Md. Al-Amin Khandaker

curriculum vitae

Contact Information

Tokyo, Japan
+81-80-9791-8581
tokhandaker@outlook.com
https://al-am.in
www.linkedin.com/in/khandakermd
https://github.com/eNipu

Job Experience

- **Secure Computing Engineer,** *EAGLYS Inc., Tokyo, Japan* 2020.11 – present
  - Restructured system efficiency by implementing and improving secure computing protocols, leading to a 30% performance increase and significantly reduced IO bottlenecks.
  - Pioneered and optimized the development pipeline with Skaffold, K8s, Terraform, and Microsoft Azure while working in the following projects:
  - *DataArmor GateDB:* A novel database proxy application performing SQL queries on encrypted data without storing the key on the database server.
    - Implemented the application of Homomorphic-encryption for SQL aggregate functions in PostgreSQL server using C++.
    - Improved the encryption/decryption speed by 17x using Rust and Python.
    - Implemented and adopted Lifted-ElGamal as Somewhat-Homomorphic-Encryption using BLS curve for faster aggregate operation on 32-bit Integer.
    - Advanced the CI/CD pipeline using Bazel, Skaffold, GitLab CI, and Kubernetes.
  - *User Identity Management System:* A secure Identity Management Service offering fine-grained access control.
    - Led the building of this system using innovative Attribute-Based Encryption.
  - *Secure morphological analyzer for Japanese text:*
    - Designed the core security architecture, boosting the overall security of the system.
  - *DataArmor GateAI:* An innovative service delivering inferences from pre-trained Machine Learning models using encrypted data.
    - Improved inference performance by 20% by migrating performance-critical modules from Python to C++.

- **Systems Development Engineer,** *Cardservice Inc., Tokyo, Japan* 2019.04 – 2020.11
  - Engineered and refined user-friendly payment terminal software, enhancing the end-user experience and security.
  - Conceptualized and developed an in-house emulator, simulating communication protocols between POS machines and payment terminals.
  - Implemented cutting-edge security protocols including DUKPT and 3-DES in legacy payment gateway.

- **Associate Software Engineer (iOS),** Metatude Asia Ltd., Dhaka (under Viadesk BV, The Netherlands) 2014.04 – 2015.09
  - Led the development of the iOS app for Viadesk, enriching user interaction by implementing features like Appointments, Events, File sharing, and data caching.
  - Key contributor to the initial development stages of the web application for Coursepath, a novel online E-learning platform.

- **Junior Software Engineer (iOS),** Metatude Asia Ltd., Dhaka (under Viadesk BV, The Netherlands) 2012.05 – 2014.03
  - Played an instrumental role in Viadesk's iOS application development from scratch, UI modifications without storyboard, implementing new features, and fixing critical bugs.

Technical Skills

- *Programming Languages*:
  - Expertise: Python, Rust
  - Working experience: C++, Java, Javascript, SQL
  - Familiarity: Objective-C, C#, C
- *Software Engineering*:
  - Thorough understanding of Scrum Framework, SOLID principle, and common design patterns.

  - Proficient in using VCS (Git), Docker, K8s, GitLab-CI.
  - Solid experience with Unix build system (CMake, Autotools, Bazel), cloud services (Azure, AWS).
- *Cryptography*:
  - In-depth understanding of mathematical concepts related to Elliptic Curves, Finite Fields and Bi-linear Pairing.
- *Machine Learning and Data Science Frameworks*:
  - Basic understanding of Scikit-learn, TensorFlow, PyTorch, and several data analysis frameworks (NumPy, Pandas, Matplotlib).
- *Development and Operations (DevOps)*:
  - Proficient with Skaffold, Kubernetes, Docker, Git.
  - Familiarity with GitHub Actions, GitLab CI.
- *Soft Skills*:
  - Leadership, Project Management, Writing, Public Speaking.

Education

Ph.D. in Engineering, Okayama University, Okayama, Japan 2015.10.1–2019.03.25

- *Thesis*: A Study of Efficient Pairing Computation Algorithm Using KSS Curves
- Focused on Optimization Finite Field Operation for Elliptic Curve Pairing.
- Achieved a GPA of 4.0/4.0.
- Advisor: Prof. Yasuyuki Nogami.

Bachelor of Science in Computer Science, Jahangirnagar University, Bangladesh. 2007–2012

- GPA: 3.71/4.00 –163 credits, Rank: 4/40.

Research Experience

- I've spent more than five years working on research in both academia and the industry, with a focus on public-key cryptography and secure computing. My work has been applied to areas like data analytics and machine learning.
- At present, I'm working on a new database proxy application, where I'm using secure multi-party computation and homomorphic encryption.
- In the past, I optimized Miller's Algorithm for KSS and BLS pairing-friendly curves. These improvements have broader applications, benefitting cryptographic protocols such as attribute-based encryption and zero-knowledge proofs, beyond just the blockchain.

Research Profiles

ResearchGate 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.
- Granted continuous merit scholarship by the Government of Bangladesh from grade 6 until completion of undergraduate studies in 2012.