Md. Al-Amin Khandaker

curriculum vitae

CONTACT INFORMATION

Berlin, Germany
+49-1577-3637166
tokhandaker@outlook.com
https://al-am.in
www.linkedin.com/in/khandakermd
https://github.com/eNipu

CAREER OBJECTIVE

Pursuing advanced cryptography R&D to drive secure data processing, leveraging my academic and professional background in Homomorphic encryption while expanding into Post-Quantum solutions.

PROFILE

- **PhD in Engineering** with 6+ years of experience in **data security and applied cryptography**, specializing in homomorphic encryption, secure multi-party computation, and identity management.
- Strong track record of **bridging academic research with industrial R&D**, delivering prototypes, PoCs, and secure product integrations in *cloud and mobile security* domains.
- **Hands-on development** in C/C++, Python, and Rust; **DevOps proficiency** using Docker, Kubernetes, GitLab CI and Terraform on Azure and AWS.
- **Excellent communication** and team leadership skills, with proven ability to collaborate on complex cryptographic solutions across diverse, multinational teams.

PROFESSIONAL EXPERIENCE

- **Cybersecurity Engineer**, *ITK Engineering GmbH, Berlin, Germany* 2024.1 – Present
  - Performed in-depth Threat Analysis & Risk Assessment, integrating cryptographic measures to comply with industry security standards (e.g., ISO/SAE 21434).
  - Developed and integrated cryptographic libraries (Mbed-TLS) across large-scale systems for secure data processing in diverse environments.
  - Prepared secure coding guidelines (aligned with SEI CERT) and performed code reviews to ensure robust security for embedded systems.
- **Secure Computing Engineer**, *EAGLYS Inc., Tokyo, Japan* 2020.11 – 2023.12
  - **R&D on Encrypted Data Processing**
    - Researched and implemented homomorphic encryption (Lifted-ElGamal on BLS curves) and secure multi-party computation for *DataArmor GateDB*—enabling SQL queries on encrypted data without exposing the decryption key.
    - Accelerated encryption/decryption by 17× through Rust and Python optimizations; improved system performance by 30%.
  - **Identity & Access Management**
    - Led design and implementation of an Attribute-Based Encryption (ABE) system, enabling fine-grained access control in cloud-based environments.
  - **Secure ML & Cloud Integration**
    - Advanced *DataArmor GateAI* to deliver encrypted AI inferences, migrating critical modules from Python to C++ for a 20% performance boost.
    - Streamlined secure CI/CD pipelines with Bazel, Skaffold, and Kubernetes.
- **Systems Development Engineer**, *Cardservice Inc., Tokyo, Japan* 2019.04 – 2020.11
  - Developed secure payment terminal software, focusing on cryptographic protocols and data integrity.
  - Created an in-house emulator for protocol testing between POS devices and payment gateways, improving reliability and reducing integration time.
- **Associate & Junior Software Engineer (iOS)**, *Metatude Asia Ltd.* 2012.05 – 2015.09
  - Built and iterated on the Viadesk iOS application, implementing secure data-sharing features and caching mechanisms.
  - Contributed to the early-stage development of Coursepath, an online e-learning platform that integrates secure authentication and data flows.

Skills

- **Programming Languages**:
  - Proficient in Python, Rust, C (focus on secure computing and cryptographic implementations).
- **Secure Computing & Cryptography**:
  - In-depth knowledge of public-key cryptosystems, homomorphic encryption, elliptic curves, and bilinear pairings.
- **DevOps & Cloud**:
  - Proficient with Docker, Kubernetes, GitLab CI, and Terraform; experience with Azure and AWS.
- **Languages**:
  - **English**: Fluent
  - **Japanese**: Conversational
  - **Bengali**: Native
- **Soft Skills**:
  - Leadership, Technical Writing, Public Speaking.

Education

Ph.D. in Engineering, Okayama University, Okayama, Japan 2015.10 – 2019.03

- *Thesis*: *A Study of Efficient Pairing Computation Algorithm Using KSS Curves.*
- Focused on **optimizing finite field operations** for elliptic curve pairings, with applications to attribute-based encryption and zero-knowledge proofs.

B.Sc. in Computer Science & Engineering, Jahangirnagar University, Bangladesh 2007 – 2012

- GPA: 3.71/4.00

Research Experience

- Conducted research in academia and industry (6+ years) on **applied cryptography**, including Homomorphic encryption, Secure multiparty computation and pairing-based cryptosystems.
- Optimized **Miller's Algorithm** for KSS & BLS pairing-friendly curves, benefiting cryptographic protocols (ABE, zero-knowledge proofs, etc.).
- Built prototypes and PoCs for secure data analytics and ML models (processing over encrypted data).

Research Profiles

Google Scholar ORCiD

Selected Publications

- Conference Proceedings: Progress in Cryptology, "Efficient Optimal Ate Pairing at 128-Bit Security Level". Dec. 2017, pp. 186–205. DOI: 10.1007/978-3-319-71667-1_10.
- Journal: IEICE Transactions on Discrete Mathematics, "An Improvement of Scalar Multiplication by Skew-Frobenius Map with Multi-Scalar Multiplication for KSS Curve". pp. 1838-1845. DOI: 10.1587/transfun.E100.A.1838

Honors and Awards

- Received Dean's Award for excellence in PhD thesis in 2019.
- Awarded MEXT scholarship by the Japanese government for doctoral studies in 2015.
- The Government of Bangladesh granted a continuous merit scholarship from grade 6 to the completion of undergraduate studies in 2012.