Md. Al-Amin Khandaker

curriculum vitae

CONTACT INFORMATION

Tokyo, Japan
+81-80-9791-8581
:alaminnipu

Homepage: https://al-amin.tech/
Linkedin: www.linkedin.com/in/khandakermd/
GitHub: https://github.com/eNipu/
✉ E-mail: khandaker@s.okayama-u.ac.jp

EDUCATION

Okayama University, Okayama, Japan 2015–2019

- Ph.D. in Public Key Cryptography, GPA: **4.0/4.0**.
- Advisor: Professor Yasuyuki Nogami.
- Ph.D. thesis: A Study of Efficient Pairing Computation Algorithm Using KSS Curves

Jahangirnagar University, Bangladesh. 2007–2012

- B.Sc., Computer Science and Engineering. GPA: **3.71/4** –163 credits, Rank: **4/40**.

JOB EXPERIENCE

- **Research Engineer, R&D** *EAGLYS Inc. Tokyo, Japan* 2020.11–present

  DataArmor GateDB: A database proxy application that enables users to perform SQL queries on encrypted data without storing to database server.
  - Key contributions:
    - Implemented Homomorphic-encryption(HE) to perform 'SQL aggregate functions'.
    - Reduced the bulk insertion and encryption time by 5 times by efficient implementation of HE algorithms and multi-processing in Rust.
    - Implemented Lifted-ElGamal over prime field as Somewhat-Homomorphic-Encryption (using BLS-12 elliptic curve pairing) for Homomorphic addition of cipher-text.
    - Improved the bulk data transmission using gRPC between client and the proxy.
  - *DataArmorGate AI:* allows to get inference from AI and ML models using encrypted data.
  - Key contributions:
    - Implemented the performance critical encryption module in C++ which speeds up the inference performance by 30%.
    - Implementation Homomorphic-Encryption Library bindings in the product.

- **Systems Development Engineer** *Cardservice Inc. Tokyo, Japan* 2019.04–2020.10
  - Designing and evaluating security architecture for payment systems.
  - Improving performance of the exiting product.

- **Associate Software Engineer** Metatude Asia Ltd. Dhaka, under Viadesk BV, The Netherlands 2012.05–2015.09
  - Project Viadesk: Designed and developed a mobile client of a intranet service.
  - Project Coursepath: Developed prototype of an online E-learning platform for private corporation.

TECHNICAL SKILLS

- *Programming Languages*:
  - Working proficiency: C/C++, Python
  - Limited working proficiency: Rust, C#, Java, Javascript, Objective-C
- *Software Engineering*:
  - Basic understanding of Scrum Framework, SOLID principle and common design patterns.
  - Working proficiency of VCS(Git), container technology (Docker).
  - Unix build system (CMake, Autotools), cloud service (Azure, AWS).
  - Working proficiency in SQL (PostgreSQL, MySQL).
  - Basic Linux system administration.

Research Experience

- 5+ years of academic and industry research experience in public-key-cryptography and secure computing while working on diverse applications from data analytics to machine learning.
- Currently working on designing and implementing PoC using the state-of-the-art research on Homomorphic-Encryption and Secure Computing for Big-Data analytic and Privacy-Preserving Machine Learning.
- Previously worked on mathematical optimization of pairing-based security protocols (BLS-signature) used in blockchain.

Research Profiles

- ResearchGate
- Google Scholar *[Complete publication list]*
- *ORCiD*

Selected Publications

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**, 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%)
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: *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%)
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: *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%)

Honors and Awards

- Dean's Scientific Award for Ph.D. thesis. 2019
- Japan Govt. MEXT scholarship for Doctor's course. 2015
- Bangladesh Govt. merit scholarship from grade 6 until undergraduate graduation in 2012.

References

Professor **Yasuyuki Nogami**
Okayama University
E-mail:yasuyuki.nogami@okayama-u.ac.jp

Professor **Takuya Kusaka**
Okayama University
E-mail:kusaka-t@okayama-u.ac.jp

Dr. **Claude Gravel**
EAGLYS Inc.
E-mail:claudegravel1980@gmail.com