Md. Al-Amin Khandaker

Google Scholar 0000-0001-7330-138X Research Gate AAD-2296-2020

Research Activities

Peer-reviewed journal and international conference papers as the first author.

1. **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, Nov. 2018, pp. 106–112. DOI: 10.1109/CANDAR.2018.00021. (Acceptance rate 28/77 ≈ 36%)

2. **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.

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. (Acceptance rate 19/75 ≈ 25%)

4. **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.

5. **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, Nov. 2016, pp. 208–219. DOI: 10.1007/978-3-31953177-9_11. (Acceptance rate 18/69 ≈ 26%)

6. **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. (Acceptance rate 31/61 ≈ 51%)

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, Nov. 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*, Dhaka, Bangladesh, 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. 2016, pp. 1–2. DOI: 10.1109/ICCE-TW.2016.7520894.

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: *32nd International Technical Conference on Circuits / Systems, Computers and Communications, ITC-CSCC 2017*, Busan, Korea, Jul. 2017, pp. 599-602, IEIE, CD-ROM (OS22-5).

Peer-reviewed journal and international conference papers as the 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. 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 in LNCS, Springer, Heidelberg], Aug. 2018. (Acceptance rate 22/44 = 50%)

14. 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.

15. 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, Nov. 2018, pp. 445–451. DOI: 10.1109/CANDARW.2018.00087.

16. 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*, Singapore, Oct. 2018, pp. 655 - 659. DOI: 10.23919/ISITA.2018.8664242.

17. 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 2018, pp. 1–2. DOI: 10.1109/ICCE-China.2018.8448768.

18. 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*, Singapore, Oct. 2018 pp. 660 - 664, DOI: 10.23919/ISITA.2018.8664405.

19. 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.

20. 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. (Acceptance rate 20/70 ≈ 29%)

21. 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. (Acceptance rate 27/53 ≈ 51%).

22. 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, Nov. 2017, pp. 445–450. DOI: 10.1109/CANDAR.2017.90.

23. 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, Nov. 2017, pp. 451–455. DOI: 10.1109/CANDAR.2017.86.

24. 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, Jun. 2017, pp. 137-138. DOI: 10.1109/ICCE-China.2017.7991033.

25. 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, Jun. 2017, pp. 287 - 288. DOI: 10.1109/ICCE-China.2017.7991108.

26. 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*, Busan, Korea, Jul. 2017, pp. 592-595, IEIE, CD-ROM (OS22-3).

27. 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.

Domestic conferences

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*, Yamagata, Oct. 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*, Okinawa, Jan. 2017, CD-ROM (B1-3).

30. Yuki Nanjo, **Md. Al-Amin Khandaker**, Masaaki Shirase, Takuya Kusaka, and Yasuyuki Nogami. "Attractive Classes of KSS Curves for Efficient Pairing". In: *Symposium on Cryptography and Information Security 2019 (SCIS)*, Shiga, Jan. 2019.

31. 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*, Nagano, Oct. 2018, CD-ROM (2A3-1).

32. Yuki Nanjo, **Md. Al-Amin Khandaker**, Masaaki Shirase, Takuya Kusaka, and Yasuyuki Nogami. "Determining BLS Curves for Pairing over Efficient Tower of Extension Field". In: *Technical Committee on Information Security (ISEC)*, Tokyo, May 2018, IEICE Tech. Rep., vol. 118, no. 30, ISEC2018-2, pp. 9-16, May 2018.

33. 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*, Niigata, Jan. 2018, CD-ROM (4D2-1).

34. 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*, Niigata, Jan. 2018, CD-ROM (4D2-3).

35. 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*, Niigata, Jan. 2018, CD-ROM (3B4-1).

36. 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*, Yamagata, Oct. 2017, CD-ROM (3E1-3).

Development Experiences

Product Planing and Development Engineer 2019.04-Current
Cardservice Inc., Tokyo, Japan

- Design, implement C++ based Linux application supporting EMVCo, QR-Code, FeliCa payment standards for payment terminals.
- Design, implement and analysis cryptography algorithms e.g. DUKPT, 3-DES for secure transaction between payment gateway, payment terminal and Point-Of-Sale(POS) machine.
- Implement C# based POS emulator to simulate different vendor's POS API.
- Used tools: C++, C, Java, C#.

Associate Software Engineer (iOS) 2014-2015
Metatude Asia Ltd. Dhaka, under business contract with Viadesk BV, The Netherlands

- Project Viadesk: A social intranet for private corporations. Responsibilities include making product specification, API design, implement and deploy native iOS client app.
- Project Coursepath: E-learning platform for private corporations to train their employees.
- Used tools: Objective-C, C, RESTful Services, Couchbase, SQLite.

Junior Software Engineer (iOS) 2012-2014
Metatude Asia Ltd. Dhaka under business contract with Viadesk BV, The Netherlands

- Project Viadesk: Develop mobile application Viadesk to imitate the web platform.
- Used tools: Objective-C, C, RESTful Services.