MD. AL-AMIN KHANDAKER

Software Engineer

@ tokhandaker@outlook.com +8180-9791-8581 Tokyo, Japan al-amin.dev linkedin.com/in/khandakermd
github.com/eNipu orcid.org/0000-0001-7330-138X

EXPERIENCE

Product Planing and Development Engineer

Cardservice Inc.

Apr 2019 – Present 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)

Metatude Asia Ltd. (Viadesk BV)

Apr 2014 – Sep 2015 Dhaka, Bangladesh

- 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)

Metatude Asia Ltd. (Viadesk BV)

May 2012 – Mar 2014 Dhaka, Bangladesh

- Project Viadesk:Responsibilities include understanding specification, API design and implement native iOS app.
- Used tools: Objective-C, iOS.

TECHNICAL SKILLS

C++, Objective-C
Java, C#, Python, JavaScript, C
iOS, GNU Autotools, Doxygen, LaTeX 2ε
Git, GitHub, SVN
Scrum
SOLID Principles
Linux System Administration, Design Patterns
Cryptography, Research

LANGUAGE SKILLS

- English: Fluent in business communication (TOEIC-890).
- Japanese: Basic conversational skill (JLPT-N4).
- Bengali: Native.

EDUCATION

Ph.D. in Engineering

Okayama University, Japan

Oct 2015-Mar 2019 Okayama, Japan

- Thesis title:"A Study of Efficient Pairing Computation Algorithm Using KSS Curves"

Bachelor of Science in Computer Science & Engineering

Jahangirnagar University

Mar 2008- Nov 2012 Dhaka, Bangladesh

- CGPA 3.71/4.00

Dean's scientific award for Ph.D. thesis.

MEXT scholarship for doctor's course.

Bangladesh Govt. merit scholarships.

PROJECTS

ELiPS

Efficient Library for Pairing-based Crypto-Systems.

- The project was targeted to make an UNIX configurable shared C/C++ library for cryptography researchers working on high-level protocols like homomorphic encryption.
- GitHub: github.com/eNipu/elips_bn_bls
- The similar BLS-381 curve is used in ethereum blockchain and Zcash(zk-SNARKs).
- Used tools: C, GNU MP Library, Autotools.

HackAPi

Guessing the password from time series data.

- The target of project was to check the security vulnerability of Raspberry pi 3B by taking voltage data of RSA decryption stage and apply side-channel-attack (chosen cipher text attack).
- Used tools: C, Raspberry pi 3B, oscilloscope.

PUBLICATIONS

Google Scholar's link

- **M.A-A Khandaker** et al. "Efficient Optimal Ate Pairing at 128-Bit Security Level". In: *INDOCRYPT 2017*. Ed. by A. Patra and N.P. Smart. Vol. 10698. LNCS. Springer, Dec. 2017, pp. 186–205. doi: 10.1007/978-3-319-71667-1_10.