 curve defined by Eq.(1.2.4). From the isomorphic mapping Eq.(1.4), such z is obtained by solving the following equation considering the input $P(x_P, y_P)$.

$$z^{1/3} x_P = z^{1/2} y_P, \tag{1.13}$$

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

$$\hat{P}(x_{\hat{P}}, y_{\hat{P}}) = (x_P^3 y_P^{-2}, x_P^3 y_P^{-2}). \tag{1.14}$$

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.(1.2.4), first mapping not only P to $\hat{P}$ shown above but also Q to $\hat{Q}$ shown below.

$$\hat{Q}(x_{\hat{Q}}, y_{\hat{Q}}) = (x_P^2 y_P^{-2} x_Q, x_P^3 y_P^{-3} y_Q). \tag{1.15}$$

When we define a new variable $L = (x_P^{-3} y_P^2) = y_{\hat{P}}^{-1}$, the line evaluations, Eq.(1.9) and Eq.(1.10) 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.

1.3.2.1 Step 3: Doubling Phase ($T = Q$)

$$\begin{gathered} A = \tfrac{1}{2y}, B = 3x^2, C = AB, D = 2x, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, \\ \hat{l}_{T,T}(P) = y_P^{-1} l_{T,T}(P) = 1 + ELv - C\theta, \end{gathered} \tag{1.16}$$

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

1.3.2.2 Step 5: Addition Phase ($T \neq Q$)

$$\begin{gathered} A = \tfrac{1}{x_2 - x}, B = y_2 - y, C = AB, D = x + x_2, x_3 = C^2 - D, \\ E = Cx - y, y_3 = E - Cx_3, \\ \hat{l}_{T,Q}(P) = y_P^{-1} l_{T,Q}(P) = 1 + ELv - C\theta, \end{gathered} \tag{1.17}$$

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

As we compare the above equation with to Eq.(1.9) and Eq.(1.10), 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.

1.4 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.

1.4.1 Parameter Settings and Computational Environment

In the experimental simulation, this chapter has considered the 192 bit security level for KSS-18 curve. Table 1.1 shows the parameters settings suggested in [Ara+13] for 192 bit security over KSS-18 curve. However this parameter settings does not necessarily comply with the recent suggestion of key size by Kim et al. [KB16] for 192 bit security level. The sole purpose to use this parameter settings in this chapter is to compare the literature with the experimental result.

TABLE 1.1: Parameters for Optimal-Ate pairing over KSS-18 curve.

Security level	u	$p(u)$ [bit]	c Eq.(1.3)	b Eq.(1.1)
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 1.2 shows the computational environment.

1.4.2 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 $\in \mathbb{F}_{p^{18}}$

TABLE 1.2: Computing environment of Optimal-Ate pairing over KSS-18 curve.

CPU	Core i5 6600
Memory	8.00GB
OS	Ubuntu 16.04 LTS
Library	GMP 6.1.0 [Gt15]
Compiler	gcc 5.4.0
Programming language	C

respectively. Table 1.3 and Table 1.4 show the calculation costs with respect to operation count.

TABLE 1.3: 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 1.4: Operation count of multiplication.

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

By analyzing the Table 1.4 we can find that 11-sparse multiplication requires 18 more multiplication in $\mathbb{F}_p$ than pseudo 12-sparse multiplication.

1.4.3 Experimental Result

Table 1.5 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.

1.5 Contribution Summary

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

TABLE 1.5: 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

parameter but also on efficient elliptic curve arithmetic operation and efficient final exponentiation. This chapter has proposed a *pseudo 12-sparse multiplication* to accelerate Miller's loop calculation in KSS-18 curve by utilizing the property of rational point groups. In addition, this chapter has shown 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 chapter has implemented the proposal with recommended security parameter settings for KSS-18 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.

1.6 Conclusion

This chapter has proposed pseudo 12-sparse multiplication for accelerating Optimal-Ate pairing on KSS-18 curve. According to the calculation costs and experimental results shown in this chapter, the proposed method can calculate Optimal-Ate pairing more efficiently.

Chapter 2

Isomorphic Mapping over Quartic and Sextic twisted KSS Curves

Implementing asynchronous pairing operation on a certain pairing-friendly non-supersingular curve requires two rational points typically denoted as P and Q. Generally, P is spotted on the curve $E(\mathbb{F}_p)$, defined over the prime field $\mathbb{F}_p$ and Q is placed in a group of rational points on the curve $E(\mathbb{F}_{p^k})$, defined over $\mathbb{F}_{p^k}$, where k is the *embedding degree* of the pairing-friendly curve. In the case of Kachisa-Schaefer-Scott (KSS) pairing-friendly curve family, $k \geq 16$. Therefore performing pairing calculation on such curves requires calculating elliptic curve operations in higher degree extension field, which is regarded as one of the major bottlenecks to the efficient pairing operation. However, there exists a *twisted* curve of $E(\mathbb{F}_{p^k})$, denoted as $E'(\mathbb{F}_{p^{k/d}})$, where d is the twist degree, on which calculation is faster than the k-th degree extension field. Rational points group defined over such twisted curve has an isomorphic group in $E(\mathbb{F}_{p^k})$. This thesis explicitly shows the mapping procedure between the isomorphic groups in the context of Ate-based pairing over KSS family of pairing-friendly curves. This thesis considers *quartic twist* and *sextic twist* for KSS curve of embedding degree $k = 16$ and $k = 18$ receptively. To evaluate the performance enhancement of isomorphic mapping, this papers shows the experimental result by comparing the scalar multiplication. The result shows that scalar multiplication in $E(\mathbb{F}_{p^{k/d}})$ is 10 to 20 times faster than scalar multiplication in $E(\mathbb{F}_{p^k})$. It also shows that sextic twist is faster than the quartic twist for KSS curve when parameter settings for 192-bit security level are considered.

2.1 Introduction

Pairing-based cryptography is comparatively a new field of cryptographic research which generally deals with a specific algorithm with some certain characteristics. It has emerged at the very begining of the 21^{st} century when Sakai et al. [Sak00] and Joux et al. [Jou04] independently proposed a new cryptosystem based on elliptic curve pairing. Since then, pairing-based cryptography has attracted many researchers. As a result, several innovative pairing-based cryptographic applications such as ID-based encryption [Sak00], attribute base encryption [SW04], broadcast encryption [BGW05] and group

signature authentication [BBS04] escalated the popularity of pairing-based cryptography. In such outcome, Ate-based pairings such as Ate [Coh+05], Optimal-ate [Ver10], χ-Ate [Nog+08], R-ate [LLP09] and twisted Ate [Mat+07] 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 thesis focuses on a peripheral technique of Ate-based pairings with Kachisa-Schaefer-Scott (KSS) family of pairing-friendly curves [KSS07].

In general, pairing is a bilinear map from two additive rational point groups $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group $\mathbb{G}_3$ [SCA86], 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:

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

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

where ξ 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 of the field 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. In [Ara+13], Aranha et al. have presented pairing calculation for 192-bit security level where KSS curve of embedding degree 18 is regarded as one of the good candidates for 192-bit security level. Recently Zhang et al. [ZL12] have shown that the KSS curve of embedding degree 16 are more suitable for 192-bit security level. Therefore this thesis has considered KSS pairing-friendly curves of embedding degree $k = 16$ and 18.

In Ate-based pairing with KSS curve, pairing computations are done in higher degree extension field $\mathbb{F}_{p^k}$. However, KSS curves defined over $\mathbb{F}_{p^{18}}$ have the sextic twisted isomorphic rational point group defined over $\mathbb{F}_{p^3}$ and KSS curves defined over $\mathbb{F}_{p^{16}}$ have the quartic twisted isomorphism over $\mathbb{F}_{p^4}$. Therefore we can execute computations in the subfield $\mathbb{F}_{p^{k/d}}$ where d is the twist degree. Exploiting such a property, different arithmetic operations of Ate-based pairing can be efficiently performed in $\mathbb{G}_2$. However, performing elliptic curve operations in small extension field brings security issue since they are vulnerable to small subgroup attack [LL97]. Recently Barreto et al. [Bar+15] have studied the resistance of KSS18 curves to small subgroup attacks. Such resistible KSS16 curve is also studied by Loubna et al. [GF16] at 192-bit security level. Therefore isomorphic mapping of KSS18 and KSS16 curves and implementing arithmetic operation can be done securely in subfield twisted curves for 192-bit security level. This thesis has mainly focused on isomorphic mapping of $\mathbb{G}_2$ rational points from extension field $\mathbb{F}_{p^k}$ to its twisted (sextic and quartic) subfield $\mathbb{F}_{p^{k/d}}$ and its reverse procedure for both KSS18 and KSS16 curves.

The advantage of such isomorphic mapping is examined by performing scalar multiplication on $\mathbb{G}_2 \subset E(\mathbb{F}_{p^k})$ rational point, since scalar multiplication is required repeatedly in cryptographic calculation. Three well-known scalar multiplication algorithms are considered for the comprehensive experimental implementation named as binary method, Montgomery ladder and sliding-window method. This thesis has considered subfield twisted curve of both KSS16 and KSS18 curve, denoted as E'. KSS18 curve E' includes sextic twisted isomorphic rational point group denoted as $\mathbb{G}_2' \subset E'(\mathbb{F}_{p^3})$, whereas for KSS16 curve E' contains the quartic twisted isomorphic rational point group denoted as $\mathbb{G}_2' \subset E'(\mathbb{F}_{p^4})$. 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 is performed in $\mathbb{G}_2'$ and then resulted points are re-mapped to $\mathbb{G}_2$.

The experiment result shows that efficiency of scalar multiplication is increased by more than 20 to 10 times in subfield twisted curve E' than scalar multiplication in $E(\mathbb{F}_{p^{18}})$ and $E(\mathbb{F}_{p^{16}})$ respectively without applying the proposed mapping. The mapping and remapping for sextic twisted curves 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 sextic twisted mapping procedure has no expensive arithmetic operation. On the other hand, quartic twisted mapping requires no arithmetic operation rather it needs some attention since elliptic curve doubling in the twisted curve has a tricky part. The experiment also reveals that sextic twist is preferable since it gives better performance than quartic twist. Performance of such isomorphic mapping can be fully realized when it is applied in some pairing-based protocols. It is obvious that efficiency of Ate-based pairing protocols depends not only on improved scalar multiplication but also on efficient Miller's algorithm and final exponentiation implementation. In our recent work [Kha+17], presented in ICISC'16 shows the efficient Miller's algorithm implementation for Ate-based pairings. As a future work, we would also like to apply this isomorphic mapping in [Kha+17] with real pairing-based protocols implementation and evaluate its advantage.

A part of this work, isomorphic mapping of KSS curve of embedding degree 18, has been presented at CANDAR'16 [KN16]. In this thesis, we have additionally considered quartic twist for KSS16 curve. We have chosen the parameter of KSS16 curve from [GF16] for 192-bit security. The quartic twist is also compared with sextic twist of KSS18 curve with detailed implementation procedure. The main focus of this thesis is to demonstrate the details implementation procedure of sextic and quartic twist on KSS18 and KSS16 curve respectively at 192-bit security level.

The rest of the thesis is organized as follows: section 2 briefly overviews the fundamentals of elliptic curve arithmetic, scalar multiplication and the construction of KSS curves over $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{16}}$ extension field. The rational point groups for asynchronous pairing and the twist (quartic, sextic) property is also discussed in this section. In section 3, the proposed isomorphic mapping technique between rational point Q and Q' over the twisted KSS curves is described in details. The experimental result is presented in section

4, which shows that scalar multiplication on $\mathbb{G}_2$ point can be accelerated by 10 to 20 times by applying the proposed mapping technique in both KSS16 and KSS18. The result also shows that the sextic twist of KSS18 is faster than the quartic twist of the KSS16 curve. The thesis concludes in section 5 with an outline of future enhancement.

2.2 Fundamentals

The brief overview of the fundamental elliptic curve operations, KSS family of pairing-friendly curves and twisted property of KSS curve is discussed concisely in this section.

This thesis has considered left-to-right binary scalar multiplication for evaluating the efficiency of the proposed mapping operation. From the view point of security binary method is vulnerable to side channel attack. Therefore this thesis has also experimented with Montgomery ladder [SCA86] and siding window method for scalar multiplication evaluation.

2.2.1 Kachisa-Schaefer-Scott (KSS) curve [KSS07]

In [KSS07], Kachisa, Schaefer, and Scott proposed a family of non supersingular Brezing-Weng pairing-friendly elliptic curves of embedding degree $k = \{16, 18, 32, 36, 40\}$, using elements in the cyclotomic field. Similar to other pairing-friendly curves, *characteristic p*, *Frobenius trace t* and *order r* of these curves are given systematically by using an integer variable also known as mother parameter. In what follows, this papers considers two curves of this family named as *KSS16* of embedding degree $k = 16$ and *KSS18* of $k = 18$.

KSS18 curve, defined over $\mathbb{F}_{p^{18}}$, is given by the following equation

$$E/\mathbb{F}_{p^{18}} : Y^2 = X^3 + b, \quad b \in \mathbb{F}_p \text{ and } b \neq 0\,, \tag{2.1}$$

where $X, Y \in \mathbb{F}_{p^{18}}$. KSS18 curve is parametrized by an integer variable u as follows:

$$p(u) = (u^8 + 5u^7 + 7u^6 + 37u^5 + 188u^4 + 259u^3 + 343u^2 + 1763u + 2401)/21, \tag{2.2a}$$
$$r(u) = (u^6 + 37u^3 + 343)/343, \tag{2.2b}$$
$$t(u) = (u^4 + 16u + 7)/7. \tag{2.2c}$$

The necessary condition for u is $u \equiv 14 \pmod{42}$ and the ρ value is $\rho = (\log_2 p/\log_2 r) \approx 1.33$.

On the other hand, KSS16 curve is defined over $\mathbb{F}_{p^{16}}$, represented by the following equation

$$E/\mathbb{F}_{p^{16}} : Y^2 = X^3 + aX, \quad (a \in \mathbb{F}_p) \text{ and } a \neq 0, \tag{2.3}$$

where $X, Y \in \mathbb{F}_{p^{16}}$. Its characteristic p, Frobenius trace t and order r are given the integer variable u as follows:

$$p(u) = (u^{10} + 2u^9 + 5u^8 + 48u^6 + 152u^5 + 240u^4 + 625u^2 + 2398u + 3125)/980, \quad (2.4a)$$
$$r(u) = u^8 + 48u^4 + 625, \quad (2.4b)$$
$$t(u) = (2u^5 + 41u + 35)/35, \quad (2.4c)$$

where u is such that $u \equiv 25$ or $45 \pmod{70}$ and the ρ value is $\rho = (\log_2 p/\log_2 r) \approx 1.25$.

2.2.2 Extension field arithmetic

Pairing-based cryptography requires performing the arithmetic operation in extension fields of degree $k \geq 6$ [SCA86]. Consequently, such higher extension field needs to be constructed as a tower of extension fields [BS09] to perform arithmetic operation cost effectively. In the previous works of Bailey et al. [BP01] explained optimal extension field by towering by using irreducible binomials. Since this thesis uses two curves of different extension degree, therefore, the construction process of $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{16}}$ are represented in the following as a tower of subfields.

2.2.2.1 Towering of $\mathbb{F}_{p^{18}}$ extension field

Let $3|(p-1)$, where p is the characteristics of KSS18 and c is a quadratic and cubic non residue in $\mathbb{F}_p$. In the context of KSS18, where $k = 18$, $\mathbb{F}_{p^{18}}$ is constructed as tower field with irreducible binomial as follows:

$$\begin{cases} \mathbb{F}_{p^3} = \mathbb{F}_p[i]/(i^3 - c), \\ \mathbb{F}_{p^6} = \mathbb{F}_{p^3}[v]/(v^2 - i), \\ \mathbb{F}_{p^{18}} = \mathbb{F}_{p^6}[\theta]/(\theta^3 - v). \end{cases} \quad (2.5)$$

Here $c = 2$ is considered to be the best choice for efficient extension field 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 $\mathbb{F}_{p^3}$.

2.2.2.2 Towering of $\mathbb{F}_{p^{16}}$ extension field

Let the characteristics p of KSS16 is such that $4|(p-1)$ and z is a quadratic non residue in $\mathbb{F}_p$. By using irreducible binomials, $\mathbb{F}_{p^{16}}$ is constructed for KSS16 curve as follows:

$$\begin{cases} \mathbb{F}_{p^2} = \mathbb{F}_p[\alpha]/(\alpha^2 - z), \\ \mathbb{F}_{p^4} = \mathbb{F}_{p^2}[\beta]/(\beta^2 - \alpha), \\ \mathbb{F}_{p^8} = \mathbb{F}_{p^4}[\gamma]/(\gamma^2 - \beta), \\ \mathbb{F}_{p^{16}} = \mathbb{F}_{p^8}[\omega]/(\omega^2 - \gamma), \end{cases} \quad (2.6)$$

Here $z = 11$ is chosen along with the value of mother parameter u as given in Appendix **??**.

2.2.3 $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ groups

In the context of pairing-based cryptography, especially on KSS curve, two addititive rational point groups $\mathbb{G}_1, \mathbb{G}_2$ and a multiplicative group $\mathbb{G}_3$ of order r are considered. From [Mor+14], $\mathbb{G}_1$, $\mathbb{G}_2$ and $\mathbb{G}_3$ are defined as follows:

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

$$\xi : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_3, \tag{2.7}$$

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

2.2.4 Twist of KSS curves

Let us consider performing an asynchronous type of pairing operation on KSS curves. Let it be the Ate pairing $\xi(P, Q)$, one of asynchronous variants. P is defined over the prime field $\mathbb{F}_p$ and Q is typically placed on the k-th degree extension field $\mathbb{F}_{p^k}$ on the defined KSS curve. There exists a *twisted curve* with a group of rational points of order r which are isomorphic to the group where rational point $Q \in E(\mathbb{F}_{p^k})$ belongs to. This subfield isomorphic rational point group includes a twisted isomorphic point of Q, typically denoted as $Q' \in E'(\mathbb{F}_{p^{k/d}})$, where k is the embedding degree and d is the twist degree.

Since points on the twisted curve are defined over a smaller field than $\mathbb{F}_{p^k}$, therefore ECA and ECD becomes faster. However, when required in the pairing calculation such as for line evaluation they can be quickly mapped to a point on $E(\mathbb{F}_{p^k})$. Defining such mapping and re-mapping techniques is the main focus of this thesis. Since the pairing-friendly KSS16 [KSS07] curve has CM discriminant of $D = 1$ and $4|k$, therefore quartic twist is available. For sextic twist, the curve should have $D = 3$ and $6|k$, which exists in KSS18.

2.2.4.1 Sextic twist of KSS18 curve

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

$$E : \quad y^2 = x^3 + b, \quad b \in \mathbb{F}_p, \tag{2.8}$$

$$E'_6 : \quad y^2 = x^3 + bv^{-1}, \tag{2.9}$$

where v is a quadratic and cubic non residue in $E(\mathbb{F}_{p^e})$ and $3|(p^e - 1)$. For KSS18 curve $e = 3$. Isomorphism between $E'_6(\mathbb{F}_{p^e})$ and $E(\mathbb{F}_{p^{6e}})$, is given as

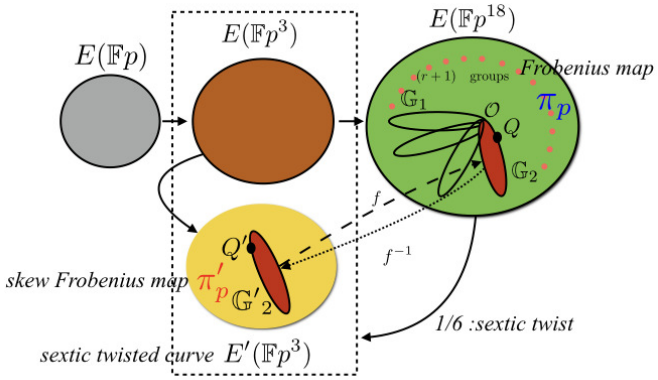


FIGURE 2.1: *sextic twist* in KSS18 curve.

follows:

$$\psi_6 : \begin{cases} E'_6(\mathbb{F}_{p^e}) \rightarrow E(\mathbb{F}_{p^{6e}}), \\ (x, y) \quad \mapsto (xv^{1/3}, yv^{1/2}). \end{cases} \tag{2.10}$$

2.2.4.2 Quartic twist of KSS16 curve

The quartic twist of KSS16 curve is given as follows:

$$E : \quad y^2 = x^3 + ax, \quad a \in \mathbb{F}_p, \tag{2.11}$$

$$E'_4 : \quad y^2 = x^3 + a\sigma^{-1}x, \tag{2.12}$$

where σ is a quadratic non residue in $E(\mathbb{F}_{p^4})$ and $4|(p-1)$. The Isomorphism between $E'_4(\mathbb{F}_{p^4})$ and $E(\mathbb{F}_{p^{16}})$, is given as follows:

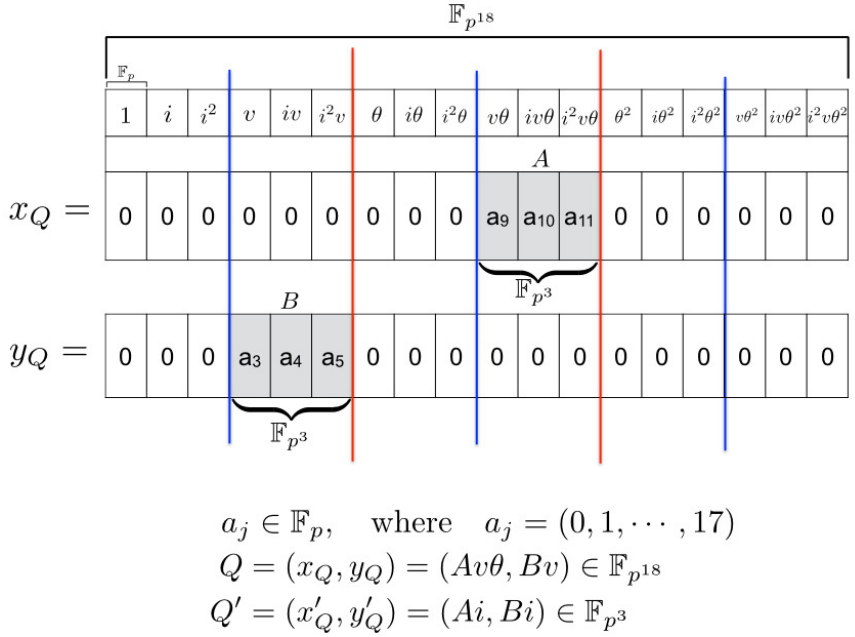
$$\psi_4 : \begin{cases} E'_4(\mathbb{F}_{p^4}) \rightarrow E(\mathbb{F}_{p^{16}}), \\ (x, y) \quad \mapsto (x\sigma^{1/2}, y\sigma^{3/4}). \end{cases} \tag{2.13}$$

2.3 Proposed isomorphic mapping between Q and Q'

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

2.3.1 Sextic twisted isomorphic mapping between $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{18}})$ and $Q' \in \mathbb{G}'_2 \subset E'(\mathbb{F}_{p^3})$

Figure 3.1 shows an overview of sextic twisted curve $E'(\mathbb{F}_{p^3})$ of $E(\mathbb{F}_{p^{18}})$.



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

FIGURE 2.2: $Q \in \mathbb{F}_{p^{18}}$ and its sextic twisted isomorphic rational point $Q' \in \mathbb{F}_{p^3}$ structure in KSS18 curve.

Let us consider E be the KSS18 curve in base field $\mathbb{F}_{p^3}$ and E' is sextic twist of E' given as follows:

$$E : y^2 = x^3 + b, \tag{2.14}$$
$$E' : y^2 = x^3 + bi, \tag{2.15}$$

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 the context of KSS18 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 coordinate. Figure 3.2 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 KSS18 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 a $\mathbb{F}_{p^3}$ field.

This thesis considers parameter given in Appendix **??** for KSS18 curve where mother parameter u = 65-bit and characteristics p = 511-bit. In such consideration, Q is given as $Q = (Av\theta, Bv)$, showed in Figure 3.2, 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 subfield 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.(3.15) with θ^{-6}, where $i = \theta^6$ and $v = \theta^3$.

$$E' : \left(\frac{y}{\theta^3}\right)^2 = \left(\frac{x}{\theta^2}\right)^3 + b. \tag{2.16}$$

θ^{-2} of Eq.(3.16) can be represented as follows:

$$\begin{aligned} \theta^{-2} &= i^{-1} i \theta^{-2}, \\ &= i^{-1} \theta^4, \end{aligned} \tag{2.17a}$$

and multiplying i with both sides.

$$\theta^4 = i\theta^{-2}. \tag{2.17b}$$

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

$$\begin{aligned} \theta^{-3} &= i^{-1} i \theta^{-3}, \\ &= i^{-1} \theta^3. \end{aligned} \tag{2.17c}$$

Multiplying i with both sides of Eq.(3.17c) we get θ^3 as,

$$\theta^3 = i\theta^{-3}, \tag{2.17d}$$

2.3.1.1 Q to Q' mapping

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

$$Q = (A\theta^4, B\theta^3), \quad \text{where } v = \theta^3. \tag{2.18}$$

From Eq.(3.17b) and Eq.(3.17d), we substitute $\theta^4 = i\theta^{-2}$ and $\theta^3 = i\theta^{-3}$ in Eq.(3.18) as follows:

$$Q = (Ai\theta^{-2}, Bi\theta^{-3}), \tag{2.19}$$

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 coordinate of Q. Then these nonzero $\mathbb{F}_p$ elements form a $\mathbb{F}_{p^3}$ 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.(3.5), this mapping has required no expensive arithmetic operation. Multiplication by the basis element i in $\mathbb{F}_{p^3}$ can be done by 1 bitwise left shifting since $c = 2$ is considered for towering in Eq.(3.5).

2.3.1.2 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.(3.17a), Eq.(3.17c) and Eq.(3.16) 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.

2.3.2 Quartic twisted isomorphic mapping

For quartic twisted mapping first we need to obtain certain ration point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{16}})$ of subgroup order r. One necessary condition for obtaining such Q is $r^2 \mid \#E(\mathbb{F}_{p^{16}})$, where $\#E(\mathbb{F}_{p^{16}})$ is the number of rational points in $E(\mathbb{F}_{p^{16}})$. But it is carefully observed that $\#E(\mathbb{F}_{p^{16}})$ is not divisible by r^2 when r is given by Eq.(3.4b). Therefore polynomial of r, given in [KSS07] is divided as follows:

$$r(u) = (u^8 + 48u^4 + 625)/61250, \tag{2.21}$$

to make it dive $\#E(\mathbb{F}_{p^{16}})$ completely.

Let us consider the rational point $Q \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{16}})$ and its quartic twisted rational point $Q' \in \mathbb{G}_2 \subset E'(\mathbb{F}_{p^4})$. Rational point Q has a special vector representation given in Table 3.1.

TABLE 2.1: Vector representation of $Q = (x_Q, y_Q) \in \mathbb{F}_{p^{18}}$

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

From Table 3.1 co-ordinates of $Q = (x_Q, y_Q) \in \mathbb{F}_{p^{18}}$ is obtained as $Q = (x_Q, y_Q) = (\gamma x_{Q'}, \omega\gamma y_{Q'})$ where $x_{Q'}, y_{Q'}$ are the co-ordinates of the rational point Q' in the twisted curve. Now let's find the twisted curve of Eq.(3.3) in $\mathbb{F}_{p^4}$ as follows:

$$\begin{aligned} (\omega\gamma y_{Q'})^2 &= (\gamma x_{Q'})^3 + a(\gamma x_{Q'}), \\ \gamma\beta y_{Q'}^2 &= \gamma\beta x_{Q'}^3 + a\gamma x_{Q'}, \\ y_{Q'}^2 &= x_{Q'}^3 + a\beta^{-1} x_{Q'}, \quad \text{multiplying } (\gamma\beta)^{-1} \text{ both sides.} \end{aligned} \tag{2.22}$$

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

$$\lambda = (3x_{Q'}^2 + \mathbf{a})(2y_{Q'})^{-1}, \tag{2.23}$$

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

$$\begin{aligned} a\beta^{-1} &= (a + 0\alpha + 0\beta + 0\alpha\beta)\beta^{-1}, \\ &= z^{-1}a\alpha\beta \quad \text{where } \alpha^2 = z \end{aligned} \tag{2.24}$$

Now let us denote the quartic mapping as follows:

$$Q = (x_Q, y_Q) = (\gamma x_{Q'}, \omega\gamma y_{Q'}) \in \mathbb{G}_2 \subset E(\mathbb{F}_{p^{16}}) \longmapsto Q' = (x_{Q'}, y_{Q'}) \in \mathbb{G}_2' \subset E'(\mathbb{F}_{p^4}).$$

For mapping from Q to Q' no extra calculation is required. By picking the non-zero coefficients of Q and placing it to the corresponding basis position is enough to get Q'. Similarly, re-mapping from Q' to Q can also be done without any calculation rather multiplying with basis elements.

2.4 Result Analysis

The main focus of this proposed mapping is to find out the isomorphic mapping of two well-known pairing-friendly curves, KSS16 and KSS18. In order to determine the advantage of the proposal, this thesis has implemented 3 well-known elliptic curve scalar multiplication method named as the binary method, Montgomery ladder method, and sliding-window method.

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

In the experiment, after many careful searches, the mother parameter u is selected to find out $\mathbb{G}_2$ rational point Q for KSS18 curve. On the other hand, for KSS16 curve, parameters are given by Loubna et al. [GF16]. In pairing-based cryptosystems, both KSS16 and KSS18 are regarded as good candidates for implementing 192-bit security. Therefore, while choosing parameters for the experiment, this thesis has adapted 192-bit security level. But the main focus of this thesis is not to find out efficient parameters for certain security levels. The main purpose of the selected the parameters is to compare the twisted isomorphic mappings on the nominated curves at standard security levels.

Appendix **??** and Appendix **??** show the parameters used in the experiment. Table 4.2 shows the experiment environment, used to evaluate the usefulness of the proposed mapping. In the experiment, 100 scalar numbers of size less than order r is generated randomly and then scalar multiplication is calculated for both cases. Average value of execution time in [ms] is considered for comparison. Table 3.3 shows the additional settings considered during the experiment. The comparative result is shown in Table 3.4.

Analyzing Table 3.4, we can find that scalar multiplication on the sextic twisted KSS18 curve using the proposed mapping technique is more than 20 times faster than scalar multiplication without the proposed mapping. On the other hand, in the quartic twisted KSS16 curve, scalar multiplication becomes at most 10 times faster after applying proposed mapping techniques than no

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 10.12.3	iOS 10.2.1
Compiler	gcc 4.2.1	gcc 4.2.1
Programming Language	C	Objective-C, C
Library	GNU MP 6.1.1[Gt15]	GNU MP 6.1.1

*Only single core is used from two cores.

TABLE 2.3: Additional settings used in the experiment

	KSS18	KSS16
Number of sample s	100	100
Average bit size of s	377-bit	385-bit
Average hamming weight of s	187	193
Window size for sliding window method	4	4
No. of Pre-computed ECA in sliding window	14	14
Perceived level of security	192-bit	192-bit

mapping. Another important difference is sextic twisted mapped points take less time for scalar multiplication in both experiment environments. Therefore we can certainly say sextic twist over KSS18 is more efficient than the quartic twisted KSS16 curve for implementing pairing operations.

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 ratio of CPU frequencies of iPhone and PC is about $1.84/2.7 \approx 0.68$. The result shows that the ratio of execution time of PC and iPhone without mapping for KSS18 curve is around 0.62 to 0.66. Which is close to CPU frequency ratio. On the other hand, the ratio of execution time with mapping of KSS18 curve is also around 0.6. For KSS16 curve, the ratio with no mapping case is more than 0.8 and for mapping case it is around 0.7 to 0.9. Since PC and iPhone has different processor architectures therefore it's frequency ratio has modest relation with the execution time ratio. The ratio may also be effected by the other processes, running in certain environment during the experiment time.

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 the nominated KSS curves. The experiment does not focus on efficiently implementing scalar multiplication for certain environment. There

TABLE 2.4: Comparative result of average execution time in [ms] for scalar multiplication

	Average execution time [ms] comparison			
	KSS18		KSS16	
	PC	iPhone 6s	PC	iPhone 6s
Binary with mapping	5.7×10^1	8.2×10^1	1.3×10^2	1.4×10^2
Binary w/o mapping	1.2×10^3	1.8×10^3	1.2×10^3	1.3×10^3
Montgomery ladder with mapping	7.1×10^1	1.1×10^2	1.7×10^2	1.8×10^2
Montgomery ladder w/o mapping	1.5×10^3	2.4×10^3	1.6×10^3	1.8×10^3
Sliding-window with mapping	4.9×10^1	7.5×10^1	1.0×10^2	1.3×10^2
Sliding-window w/o mapping	1.0×10^3	1.6×10^3	1.0×10^3	1.2×10^3

are other pairing-friendly curves such as BLS-12, BLS-24 [FST10] where sextic twist is available. As our future work, we will try to apply the proposed mapping on those curves.

2.5 Conclusion and future work

In this thesis, we have proposed isomorphic mapping procedure of $\mathbb{G}_2$ rational point group to its sextic and quartic twisted subfield isomorphic rational point group $\mathbb{G}_2'$ and its reverse mapping for KSS18 and KSS16 curves in the context of Ate-based pairing. We have also evaluated the advantage of such mapping by applying binary scalar multiplication, Montgomery ladder, and sliding- window method on 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 20 to 10 times than scalar multiplication of $\mathbb{G}_2$ rational point directly in $\mathbb{F}_{p^{18}}$ and $\mathbb{F}_{p^{16}}$. In the previous work of Nogami et al. [Nog+09], have showed the procedure to apply skew Frobenius mapping on the twisted elliptic curve for Ate-based pairing. Such technique can also be applied on twisted isomorphic rational point after applying the proposed mapping techniques. In [Sak+08], Sakemi et al. have 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 curves. Together with the proposed mapping and the skew Frobenius mapping of $\mathbb{G}_1$ will remarkably accelerate the scalar multiplication over KSS curves in the context of pairing-based cryptography.

??

Chapter 3

ICCIT 2016

A Consideration of Towering Scheme for Efficient Arithmetic Operation over Extension Field of Degree 18

Barreto-Naehrig (BN) curve is a well studied pairing friendly curve of embedding degree 12, that uses arithmetic in $\mathbb{F}_{p^{12}}$. Therefore the arithmetic of $\mathbb{F}_{p^{12}}$ extension field is well studied. In this thesis, we have proposed an efficient approach of arithmetic operation over the extension field of degree 18 by towering. $\mathbb{F}_{p^{18}}$ extension field arithmetic is considered to be the basis of implementing the next generation pairing based security protocols. We have proposed to use $\mathbb{F}_p$ element to construct irreducible binomial for building tower of extension field up to $\mathbb{F}_{p^6}$, where conventional approach uses the root of previous irreducible polynomial to create next irreducible polynomials. Therefore using $\mathbb{F}_p$ elements in irreducible binomial construction, reduces the number of multiplications in $\mathbb{F}_p$ to calculate inversion and multiplication over $\mathbb{F}_{p^{18}}$, which effects acceleration in total arithmetic operation over $\mathbb{F}_{p^{18}}$.

3.1 Introduction

The emerging information security of computer system stands on the strong base of cryptography. Compared to RSA cryptography, elliptic curve cryptography [Kob87] gained much attention for its faster key generation, shorter key size with same security level and less memory and computing power consumption. Intractability of Elliptic Curve Discrete Logarithm Problem (ECDLP) encourages many innovative cryptographic protocols. At the very beginning of the twenty first century, a cyptosystems based on elliptic curve pairing was proposed independently by Sakai et al. [SK03] and Joux [Jou04]. Since then this pairing based cryptosystem has unlocked several novel ideas to researchers such as Identity based encryption scheme explained by Boneh et al. [BF01]. In addition, group signature authentication [BBS04],[NF05] and broadcast encryption [BGW05] has increased the popularity of pairing based cryptography. Pairings such as Weil[**Weil_p**], Tate and Optimal-ate [Ver10], Eta [HSV06] and χ-Ate [Nog+08] pairings has gained much attention in recent years. Pairing is a bilinear map from two rational point groups denoted

by $\mathbb{G}_1$ and $\mathbb{G}_2$ to a multiplicative group denoted by $\mathbb{G}_3$ [SCA86]. It is generally denoted by $\mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_3$. In addition, these groups are defined over a certain extension field $\mathbb{F}_{p^k}$, where p is the prime number, also called characteristics and k is the extension degree, especially called *embedding* degree. Therefore it is important to efficiently construct extension field arithmetic in order to make pairing based cryptography efficient.

In prairing based cryptography, rational points are defined over a certain pairing friendly elliptic curve. Let $E(\mathbb{F}_{p^k})$ be a set of rational points such as (x, y), $x, y \in \mathbb{F}_{p^k}$ lies in the elliptic curve E, defined over extension field $\mathbb{F}_{p^k}$ of embedding degree k. Security level of pairing based cryptography depends on the sizes of both r and p^k, where r denotes the largest prime number that divides the order of $E(\mathbb{F}_p)$. It is said that the next generation pairing-based cryptography needs $\log_2 r \approx 256$ and $\log_2 p^k \approx 3000$ to 5000. Supposing the most efficient case of $\rho = (\log_2 p)/(\log_2 r) = 1$, k needs to be 12 to 20. In this thesis we are considering $k = 18$ and 18 degree pairing friendly curve described in [FST06].

While using pairing based protocols, it is required to perform arithmetic in higher fields, such as $\mathbb{F}_{p^k}$ for moderate value of k [SCA86]. It is important to represent the field in such a way that, the arithmetic can be performed efficiently. One of the most efficient way is to use the tower of extension field [BS09]. Which explains that, higher level computations can be calculated as a function of lower level computations. Because of that, efficient implementation of lower level arithmetic results in the good performance of arithmetic in higher degree fields. Recently the implementation of pairing based cryptosystems for different low power and mobile devices are increasing. Moreover, the hardware capabilities of the embedded devices are improving which can make pairing implementations efficient and faster. Therefore efficiency of extension field arithmetic is important to improve the performance of pairing. In this thesis we have presented an efficient way to construct $\mathbb{F}_{p^{18}}$ extension field and performing arithmetic operation on that field. In current approach of constructing extension field by towering, root of previous irreducible polynomial is used to construct the irreducible polynomial for next extension field. In our proposal, element in prime field $\mathbb{F}_p$ is used to construct the irreducible polynomial for the first two extension field and for in the last extension field root of base extension field is used for constructing irreducible polynomial.

3.2 Preliminaries

In this section we will go though the background how tower of extension field is constructed in practice and some basic idea of basis to construct extension field.

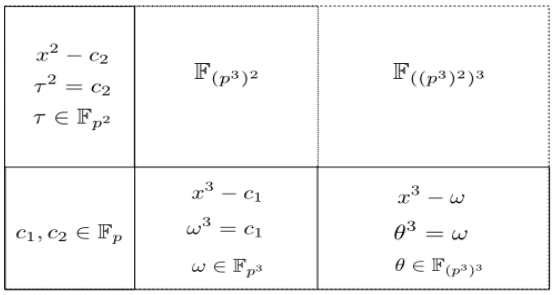


FIGURE 3.1: Construction overview of $\mathbb{F}_{((p^3)^2)^3}$

3.2.1 Basis of extension field and towering

In order to construct the arithmetic operations in $\mathbb{F}_{p^k}$, we generally need an irreducible polynomial $f(x)$ of degree k over $\mathbb{F}_p$. Let ω be a zero of $f(x)$, that is $\omega \in \mathbb{F}_{p^k}$, then the following set forms a basis of $\mathbb{F}_{p^k}$ over $\mathbb{F}_p$

$$\left\{1, \omega, \omega^2, \cdots, \omega^{k-1}\right\}, \tag{3.1}$$

which is known as polynomial basis. An arbitrary element A in $\mathbb{F}_{p^k}$ is written as

$$A = a_0 + a_1\omega + a_2\omega^2 + \cdots + a_{k-1}\omega^{k-1}. \tag{3.2}$$

The vector representation of A is $v_A = (a_0, a_1, a_2, \cdots a_{k-1})$. Multiplication and inversion in $\mathbb{F}_{p^k}$ are carried out by using the relation $f(\omega) = 0$, and therefore $f(x)$ is called the *modular reduction polynomial* of $\mathbb{F}_{p^k}$. Frobenious mapping should be efficient while calculating conjugates of ω.

Extension field of $\mathbb{F}_{p^k}$ with moderate value of k, such as $k \geq 6$ needs to be represented as a tower of sub extension field to improve pairing calculation. In [Lan08] explained tower of extension by using irreducible binomial. In case of Barreto-Naehrig (BN) curves [BN06], where $k = 12$, towering extension field with irreducible binomial is represented as follows:

$$\begin{cases} \mathbb{F}_{p^2} = \mathbb{F}_q[\omega]/(\omega^2 - \beta), \text{where } \beta = c \text{ and } c \in \mathbb{F}_p. \\ \mathbb{F}_{p^6} = \mathbb{F}_{q^2}[\tau]/(\tau^3 - \xi), \text{where } \xi = \omega + 1. \\ \mathbb{F}_{p^{12}} = \mathbb{F}_{q^6}[\theta]/(\theta^2 - \tau), \text{where } \tau = \xi. \end{cases}$$

Here p needs to be prime and $p - 1$ needs to be divisible by 4 and c should be quadratic and cubic non residue over $\mathbb{F}_p$.

In this section we will construct the extension field of degree 18 as a tower of three sub extension field. The extension field $\mathbb{F}_{p^3}$ is the sextic twist of $\mathbb{F}_{p^{18}}$. Therefore its is considered as the base field for constructing $\mathbb{F}_{((p^3)^2)^3}$ extension field in our proposal. Figure 4.1 shows the top level overview of our proposal to construct the tower of extension fields.

3.2.2 Arithmetic operations over extension field $\mathbb{F}_{p^3}$

At first, let us consider arithmetic operations in $\mathbb{F}_{p^3}$, which is the degree 3 extension field over $\mathbb{F}_p$. In order to perform arithmetic operations in $\mathbb{F}_{p^3}$, we generally need an irreducible polynomial $f(x)$ of degree 3 over $\mathbb{F}_p$. Specifically irreducible binomial is efficient to use as reduction modular polynomial. In order to obtain such binomial, Legendre symbol $\left(c_1/p\right)$ is convenient. Let us consider $3|(p-1)$ and a non-zero element $c_1 \in \mathbb{F}_p$.

$$c_1^{\frac{p-1}{3}} = \begin{cases} 0 & c_1 = 0, \\ 1 & \text{CPR}, \\ otherwise & \text{CPNR}, \end{cases} \tag{3.3}$$

where CPR and CPNR are abbreviations of cubic power residue and cubic power non residue, respectively. If c_1 does not have any cubic root in $\mathbb{F}_p$, $f(x) = x^3 - c_1$ becomes an irreducible binomial over $\mathbb{F}_p$. Let ω be a zero of $f(x)$, which is an element in $\mathbb{F}_{p^3}$. Therefore the set $\{1, \omega, \omega^2\}$ forms a polynomial basis of $\mathbb{F}_{p^3}$ over $\mathbb{F}_p$. Now let us consider two arbitrary element **a, b** in $\mathbb{F}_{p^3}$, can be represented as follows:

$$\begin{aligned} \mathbf{a} &= a_0 + a_1\omega + a_2\omega^2, \\ \mathbf{b} &= b_0 + b_1\omega + b_2\omega^2, \\ & a_i, b_j \in \mathbb{F}_p. \end{aligned}$$

3.2.2.1 Addition and subtraction in $\mathbb{F}_{p^3}$

Addition, subtraction within the elements and multiplication by a scalar with any element in $\mathbb{F}_{p^3}$ are carried out by coefficient wise operations over $\mathbb{F}_p$ as follows,

$$\mathbf{a} \pm \mathbf{b} = (a_0 \pm b_0, a_1 \pm b_1, a_2 \pm b_2), \tag{3.4}$$

$$k\mathbf{a} = (ka_0, ka_1, ka_2),\ k \in \mathbb{F}_p. \tag{3.5}$$

3.2.2.2 Multiplication in $\mathbb{F}_{p^3}$

Multiplication of two arbitrary vectors is performed as follows:

$$\begin{aligned} \mathbf{ab} &= (a_0 + a_1\omega + a_2\omega^2)(b_0 + b_1\omega + b_2\omega^2) \\ &= a_0b_0 + (a_0b_1 + a_1b_0)\omega + (a_0b_2 + a_1b_1 + a_2b_0)\omega^2 \\ &\quad +(a_1b_2 + a_2b_1)\omega^3 + a_2b_2\omega^4. \end{aligned} \tag{3.6}$$

Here in Eq.(4.6), there are 9 multiplications and 4 additions in $\mathbb{F}_p$. To reduce the number of multiplications in Eq.(4.6), we apply Fast Polynomial Multiplication introduced in [BP01] as follows:

$$\begin{aligned} A_0 &= a_0 b_0 \\ A_1 &= a_1 b_1 \\ A_2 &= a_2 b_2 \\ A_3 &= (a_0 + a_1)(b_0 + b_1) \\ A_4 &= (a_0 + a_2)(b_0 + b_2) \\ A_5 &= (a_1 + a_2)(b_1 + b_2), \end{aligned} \tag{3.7}$$

where $A_i, i = 0, 1, \cdots, 5$ are the auxiliary products. Let us consider $\mathbf{ab} = t(\omega) = \sum_{i=0}^{4} t_i \omega^i$. Now we can represent the coefficients $t(\omega)$ as only additions and subtractions of A_i,

$$\begin{aligned} t_0 &= A_0 \\ t_1 &= A_3 - A_1 - A_0 \\ &= (a_0 b_0 + a_0 b_1 + a_1 b_0 + a_1 b_1) - a_1 b_1 - a_0 b_0 \\ t_2 &= A_4 - A_2 - A_0 + A_1 \\ &= (a_0 b_0 + a_2 b_0 + a_0 b_2 + a_2 b_2) - a_2 b_2 - a_0 b_0 + a_1 b_1 \\ t_3 &= A_5 - A_1 - A_2 \\ &= (a_1 b_1 + a_1 b_2 + a_2 b_1 + a_2 b_2) - a_1 b_1 - a_2 b_2 \\ t_4 &= A_2. \end{aligned} \tag{3.8}$$

Considering subtractions as additions, from the above equations we find that only 6 multiplications and 13 additions are required in $\mathbb{F}_p$ for multiplying two arbitrary vectors in $\mathbb{F}_{p^3}$. Therefore, compared to Eq.(4.6) the above method will accelerate the vector multiplication, since in most processors multiplication is slower than addition. Substituting $\omega^3 = c_1$ in Eq.(4.6), owing to the fact that $f(\omega) = 0$ of the irreducible binomial $f(x) = x^3 - c_1$; **ab** becomes as follows:

$$\begin{aligned} \mathbf{ab} &= t_0 + t_1\omega + t_2\omega^2 + t_3\omega^3 + t_4\omega^4 \\ &= (t_0 + c_1 t_3) + (t_1 + c_1 t_4)\omega + t_2\omega^2. \end{aligned} \tag{3.9}$$

Here it requires 2 more $\mathbb{F}_p$ additions. Multiplication with c_1 will not increase the number of multiplications in $\mathbb{F}_p$ since c_1 is small such as 2 and it can be achieved using bit wise shifting. Finally 6 multiplications and 15 additions are required in $\mathbb{F}_p$ to multiply two elements in $\mathbb{F}_{p^3}$.

3.2.2.3 Squaring in $\mathbb{F}_{p^3}$

Squaring of an $\mathbb{F}_{p^3}$ element A is performed by applying Chung-Hasan method [CH07] as following.

$$\begin{aligned} A^2 &= (a_0 + a_1\omega + a_2\omega^2)^2 \\ &= a_0^2 + 2c_1a_1a_2 + [2a_0a_1 + c_1a_2^2]\omega + [(a_0 + a_1 + a_2)^2 \\ &\quad -(a_0^2 + a_2^2 + 2a_1a_2 + 2a_0a_1)]\omega^2. \end{aligned} \tag{3.10}$$

In what follows, let us consider Eq.(4.10) be written as $\mathbf{AB} = S_1 + S_2\omega + S_3\omega^2$ and the coefficients are expressed as Eq.(4.11). The following terms can be pre-calculated to reduce the number of operations. $T_1 = 2a_1$, $T_2 = a_0^2$, $T_3 = a_2^2$, $T_4 = T_1a_2$, $T_5 = T_1a_0$, $T_6 = (a_0 + a_1 + a_2)^2$.

$$S_1 = T_2 + c_1T_4, \tag{3.11a}$$
$$S_2 = T_5 + c_1T_3, \tag{3.11b}$$
$$S_3 = T_6 - (T_2 + T_3 + T4 + T_5). \tag{3.11c}$$

When $c_1 = 2$, the operation cost of a squaring in $\mathbb{F}_{p^3}$ is 2 multiplications, 3 squaring and 8 additions in $\mathbb{F}_p$ and 2 bit wise left shifting.

3.2.2.4 Vector inversion in $\mathbb{F}_{p^3}$

The inverse element $\mathbf{a}^{-1} \in \mathbb{F}_{p^3}$, can be easily calculated using Frobenius mapping (FM) $\pi(\mathbf{a})$. At first we find the conjugates $\mathbf{a}^p$, $\mathbf{a}^{p^2}$ of $\mathbf{a}$ by applying FM. Then the inverse element $\mathbf{a}^{-1}$ is calculated as follows.

$$\mathbf{a}^{-1} = n(\mathbf{a})^{-1}(\mathbf{a}^p\mathbf{a}^{p^2}), \tag{3.12}$$

where $n(\mathbf{a}) = (\mathbf{a}\mathbf{a}^p\mathbf{a}^{p^2}) \in \mathbb{F}_p^*$ is the product of conjugates. Conjugate $\mathbf{a}^p = (a_0 + a_1\omega + a_2\omega^2)^p$ can be easily calculated as follows:

$$\begin{aligned} (a_0 + a_1\omega + a_2\omega^2)^p &= (a_0 + a_1\omega)^p + (a_2\omega^2)^p \\ &= a_0 + a_1(\omega^3)^{\frac{p-1}{3}}\omega \\ &\quad +a_2((\omega^3)^{\frac{p-1}{3}})^2\omega^2 \\ &= a_0 + a_1(c_1)^{\frac{p-1}{3}}\omega \\ &\quad +a_2((c_1)^{\frac{p-1}{3}})^2\omega^2 \\ &= a_0 + a_1c_1'\omega + a_2c_1''\omega^2 \\ &= a_0 + a_1'\omega + a_2'\omega^2, \end{aligned} \tag{3.13}$$

where $a_1', a_2' \in \mathbb{F}_p$ and $c_1' = (c_1)^{\frac{p-1}{3}}$ is already known from Eq.(4.3) and $c_1'' = (c_1')^2$ can be precalculated. In the above computation, 2 multiplications in $\mathbb{F}_p$ is required. Now the other conjugate $\mathbf{a}^{p^2}$ can be calculated with the same

number of operations according to the above procedure as follows:

$$\begin{aligned}\mathbf{a}^{p^2} &= (\mathbf{a}^p)^p \\ &= (a_0 + a_1'\omega + a_2'\omega^2)^p \\ &= a_0 + a_1'c_1'\omega + a_2'c_1''\omega^2 \\ &= a_0 + a_1''\omega + a_2''\omega^2, \end{aligned} \tag{3.14}$$

where $a_1'', a_2'' \in \mathbb{F}_p$. Before calculating $n(\mathbf{a})$ we first calculate the multiplication of $(\mathbf{a}^p\mathbf{a}^{p^2})$ like Eq.(4.6) as follows

$$\mathbf{a}^p\mathbf{a}^{p^2} = (a_0 + a_1'\omega + a_2'\omega^2)(a_0 + a_1''\omega + a_2''\omega^2). \tag{3.15}$$

Now let us consider the following representation.
$\mathbf{T} = \mathbf{a}^p\mathbf{a}^{p^2} = (t_0, t_1, t_2), \quad n(\mathbf{a}) = s = \mathbf{a}\mathbf{T},$
Thereby the inversion of $\mathbf{a}$ can be expressed as $\mathbf{a}^{-1} = s^{-1}\mathbf{T}$. The vector representation of the non-zero scalar s is written as $s = (s, 0, 0)$. In addition, $\mathbf{a}^p$ and $\mathbf{a}^{p^2}$ is represented by the following equations by using the relation $c_1'^2 + c_1' + 1 = 0$, where $c_1'^3 = 1$.

$$\mathbf{a}^p = (a_0, c_1'a_1, c_1'^2a_2) = (a_0, c_1'a_1, -a_2 - c_1'a_2), \tag{3.16a}$$

$$\mathbf{a}^{p^2} = (a_0, c_1'^2a_1, c_1'a_2) = (a_0, -a_1 - c_1'a_1, c_1'a_2). \tag{3.16b}$$

Now let us consider the variables $T_0 \sim T_5$ as following expressions.

$$\begin{aligned} T_0 &= a_0^2, \\ T_1 &= a_1^2, \\ T_2 &= a_2^2, \\ T_3 &= (c_1'a_1 + c_1'^2a_2)(c_1'^2a_1 + c_1'a_2) \\ &= a_1^2 - a_1a_2 + a_2^2 \\ T_4 &= (a_0 + c_1'a_1)(a_0 + c_1'^2a_1) \\ &= a_0^2 - a_0a_1 + a_1^2 \\ T_5 &= (a_0 + c_1'^2a_2)(a_0 + c_1'a_2) \\ &= a_0^2 - a_0a_2 + a_2^2. \end{aligned}$$

The elements of $\mathbf{T} = (t_0, t_1, t_2)$ can be obtained as follows:

$$\begin{aligned} t_1 &= T_0 + c_1(T_3 - T_1 - T_2) \\ &= a_0^2 - c_1a_1a_2, \qquad (3.18a) \\ t_2 &= T_4 - T_0 - T_1 + c_1T_2 \\ &= c_1a_2^2 - a_0a_1, \qquad (3.18b) \\ t_3 &= T_5 - T_0 - T_2 + T_1 \\ &= a_1^2 - a_0a_2. \qquad (3.18c) \end{aligned}$$

The calculation cost of t_1, t_2, t_3 is 3 multiplications, 3 squaring, 3 additions and 2 bit shifting. The vector multiplication for getting $s = \mathbf{aT} = (s, 0, 0)$ can be done by calculating $s = a_0b_0 + c_1(a_1b_2 + a_2b_1)$ which costs 3 multiplication, 2 additions and 1 bit shifting.

Finally the inversion of the scalar s and multiplication by the inverse of scalar s with vector $\mathbf{T} = \mathbf{a}^p\mathbf{a}^{p^2}$ can be obtained by distributive law which takes 1 inversion and 3 multiplication in $\mathbb{F}_p$. Therefore the total cost of inversion is 9 multiplications, 3 squaring, 5 additions, 3 bit shifting and 1 inversion in $\mathbb{F}_p$.

3.2.3 Arithmetic operations over extension field $\mathbb{F}_{(p^3)^2}$

$\mathbb{F}_{(p^3)^2}$ is constructed with the irreducible binomial $g(x) = x^2 - c_2$ where $c_2 \in \mathbb{F}_p$. Here it differs from the existing method to towering. Existing method uses $x^2 - \omega$ as the irreducible polynomial in $\mathbb{F}_{p^6}$; that is the root of irreducible binomial of $\mathbb{F}_{p^3}$ is used to construct irreducible binomial in $\mathbb{F}_{p^6}$. In this proposed approach, such binomial can be easily obtained by applying Legendre Symbol (c_2/p) over $\mathbb{F}_p$. Then let its zero be τ,$\tau \in \mathbb{F}_{(p^3)^2}$, therefore the set $\{1, \tau\}$ forms the polynomial basis in $\mathbb{F}_{(p^3)^2}$. If we choose p such that $p \equiv 3 \pmod 4$, that will accelerate the arithmetic operation significantly; since multiplication by $c_2 = -1$ will be calculated only by substitution. Let us consider $\mathbf{m}, \mathbf{n}$ as two arbitrary elements in $\mathbb{F}_{(p^3)^2}$ as follows:

$$\begin{aligned} \mathbf{m} &= \mathbf{a}_0 + \mathbf{a}_1\tau, \\ \mathbf{n} &= \mathbf{b}_0 + \mathbf{b}_1\tau, \\ & \mathbf{a}_i, \mathbf{b}_j \in \mathbb{F}_{p^3}. \end{aligned}$$

Addition and Subtraction is done coefficient wise similar to those in $\mathbb{F}_{p^3}$. Multiplication of $\mathbf{m}, \mathbf{n}$ is done as follows:

$$\begin{aligned} \mathbf{mn} &= (\mathbf{a}_0 + \mathbf{a}_1\tau)(\mathbf{b}_0 + \mathbf{b}_1\tau) \\ &= \mathbf{a}_0\mathbf{b}_0 + (\mathbf{a}_0\mathbf{b}_1 + \mathbf{a}_1\mathbf{b}_0)\tau + \mathbf{a}_1\mathbf{b}_1\tau^2 \\ &= (\mathbf{a}_0\mathbf{b}_0 + c_2\mathbf{a}_1\mathbf{b}_1) + (\mathbf{a}_0\mathbf{b}_1 + \mathbf{a}_1\mathbf{b}_0)\tau \qquad (3.19) \\ &= (\mathbf{a}_0\mathbf{b}_0 + c_2\mathbf{a}_1\mathbf{b}_1) + (\mathbf{a}_0 + \mathbf{a}_1)(\mathbf{b}_0 + \mathbf{b}_1)\tau \\ &\quad -(\mathbf{a}_0\mathbf{b}_0)\tau - (\mathbf{a}_1\mathbf{b}_1)\tau. \qquad (3.20) \end{aligned}$$

Here Karatsuba method [KO62] is applied. In this calculation, we have substituted $\tau^2 = c_2$, as τ is a zero of the irreducible binomial $g(x) = x^2 - c_2$. Since prime number p is chosen such that $p \equiv 3 \pmod 4$, therefore c_2 is just substituted with -1. That means multiplication with c_2 needs no countable computations in $\mathbb{F}_p$. Moreover multiplication of $\mathbf{a}_1\mathbf{b}_1$ and $\mathbf{a}_0\mathbf{b}_0$ will be reused. Therefore we need 3 multiplications and 5 additions in $\mathbb{F}_{p^3}$ to multiply two vectors over $\mathbb{F}_{(p^3)^2}$, where we consider subtractions as additions.

3.2.3.1 Vector inversion in $\mathbb{F}_{(p^3)^2}$

For calculating the multiplicative inverse vector of a non-zero vector $\mathbf{m} \in \mathbb{F}_{(p^3)^2}$, first we calculate the conjugate of $\mathbf{m}$ that is given by Frobenius mapping $\pi_{p^3}(\mathbf{m}) = \mathbf{m}^{p^3}$. Then the inverse of $\mathbf{m}$, $\mathbf{m}^{-1}$ is calculated as follows:

$$\mathbf{m}^{-1} = n(\mathbf{m})^{-1}(\mathbf{m}^{p^3}), \tag{3.21}$$

where $\mathbf{m}$, $\mathbf{m}^{p^3}$ are the conjugates and $n(\mathbf{m})$ is their product. FM of $\mathbf{m}$, $\pi_{p^3}(\mathbf{m}) = (\mathbf{a}_0 + \mathbf{a}_1\tau)^{p^3}$ can be easily calculated using the defined irreducible binomial $g(x)$ as follows:

$$\begin{aligned}(\mathbf{a}_0 + \mathbf{a}_1\tau)^{p^3} &= \mathbf{a}_0 + \mathbf{a}_1\tau^{p^3} \\ &= \mathbf{a}_0 + \mathbf{a}_1(\tau^2)^{\frac{p^3-1}{2}}\tau \\ &= \mathbf{a}_0 + \mathbf{a}_1(c_2)^{\frac{p^3-1}{2}}\tau \\ &= \mathbf{a}_0 - \mathbf{a}_1\tau, \end{aligned} \tag{3.22}$$

where the modular relation $\tau^2 = c_2$ and $c_2 = -1$ is substituted. In other words, the conjugate of $\mathbf{m}$ is given as $\mathbf{a}_0 - \mathbf{a}_1\tau$. No addition and multiplication is required here. Now the calculation procedure for $n(\mathbf{m}) = \mathbf{m}\mathbf{m}^{p^3}$ is as follows:

$$\begin{aligned} n(\mathbf{m}) &= (\mathbf{a}_0 + \mathbf{a}_1\tau)(\mathbf{a}_0 - \mathbf{a}_1\tau) \\ &= \mathbf{a}_0^2 - \mathbf{a}_1^2\tau^2 \\ &= \mathbf{a}_0^2 - c_2\mathbf{a}_1^2 \\ &= \mathbf{a}_0^2 + \mathbf{a}_1^2. \end{aligned} \tag{3.23}$$

Here 2 squaring and 1 addition is required over $\mathbb{F}_{p^3}$. Since $n(\mathbf{m})$ is given without τ, it is found that $n(\mathbf{m}) \in \mathbb{F}_{p^3}$. Therefore, the inversion element $n(\mathbf{m})^{-1}$ is calculated using Eq.(4.12) over $\mathbb{F}_{p^3}$. Finally 2 multiplications, 2 squaring, 1 inversion and 1 addition in $\mathbb{F}_{p^3}$ is required to get an inverse element over $\mathbb{F}_{(p^3)^2}$.

3.2.4 Arithmetic operations over extension field $\mathbb{F}_{((p^3)^2)^3}$

To construct $\mathbb{F}_{((p^3)^2)^3}$ arithmetic operation let us consider irreducible binomial $h(x) = x^3 - \omega$ where $\omega \in \mathbb{F}_{p^3}$ and ω is the root of $f(x)$. Then let θ be a root of $h(x)$, where $\theta \in \mathbb{F}_{((p^3)^2)^3}$, therefore the set $\{1, \theta, \theta^2\}$ forms the polynomial basis in $\mathbb{F}_{((p^3)^2)^3}$. Let us consider $\mathbf{u}, \mathbf{v}$ as two arbitrary elements in $\mathbb{F}_{((p^3)^2)^3}$ as follows:

$$\begin{aligned} \mathbf{u} &= \mathbf{m}_0 + \mathbf{m}_1\theta + \mathbf{m}_2\theta^2, \\ \mathbf{v} &= \mathbf{n}_0 + \mathbf{n}_1\theta + \mathbf{n}_2\theta^2, \\ &\quad \mathbf{m}_i, \mathbf{n}_j \in \mathbb{F}_{(p^3)^2}. \end{aligned}$$

In $\mathbb{F}_{((p^3)^2)^3}$, vector addition and subtraction is performed coefficient wise over $\mathbb{F}_{(p^3)^2}$. Multiplication of $\mathbf{u}, \mathbf{v}$ is performed by using $h(x)$ as follows:

$$\mathbf{uv} = (\mathbf{m}_0 + \mathbf{m}_1\theta + \mathbf{m}_2\theta^2)(\mathbf{n}_0 + \mathbf{n}_1\theta + \mathbf{n}_2\theta^2). \tag{3.24}$$

After applying fast polynomial multiplication according to Eq.(4.7) and Eq.(4.8), here we have 6 multiplications and 15 additions in $\mathbb{F}_{(p^3)^2}$ as follows:

$$\begin{aligned} \mathbf{uv} &= t'_0 + t'_1\theta + t'_2\theta^2 + t'_3\theta^3 + t'_4\theta^4 \\ &= (t_0 + \omega t_3) + (t_1 + \omega t_4)\theta + t'_2\theta^2. \end{aligned} \tag{3.25}$$

Multiplication of basis element with vector will not effect the calculation since it is comparatively small, which will be calculated as bit wise shifting.

3.2.4.1 Vector inversion in $\mathbb{F}_{((p^3)^2)^3}$

Inversion of $\mathbb{F}_{((p^3)^2)^3}$ vector can be easily carried out by applying the similar steps of $\mathbb{F}_{p^3}$ vector inversion. For calculating the multiplicative inverse vector of a non-zero vector $\mathbf{v} \in \mathbb{F}_{((p^3)^2)^3}$, at first we find the conjugates $\mathbf{v}^{p^6}$, $\mathbf{v}^{p^{12}}$ of $\mathbf{v}$ applying FM. Then the inverse element $\mathbf{v}^{-1}$ is calculated as follows:

$$\mathbf{v}^{-1} = n(\mathbf{v})^{-1}(\mathbf{v}^{p^6}\mathbf{v}^{p^{12}}), \tag{3.26}$$

where $\mathbf{v}$, $\mathbf{v}^{p^6}, \mathbf{v}^{p^{12}}$ are the conjugates and $n(\mathbf{v})$ is their product. Here we first calculate $\pi_{p^6}(\mathbf{v}) = (\mathbf{n}_0 + \mathbf{n}_1\theta + \mathbf{n}_2\theta^2)^{p^6}$ using the defined irreducible binomial $h(x)$ as follows:

$$\begin{aligned} (\mathbf{n}_0 + \mathbf{n}_1\theta + \mathbf{n}_2\theta^2)^{p^6} &= (\mathbf{n}_0 + \mathbf{n}_1\theta)^{p^6} + (\mathbf{n}_2\theta^2)^{p^6} \\ &= \mathbf{n}_0 + \mathbf{n}_1(\theta^3)^{\frac{p^6-1}{3}}\theta \\ &\quad +\mathbf{n}_2((\theta^3)^{\frac{p^6-1}{3}})^2\theta^2 \\ &= \mathbf{n}_0 + \mathbf{n}_1(\omega)^{\frac{p^6-1}{3}}\theta \\ &\quad +\mathbf{n}_2((\omega)^{\frac{p^6-1}{3}})^2\theta^2 \\ &= \mathbf{n}_0 + \mathbf{n}_1(\omega^3)^{\frac{p^6-1}{9}}\theta \\ &\quad +\mathbf{n}_2((\omega^3)^{\frac{p^6-1}{9}})^2\theta^2 \\ &= \mathbf{n}_0 + \mathbf{n}_1(c_1)^{\frac{p^6-1}{9}}\theta \\ &\quad +\mathbf{n}_2((c_1)^{\frac{p^6-1}{9}})^2\theta^2 \\ &= \mathbf{n}_0 + \mathbf{n}_1c'_\omega\theta + \mathbf{n}_2c''_\omega\theta^2 \\ &= \mathbf{n}_0 + \mathbf{n}'_1\theta + \mathbf{n}'_2\theta^2, \end{aligned} \tag{3.27}$$

where $n'_1, n'_2 \in \mathbb{F}_{(p^3)^2}$ and $c'_\omega = (c_1)^{\frac{p^6-1}{9}}$, $c''_\omega = (c'_\omega)^2$ can be precalculated. Therefore only 6 multiplications in $\mathbb{F}_p$ is required in the above calculation. Now

the other conjugate $\mathbf{v}^{p^{12}}$ can be calculated according to the above procedure with the same number of operations as follows:

$$\begin{aligned}\mathbf{v}^{(p^6)^2} &= (\mathbf{v}^{p^{12}}) \\ &= (\mathbf{n}_0 + \mathbf{n}'_1\theta + \mathbf{n}'_2\theta^2)^{p^6} \\ &= \mathbf{n}_0 + \mathbf{n}'_1 c'_\omega\theta + \mathbf{n}'_2 c''_\omega\theta^2 \\ &= \mathbf{n}_0 + \mathbf{n}''_1\theta + \mathbf{n}''_2\theta^2. \end{aligned} \tag{3.28}$$

Now computation of $(\mathbf{v}^{p^6}\mathbf{v}^{p^{12}})$ according to Eq.(4.25) will cost 6 multiplication and 15 additions in $\mathbb{F}_{(p^3)^2}$ as follows:

$$\mathbf{v}^{p^6}\mathbf{v}^{p^{12}} = (\mathbf{n}_0 + \mathbf{n}'_1\theta + \mathbf{n}'_2\theta^2)(\mathbf{n}_0 + \mathbf{n}''_1\theta + \mathbf{n}''_2\theta^2). \tag{3.29}$$

The next calculation procedure is identical of $\mathbb{F}_{p^3}$ vector inversion which also results the same number of operation counts in $\mathbb{F}_{p^6}$. Finally the total cost of 1 vector inversion in $\mathbb{F}_{p^{18}}$ is 9 multiplications, 3 squaring, 5 additions, 3 bit shifting and 1 inversion in $\mathbb{F}_{p^6}$.

3.3 Result evaluation

The main focus of this proposal is to show the construction procedure of $\mathbb{F}_{p^{18}}$ extension field in a new approach of towering that will lead to efficient arithmetic operation. We can also apply subfield isomorphic group arithmetic or Cyclic Vector Multiplication Algorithm (CVMA) to reduce the number of additions and multiplication in each extension field which will make this towering construction more efficient. But that is not focused in this thesis.

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

TABLE 3.1: Computational Environment

•	PC
CPU *	2.7 GHz Intel Core i5
Memory	16 GB
OS	Mac OS X 10.11.4
Compiler	gcc 4.2.1
Programming Language	C
Library	GNU MP

*Only single core is used from two cores.

In the experiment we have used Kachisa-Schaefer-Scott (KSS) [KSS07] pairing friendly curves with embedding degree $k = 18$ at the 192-bit security

level. The prime number p = 511-bit is considered and the curve is defined as $y^2 = x^3 + 11$.

In what follows, let us consider m, s, a and i to denote the times of multiplication, squaring, addition and inversion respectively. The bit wise shifting operation is not taken into account during the final operation count. Table 4.2 shows the calculation cost in the context of operation count and Table 4.3 shows the execution time.

TABLE 3.2: $\mathbb{F}_{((p^3)^2)^3}$ operation count

Operation in	1 inversion in $\mathbb{F}_{p^{18}}$	1 multiplication in $\mathbb{F}_{p^{18}}$
$\mathbb{F}_p$	$199m + 9s + 660a + 1i$	$108m + 402a$

TABLE 3.3: Execution time [ms] for inversion and multiplication in $\mathbb{F}_{((p^3)^2)^3}$

Operation	Execution time[ms]
Inversion	5.4×10^{-1}
Multiplication	3.3×10^{-1}

From Table 4.2 we find that only 199 multiplication, 9 squaring, 660 additions and 1 inversion is required in $\mathbb{F}_p$ to perform 1 inversion in $\mathbb{F}_{p^{18}}$. There exist a competitive toweting scheme prsented by Aranha et al. [Ara+13] that uses subfield isomorphic group to reduce number of arithmetic operation. Such isomorphic subfield isomorphic rational point group technique can also be applied in the proposed towering approach which will be presented as our future work.

3.4 Conclusion and future work

In this thesis we have presented a new towering scheme to construct $\mathbb{F}_{p^{18}}$ extension field arithmetic. This towering approach is one of the most important step for constructing the basis of pairing based cryptography defined over extension field of degree 18. This thesis also presented the mathematical derivation for efficiently constructing the $\mathbb{F}_{((p^3)^2)^3}$ extension field to accelerate arithmetic operation in $\mathbb{F}_{p^{18}}$. The main focus of this thesis was to present the new towering technique along with its implementation procedure that can be used for performing operation efficiently in the context of pairing based cryptography. As our future work, we would like to reduce the number of arithmetic operation by applying subfield isomorphic rational point group technique in the proposed towering approach along with some pairing algorithms implementation in practical case.

Bibliography

[Ara+13] Diego F. Aranha, Laura Fuentes-Castañeda, Edward Knapp, Alfred Menezes, and Francisco Rodríguez-Henríquez. "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.

[Bar+15] Paulo S. L. M. Barreto, Craig Costello, Rafael Misoczki, Michael Naehrig, Geovandro C. C. F. Pereira, and Gustavo Zanon. "Subgroup Security in Pairing-Based Cryptography". In: *LATINCRYPT 2015*. Ed. by Kristin E. Lauter and Francisco Rodríguez-Henríquez. Vol. 9230. LNCS. Springer, Heidelberg, Aug. 2015, pp. 245–265. DOI: 10.1007/978-3-319-22174-8_14.

[BBS04] Dan Boneh, Xavier Boyen, and Hovav Shacham. "Short Group Signatures". In: *CRYPTO 2004*. Ed. by Matthew Franklin. Vol. 3152. LNCS. Springer, Heidelberg, Aug. 2004, pp. 41–55. DOI: 10.1007/978-3-540-28628-8_3.

[BF01] Dan Boneh and Matthew K. Franklin. "Identity-Based Encryption from the Weil Pairing". In: *CRYPTO 2001*. Ed. by Joe Kilian. Vol. 2139. LNCS. Springer, Heidelberg, Aug. 2001, pp. 213–229. DOI: 10.1007/3-540-44647-8_13.

[BGW05] Dan Boneh, Craig Gentry, and Brent Waters. "Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys". In: *CRYPTO 2005*. Ed. by Victor Shoup. Vol. 3621. LNCS. Springer, Heidelberg, Aug. 2005, pp. 258–275. DOI: 10.1007/11535218_16.

[BLS03] Paulo S. L. M. Barreto, Ben Lynn, and Michael Scott. "Constructing Elliptic Curves with Prescribed Embedding Degrees". In: *SCN 02*. Ed. by Stelvio Cimato, Clemente Galdi, and Giuseppe Persiano. Vol. 2576. LNCS. Springer, Heidelberg, Sept. 2003, pp. 257–267. DOI: 10.1007/3-540-36413-7_19.

[BN06] 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.

[BP01] 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.

[BP98] Daniel V. Bailey and Christof Paar. "Optimal Extension Fields for Fast Arithmetic in Public-Key Algorithms". In: *CRYPTO'98*. Ed. by Hugo Krawczyk. Vol. 1462. LNCS. Springer, Heidelberg, Aug. 1998, pp. 472–485. DOI: 10.1007/BFb0055748.

[BS09] Naomi Benger and Michael Scott. *Constructing Tower Extensions for the implementation of Pairing-Based Cryptography*. Cryptology ePrint Archive, Report 2009/556. http://eprint.iacr.org/2009/556. 2009.

[CH07] Jaewook Chung and M Anwar Hasan. "Asymmetric squaring formulae". In: *Computer Arithmetic, 2007. ARITH'07. 18th IEEE Symposium on*. IEEE. 2007, pp. 113–122.

[Coh+05] Henri Cohen, Gerhard Frey, Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren, eds. *Handbook of Elliptic and Hyperelliptic Curve Cryptography*. Chapman and Hall/CRC, 2005. ISBN: 978-1-58488-518-4. DOI: 10.1201/9781420034981.

[DEM05] Régis Dupont, Andreas Enge, and François Morain. "Building Curves with Arbitrary Small MOV Degree over Finite Prime Fields". In: *Journal of Cryptology* 18.2 (Apr. 2005), pp. 79–89. DOI: 10.1007/s00145-004-0219-7.

[DSD07] Augusto Jun Devegili, Michael Scott, and Ricardo Dahab. "Implementing Cryptographic Pairings over Barreto-Naehrig Curves (Invited Talk)". In: *PAIRING 2007*. Ed. by Tsuyoshi Takagi, Tatsuaki Okamoto, Eiji Okamoto, and Takeshi Okamoto. Vol. 4575. LNCS. Springer, Heidelberg, July 2007, pp. 197–207. DOI: 10.1007/978-3-540-73489-5_10.

[FST06] David Freeman, Michael Scott, and Edlyn Teske. *A taxonomy of pairing-friendly elliptic curves*. Cryptology ePrint Archive, Report 2006/372. http://eprint.iacr.org/2006/372. 2006.

[FST10] David Freeman, Michael Scott, and Edlyn Teske. "A Taxonomy of Pairing-Friendly Elliptic Curves". In: *Journal of Cryptology* 23.2 (Apr. 2010), pp. 224–280. DOI: 10.1007/s00145-009-9048-z.

[GF16] Loubna Ghammam and Emmanuel Fouotsa. *Adequate Elliptic Curve for Computing the Product of n Pairings*. Cryptology ePrint Archive, Report 2016/472. http://eprint.iacr.org/2016/472. 2016.

[Gt15] Torbjörn Granlund and the GMP development team. *GNU MP: The GNU Multiple Precision Arithmetic Library*. 6.1.0. http://gmplib.org. 2015.

[HSV06] F. Hess, N. P. Smart, and F. Vercauteren. "The Eta Pairing Revisited". In: *IEEE Transactions on Information Theory* 52.10 (2006), pp. 4595–4602. ISSN: 0018-9448. DOI: 10.1109/TIT.2006.881709.

[Jou04] Antoine Joux. "A One Round Protocol for Tripartite Diffie-Hellman". In: *Journal of Cryptology* 17.4 (Sept. 2004), pp. 263–276. DOI: 10.1007/s00145-004-0312-y.

[KB16] Taechan Kim and Razvan Barbulescu. "Extended Tower Number Field Sieve: A New Complexity for the Medium Prime Case". In: *CRYPTO 2016, Part I*. Ed. by Matthew Robshaw and Jonathan Katz. Vol. 9814. LNCS. Springer, Heidelberg, Aug. 2016, pp. 543–571. DOI: 10.1007/978-3-662-53018-4_20.

[Kha+17] 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: *ICISC 16*. Ed. by Seokhie Hong and Jong Hwan Park. Vol. 10157. LNCS. Springer, Heidelberg, 2017, pp. 208–219. DOI: 10.1007/978-3-319-53177-9_11.

[KN16] Md. Al-Amin Khandaker and Yasuyuki Nogami. "Isomorphic Mapping for Ate-Based Pairing over KSS Curve of Embedding Degree 18". In: *Fourth International Symposium on Computing and Networking, CANDAR 2016, Hiroshima, Japan, November 22-25, 2016*. IEEE Computer Society, 2016, pp. 629–634. ISBN: 978-1-5090-2655-5. DOI: 10.1109/CANDAR.2016.0113.

[KO62] A Karatsuba and Y Ofman. "Multiplication of many-digital numbers by automatic computers". In: *DOKLADY AKADEMII NAUK SSSR* 145.2 (1962), p. 293.

[Kob87] Neal Koblitz. "Elliptic curve cryptosystems". In: *Mathematics of computation* 48.177 (1987), pp. 203–209. DOI: 10.1090/S0025-5718-1987-0866109-5.

[Koc96] Paul C. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems". In: *CRYPTO'96*. Ed. by Neal Koblitz. Vol. 1109. LNCS. Springer, Heidelberg, Aug. 1996, pp. 104–113. DOI: 10.1007/3-540-68697-5_9.

[KSS07] Ezekiel J. Kachisa, Edward F. Schaefer, and Michael Scott. *Constructing Brezing-Weng pairing friendly elliptic curves using elements in the cyclotomic field*. Cryptology ePrint Archive, Report 2007/452. http://eprint.iacr.org/2007/452. 2007.

[Lan08] Hoes Lane. "Draft standard for identity-based public key cryptography using pairings". In: *IEEE P1636* 3 (2008), p. D1.

[LL97] Chae Hoon Lim and Pil Joong Lee. "A Key Recovery Attack on Discrete Log-based Schemes Using a Prime Order Subgroup". In: *CRYPTO'97*. Ed. by Burton S. Kaliski Jr. Vol. 1294. LNCS. Springer, Heidelberg, Aug. 1997, pp. 249–263. DOI: 10.1007/BFb0052240.

[LLP09] E. Lee, H.-S. Lee, and C.-M. Park. "Efficient and Generalized Pairing Computation on Abelian Varieties". In: *IEEE Trans. Information Theory* 55.4 (2009), pp. 1793–1803. DOI: 10.1109/TIT.2009.2013048.

[Mat+07] Seiichi Matsuda, Naoki Kanayama, Florian Hess, and Eiji Okamoto. *Optimised versions of the Ate and Twisted Ate Pairings*. Cryptology ePrint Archive, Report 2007/013. http://eprint.iacr.org/2007/013. 2007.

[Mor+14] Yuki Mori, Shoichi Akagi, Yasuyuki Nogami, and Masaaki Shirase. "Pseudo 8-Sparse Multiplication for Efficient Ate-Based Pairing on Barreto-Naehrig Curve". In: *PAIRING 2013*. Ed. by Zhenfu Cao and Fangguo Zhang. Vol. 8365. LNCS. Springer, Heidelberg, Nov. 2014, pp. 186–198. DOI: 10.1007/978-3-319-04873-4_11.

[NF05] Toru Nakanishi and Nobuo Funabiki. "Verifier-Local Revocation Group Signature Schemes with Backward Unlinkability from Bilinear Maps". In: *ASIACRYPT 2005*. Ed. by Bimal K. Roy. Vol. 3788. LNCS. Springer, Heidelberg, Dec. 2005, pp. 533–548. DOI: 10.1007/11593447_29.

[Nog+08] Yasuyuki Nogami, Masataka Akane, Yumi Sakemi, Hidehiro Katou, and Yoshitaka Morikawa. "Integer Variable chi-Based Ate Pairing". In: *PAIRING 2008*. Ed. by Steven D. Galbraith and Kenneth G. Paterson. Vol. 5209. LNCS. Springer, Heidelberg, Sept. 2008, pp. 178–191. DOI: 10.1007/978-3-540-85538-5_13.

[Nog+09] Yasuyuki Nogami, Yumi Sakemi, Takumi Okimoto, Kenta Nekado, Masataka Akane, and Yoshitaka Morikawa. "Scalar Multiplication Using Frobenius Expansion over Twisted Elliptic Curve for Ate Pairing Based Cryptography". In: *IEICE Transactions* 92-A.1 (2009), pp. 182–189. DOI: 10.1587/transfun.E92.A.182.

[Sak00] Ryuichi Sakai. "Cryptosystems based on pairing". In: *The 2000 Symposium on Cryptography and Information Security, Okinawa, Japan, Jan.* 2000, pp. 26–28.

[Sak+08] Yumi Sakemi, Yasuyuki Nogami, Katsuyuki Okeya, Hidehiro Katou, and Yoshitaka Morikawa. "Skew Frobenius Map and Efficient Scalar Multiplication for Pairing-Based Cryptography". In: *CANS 08*. Ed. by Matthew K. Franklin, Lucas Chi Kwong Hui,

and Duncan S. Wong. Vol. 5339. LNCS. Springer, Heidelberg, Dec. 2008, pp. 226–239.

[SCA86] Joseph H Silverman, Gary Cornell, and M Artin. *Arithmetic geometry*. Springer, 1986.

[Sco+09] Michael Scott, Naomi Benger, Manuel Charlemagne, Luis J. Dominguez Perez, and Ezekiel J. Kachisa. "On the Final Exponentiation for Calculating Pairings on Ordinary Elliptic Curves". In: *PAIRING 2009*. Ed. by Hovav Shacham and Brent Waters. Vol. 5671. LNCS. Springer, Heidelberg, Aug. 2009, pp. 78–88. DOI: 10.1007/978-3-642-03298-1_6.

[Sco11] Michael Scott. "On the Efficient Implementation of Pairing-Based Protocols". In: *13th IMA International Conference on Cryptography and Coding*. Ed. by Liqun Chen. Vol. 7089. LNCS. Springer, Heidelberg, Dec. 2011, pp. 296–308.

[SK03] Ryuichi Sakai and Masao Kasahara. *ID based Cryptosystems with Pairing on Elliptic Curve*. Cryptology ePrint Archive, Report 2003/054. http://eprint.iacr.org/2003/054. 2003.

[STO06] Masaaki Shirase, Tsuyoshi Takagi, and Eiji Okamoto. *Some Efficient Algorithms for the Final Exponentiation of η_T Pairing*. Cryptology ePrint Archive, Report 2006/431. http://eprint.iacr.org/2006/431. 2006.

[SW04] Amit Sahai and Brent Waters. *Fuzzy Identity Based Encryption*. Cryptology ePrint Archive, Report 2004/086. http://eprint.iacr.org/2004/086. 2004.

[Ver10] Frederik Vercauteren. "Optimal pairings". In: *IEEE Trans. Information Theory* 56.1 (2010), pp. 455–461. DOI: 10.1109/TIT.2009.2034881.

[Was03] Lawrence Washington. *Elliptic curves : number theory and cryptography*. Chapman & Hall/CRC, 2003. ISBN: 9780203484029.

[ZL12] Xusheng Zhang and Dongdai Lin. "Analysis of Optimum Pairing Products at High Security Levels". In: *INDOCRYPT 2012*. Ed. by Steven D. Galbraith and Mridul Nandi. Vol. 7668. LNCS. Springer, Heidelberg, Dec. 2012, pp. 412–430. DOI: 10.1007/978-3-642-34931-7_24.

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.