Doctoral Thesis

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

Author:
Md. Al-Amin Khandaker

Supervisor:
Dr. Yasuyuki Nogami

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

in the

Information Security Lab.
Graduate School of Natural Science and Technology

Okayama University

November 13, 2018

Declaration of Authorship

This dissertation and the work presented here for doctoral studies were conducted under the supervision of Professor Yasuyuki Nogami. I, Md. Al-Amin KHANDAKER, declare that this thesis titled, "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 Activity". .
- 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.
- In all works my coauthors contribution is acknowledged.
- The experiments and results presented in this thesis and in the articles where I am the first author were conducted by the myself.

Signed:

Date:

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

Albert Einstein

OKAYAMA UNIVERSITY

Abstract

Faculty of Engineering
Graduate School of Natural Science and Technology

Doctor of Philosophy

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

by Md. Al-Amin KHANDAKER

Acknowledgements

The last 3 and a half year is one of the best time of my life 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 counseling and unrelenting persuasion of my Ph.D. advisor Professor Yasuyuki Nogami. I am indebted to *Nogami Sensei* for having me in his lab *(Information Security Lab.)* as a doctoral student and mentoring me on this work. He taught me how to analyze complex problems from different perspectives and express the ideas from pen and papers to a fully publishable article. I enjoyed his insightful comments on the research topics during our discussions. Sometimes his in-depth queries bewildered me and influenced my ideas in this thesis. He guided me in different ways to approach a problem and the need to be persistent to accomplish my goal. His presence and off-work discussion makes 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 talking the "Theory of Distributed Algorithm" course taught by Professor Nobuo Funabiki. His strong passion for algorithmic problem solving during the lectures were 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 the deep-seated idea of the research works and japan life. His questions and suggestions for the time of half yearly progress meetings was very intuitive.

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

I would like to express my gratitude to Senior Assistant Professor Takuya Kusaka of *(Information Security Lab.)* for our in depth discussion of scientific topics. His strong work ethics and passion for research helped us to publish some of the remarkable collaborative works. His was always there to help while any difficulty arose for 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 *Information System Design Lab* and *(Information Security Lab.)* share space, we had encountered more often and share off research discussions. His comments during the progress report was enlightening.

I am also grateful to Assistant Professor Kengo Iokibe (*Optical and Electromagnetic Waves Laboratory*) 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 was not only helpful towards to final acceptability but also intriguing. My sincere gratitude 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 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 possible. I sincere 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 Faculty of Engineering who directly or indirectly made an impact in my doctoral course studies. My especial thanks to Ms. Yumiko Kurooka for kind supports in administrative documents.

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 Mashrufee Alam (Shama) 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 shoulders 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 Abbreviations

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

List of Notations and Symbols

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

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

Research Activities

- Journal Papers (Peer-Reviewed)

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

- International conferences (Peer-Reviewed)

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

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

- Domestic conferences

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

Bibliography

[1] Diego F Aranha et al. "Faster Explicit Formulas for Computing Pairings over Ordinary Curves." In: *Eurocrypt*. Vol. 6632. Springer. 2011, pp. 48–68.

[2] Diego F Aranha et al. "Implementing pairings at the 192-bit security level". In: *Pairing-Based Cryptography–Pairing 2012*. Springer, 2012, pp. 177–195.

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

[4] 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.

[5] Daniel V Bailey and Christof Paar. "Efficient arithmetic in finite field extensions with application in elliptic curve cryptography". In: *Journal of cryptology* 14.3 (2001), pp. 153–176.

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

[7] Razvan Barbulescu and Sylvain Duquesne. "Updating Key Size Estimations for Pairings". In: *Journal of Cryptology* (2018). ISSN: 1432-1378. URL: https://doi.org/10.1007/s00145-018-9280-5.

[8] 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.

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

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

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

[12] Paulo SLM Barreto et al. "Subgroup security in pairing-based cryptography". In: *International Conference on Cryptology and Information Security in Latin America*. Springer. 2015, pp. 245–265.

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

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

[15] 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.

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

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

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

[19] Craig Costello, Tanja Lange, and Michael Naehrig. "Faster pairing computations on curves with high-degree twists". In: *International Workshop on Public Key Cryptography*. Springer. 2010, pp. 224–242.

[20] Augusto Jun Devegili et al. "Multiplication and Squaring on Pairing-Friendly Fields." In: *IACR Cryptology ePrint Archive* 2006 (2006), p. 471.

[21] 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.

[22] 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.

[23] Laura Fuentes-Castañeda, Edward Knapp, and Francisco Rodríguez-Henríquez. "Faster Hashing to ${\mathbb G}_2$". In: *Selected Areas in Cryptography - 18th International Workshop, SAC 2011, Toronto, ON, Canada, August 11-12, 2011, Revised Selected Papers*. 2011, pp. 412–430. DOI: 10.1007/978-3-642-28496-0_25. URL: https://doi.org/10.1007/978-3-642-28496-0_25.

[24] Steven D Galbraith, Kenneth G Paterson, and Nigel P Smart. "Pairings for cryptographers". In: *Discrete Applied Mathematics* 156.16 (2008), pp. 3113–3121.

[25] Loubna Ghammam and Emmanuel Fouotsa. "Adequate elliptic curves for computing the product of n pairings". In: *International Workshop on the Arithmetic of Finite Fields*. Springer. 2016, pp. 36–53.

[26] Robert Granger and Michael Scott. "Faster squaring in the cyclotomic subgroup of sixth degree extensions". In: *International Workshop on Public Key Cryptography*. Springer. 2010, pp. 209–223.

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

[28] Gurleen Grewal et al. "Efficient implementation of bilinear pairings on ARM processors". In: *International Conference on Selected Areas in Cryptography*. Springer. 2012, pp. 149–165.

[29] 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.

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

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

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

[33] Koray Karabina. "Squaring in cyclotomic subgroups". In: *Mathematics of Computation* 82.281 (2013), pp. 555–579.

[34] Koray Karabina. "Squaring in cyclotomic subgroups". In: *Math. Comput.* 82.281 (2013), pp. 555–579.

[35] Hidehiro Kato et al. "Cyclic Vector Multiplication Algorithm Based on a Special Class of Gauss Period Normal Basis". In: *ETRI Journal* 29.6 (2007), pp. 769–778. DOI: 10.4218/etrij.07.0107.0040. eprint: https://onlinelibrary.wiley.com/doi/pdf/10.4218/etrij.07.0107.0040. URL: https://onlinelibrary.wiley.com/doi/abs/10.4218/etrij.07.0107.0040.

[36] Md Al-Amin Khandaker and Yasuyuki Nogami. "Isomorphic Mapping for Ate-Based Pairing over KSS Curve of Embedding Degree 18". In: *Computing and Networking (CANDAR), 2016 Fourth International Symposium on*. IEEE. 2016, pp. 629–634.

[37] Md Al-Amin Khandaker et al. "An Improvement of Optimal Ate Pairing on KSS Curve with Pseudo 12-Sparse Multiplication". In: *International Conference on Information Security and Cryptology*. Springer. 2016, pp. 208–219.

[38] Md. Al-Amin Khandaker et al. "Efficient Optimal Ate Pairing at 128-Bit Security Level". In: *Progress in Cryptology – INDOCRYPT 2017*. Ed. by Arpita Patra and Nigel P. Smart. Cham: Springer International Publishing, 2017, pp. 186–205.

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

[40] Neal Koblitz. "Elliptic curve cryptosystems". In: *Mathematics of computation* 48.177 (1987), pp. 203–209.

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

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

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

[44] Chae Lim and Pil Lee. "A key recovery attack on discrete log-based schemes using a prime order subgroup". In: *Advances in Cryptology—CRYPTO'97* (1997), pp. 249–263.

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

[46] Victor S Miller. "The Weil pairing, and its efficient calculation". In: *Journal of Cryptology* 17.4 (2004), pp. 235–261.

[47] Peter L Montgomery. “Speeding the Pollard and elliptic curve methods of factorization”. In: *Mathematics of computation* 48.177 (1987), pp. 243–264.

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

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

[50] Yasuyuki Nogami et al. “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.

[51] Yasuyuki Nogami et al. “Scalar multiplication using frobenius expansion over twisted elliptic curve for ate pairing based cryptography”. In: *IEICE transactions on fundamentals of electronics, communications and computer sciences* 92-A.1 (2009), pp. 182–189.

[52] Tatsuaki Okamoto and Katsuyuki Takashima. “Fully secure functional encryption with general relations from the decisional linear assumption”. In: *Annual Cryptology Conference*. Springer. 2010, pp. 191–208.

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

[54] 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.

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

[56] Akihito Sanada et al. *A Consideration of an Efficient Calculation over the Extension Field of Degree 4 for Elliptic Curve Pairing Cryptography*. 2016. URL: http://www.ieice.org/ken/paper/20160729yb97/eng/.

[57] Oliver Schirokauer. “The number field sieve for integers of low weight”. In: *Mathematics of Computation* 79.269 (2010), pp. 583–602.

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

[59] Michael Scott and Paulo S. L. M. Barreto. “Compressed Pairings”. In: *Advances in Cryptology - CRYPTO 2004*. 2004, pp. 140–156.

[60] Michael Scott et al. “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.

[61] A. Shamir. “Identity-based cryptosystems and signature schemes”. In: *Proceedings of CRYPTO 84 on Advances in cryptology*. Santa Barbara, California, United States: Springer-Verlag New York, Inc., 1984, pp. 47–53. ISBN: 0-387-15658-5.

[62] 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.

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

[64] Martijn Stam and Arjen K. Lenstra. "Efficient Subgroup Exponentiation in Quadratic and Sixth Degree Extensions". In: *Cryptographic Hardware and Embedded Systems - CHES 2002*. 2002, pp. 318–332.

[65] National Institute of Standards and Technology. http://csrc.nist.gov/publications/PubsSPs.html.

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

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

[68] André Weil et al. "Numbers of solutions of equations in finite fields". In: *Bull. Amer. Math. Soc* 55.5 (1949), pp. 497–508.

[69] Xusheng Zhang and Dongdai Lin. "Analysis of optimum pairing products at high security levels". In: *Progress in Cryptology - INDOCRYPT 2012*. Springer. 2012, pp. 412–430.

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.