Mahmudul FAISAL AL AMEEN

Post-Quantum Cryptography · Side-Channel Security · Formal Verification

1 Place de Suse, Orsay 91400
France
☎ *(+33)06.83.71.91.38*
✉ *mahmudul.faisalalameen@cea.fr*
🌐 *github.com/phaysaal* □

Professional Summary

Research engineer and formal-methods specialist with 10+ years of experience building **industry-grade static analysis tools** for memory safety, information-flow security, and **constant-time verification of cryptographic implementations**. **At CEA List (France)**, I had a major contribution in research on **side-channel security of post-quantum cryptography (PQC)**:

- Systematic timing-leak analysis of NIST Post-Quantum Digital Signature Scheme (PQDSS) candidates
- Scalable constant-time verification tools applied to classical and emerging PQC primitives
- 2025 publication & presentation at the **NIST PQC Standardization Conference**, Gaithersburg, MD

Previously developed separation-logic-based verifiers at National University of Singapore, National Institute of Informatics (Japan), and University of Tokyo, with tools used in autonomous-driving software and open-source library security projects.

Core Skills

Post-Quantum Cryptography & Side-Channel Security: Systematic timing-leak analysis of NIST PQDSS candidates; constant-time verification of classical and PQC cryptographic primitives; timing/cache analysis.

Formal Methods & Program Analysis: separation logic; symbolic execution; abstract interpretation; information-flow/non-interference; constant-time reasoning.

Programming Languages & Tools: Functional (OCaml *10+ years*, Haskell, Scala) and imperative (C/C++, Java, Python; Rust *working knowledge*); LLVM reverse engineering.

Research → Industry Transfer: Converting formal methods theory into CI-integrated static analysis tools and prototypes used in cryptography, autonomous driving, and open-source libraries.

Online Reference

Google Scholar	https://scholar.google.com/citations?user=8nWNePkAAAAJ
LinkedIn	https://www.linkedin.com/in/faisalalameen/

Professional Experiences

Academic & Research (full-time)

2023/05–Present **Research Engineer**, *Software Safety & Security Lab (LSL)*, The French Alternative Energies and Atomic Energy Commission, Saclay, France

- Investigated side-channel vulnerabilities in classical and post-quantum cryptographic implementations.
- Improved scalability of static analysis for constant-time verification, applying methods to both widely used and emerging cryptographic primitives.

2021/04–2023/3 **Researcher**, *Department of Computer Science, The University of Tokyo*, Tokyo, Japan

- Worked on an autonomous vehicle software (Autoware) verification project.
  - Structure discovery in LLVM code and reverse engineering to C-like structured programs and functional programs.
- Developed a transformation algorithm for fixpoint logic formula by asynchronous unfold/fold with tool development.

2019/04–2021/3 **Researcher**, *National Institute of Informatics*, Tokyo, Japan

- Expressiveness of separation logic.
- Collaborated in development of a separation logic based analysis tool for verification of memory safety of C programs.
  - approximation of loop count
  - analysis with biabduction for array, list, and string
  - function pointer elimination

2016/11–2019/03 **Research Fellow**, *Department of Computer Science, School of Computing, National University of Singapore*, Singapore

- Collaborated on the cyber security project ‘Securify’ funded by NSF, Singapore
- Separation logic based information flow analysis for program security
  - developed a system to verify that a program does not leak secured information directly or indirectly.
  - developed a security specification synthesis tool for the open source C library 'glibc’.
- Co-lectured post-graduate and undergraduate courses:
  - Programming languages concepts and programming language implementation
- Advised postgraduate thesis

2013/1–2014/9 **Senior Lecturer**, *Department of CSE, University of Liberal Arts Bangladesh*, Dhaka, Bangladesh

- Courses taught:
  - Structured and object-oriented programming (C, C++, Java)
  - Algorithm
  - Automata and the theory of computing, and compiler design
- Developed multi-agent systems tools for research on road traffic analysis (under ULAB Research Grant)
- Advised three graduate theses and the ULAB Computer Club

Education

2016 **PhD in Informatics**, *The Graduate University for Advanced Studies*, Kanagawa, Japan

Thesis title: Completeness of Verification System with Separation Logic for Recursive Procedures

- A new complete Hoare’s logic system for recursive procedures
- A separation logic based system with completeness to verify correctness pointer programs with recursive procedures
- Expressiveness of the assertion language for the programming language.

2007 **MS in Computer Science**, *East West University*, Dhaka, Bangladesh, *3.91 out of 4.00*

`Thesis title: FCompSynth, A Toolkit for Various Automatic Matching and Synthesis of Variable Sized Analog and Digital VLSI Component`

- ○ An analog VLSI synthesizer is designed and developed to increase production efficiency
- ○ An artificial neural network simulator is developed as an academic toolkit
- ○ A scripting language is designed and implemented to describe analog VLSI devices

2006 **BSc(Engr) in Computer Science and Engineering**, *Darul Ihsan University*, Dhaka, Bangladesh, *3.91 out of 4.00*

`Thesis title: Ranaar, A Bangla Formattable SMS Mobile Software`

- ○ Segmentized complex font developement for device with low memory
- ○ A SMS formatting system is designed and developed
- ○ A lossless and a lossy data compression algorithms are invented

Selected Recent Publications

2025 Olivier Adjonyo, S. Bardin, E. Bellini, G. Dione, M. Faisal Al Ameen, R. Merget, F. Recoules, Y. Sellami, "Systematic Timing Leakage Analysis of NIST PQDSS Candidates: Tooling and Lessons Learned," PQC Standardization Conference, 2025.

2024 D. Kimura, M. Tatsuta, M. Faisal Al Ameen, et al., "Bi-Abduction in Separation Logic with Arrays and Lists for Program Analysis," Computer Software, Vol 41, Issue 1, 2024.

2024 M. Faisal Al Ameen, N. Kobayashi, R. Sato, "Asynchronous unfold/fold transformation for fixpoint logic," Science of Computer Programming, Vol. 231, 2024.

2022 M. Faisal Al Ameen, N. Kobayashi, R. Sato, "Asynchronous Unfold/Fold Transformation for Fixpoint Logic," FLOPS 2022.

2018 A. Prabawa, M. Faisal Al Ameen, B. Lee, W.-N. Chin, "A Logical System for Modular Information Flow Verification," VMCAI 2018.

2016 M. Faisal Al Ameen, M. Tatsuta, "Completeness for recursive procedures in separation logic," Theoretical Computer Science, Vol 631, 2016.

Additional Publications and Theses

Book

Dr. Md. Zahedul Hassan, PSO, BAEC, Bangladesh and Mahmudul FAISAL AL AMEEN, Dept. of CSE, Darul Ihsan University, *Java Project: Games and Database Programming*, published by Sahana Yasmin (Bobby), Dhaka, Bangladesh, ISBN: 984-32-2543-0, 2006

Journals

[2019] Makoto Tatsuta, Wei-Ngan Chin, Mahmudul FAISAL AL AMEEN, *Completeness and expressiveness of pointer program verification by separation logic*, *Information and Computation*, Vol 267, August 2019, Pages 1-27, ISSN 0890-5401

[2014] Nusrat Jahan Farin and Mahmudul FAISAL AL AMEEN, *An Efficient Technique for Inter/Intra Network Handover Process*, *ULAB Journal of Science and Engineering*, Vol 5, Page 2-6, 2014

[2007] Mahmudul FAISAL AL AMEEN, Mohammad Shorif Uddin, *An Educational Toolkit for Artificial Neural Network*, Journal of Electronics and Computer Science (ISSN: 1680-6743) 9(1), Jun 2007

Theses

[2016] Mahmudul FAISAL AL AMEEN, Dept. of Informatics (NII), SOKENDAI (The Graduate University for Advanced Studies), *Completeness of Verification System with Separation Logic for Recursive Procedures*, 2016

[2007] Mahmudul FAISAL AL AMEEN, Dept. of CSE, East West University, Bangladesh), *FCompSynth, A Toolkit for Various Automatic Matching and Synthesis of Variable Sized Analog and Digital VLSI Component*, 2007

[2006] Mahmudul FAISAL AL AMEEN, Dept. of CSE, Darul Ihsan University, Dhaka, Bangladesh, *Ranaar, A Bangla Formattable SMS Mobile Software*, 2006

Conferences

[2022] Daisuke Kimura, Mahmudul FAISAL AL AMEEN, Makoto Tatsuta, Mirai Ikebuchi, Koji Nakazawa, *Biabduction for Separation Logic with Arrays and Lists*, 2022, Workshop on Programming and Programming Language (PPL2022), Japan

[2021] Daisuke Kimura, Mahmudul FAISAL AL AMEEN, Makoto Tatsuta, Koji Nakazawa, *Function Pointer Eliminator for C Programs*, 2021, 19th Asian Symposium on Programming Languages and Systems, Chicago, IL, USA, pp. 23-37, doi: 10.1007/978-3-030-89051-3_2

[2014] Farhan Quadir, Mahmudul FAISAL AL AMEEN, Sifat Momen, *Visualization and Queuing Analysis of Spatio-Temporal Traffic Data*, 2014 17th International Conference on Computer and Information Technology (ICCIT), Dhaka, 2014, pp. 223-228. doi: 10.1109/ICCITechn.2014.7073106

[2009] Makoto Tatsuta, W.N. Chin, FAISAL AL AMEEN, Mahmudul, *Completeness of Pointer Program Verification by Separation Logic*, 2009 Seventh IEEE International Conference on Software Engineering and Formal Methods, Hanoi, 2009, pp. 179-188. doi: 10.1109/SEFM.2009.33

[2007] Mahmudul FAISAL AL AMEEN, Md. Didar Islam, Syed Akhter Hossain, *Algorithms for Synthesis and Average Distribution of Variable Sized MOS Components for Efficient Analog VLSI Devices*, 2007 10th International Conference on Computer and Information Technology, Dhaka, 2007, pp. 1-5, doi: 10.1109/ICCITECHN.2007.4579437

[2006] Mahmudul FAISAL AL AMEEN, Md. Ashfaq Islam, Md. Foysal Mamun, and Md. Zahedul Hassan, *Introducing Vector Segmented Bangla Font (FZVSBF) For Small Handheld devices*, 2006 International Conference on Electrical and Computer Engineering, Dhaka, 2006, pp. 201-204. doi: 10.1109/ICECE.2006.355325

Research Grant Received

ULAB Research Grant Award 2013
University of Liberal Arts Bangladesh, Dhaka, Bangladesh

Recent Talks & Presentations

2025 "Systematic Timing Leakage Analysis of NIST PQDSS Candidates: Tooling and Lessons Learned" at the NIST PQC Standardization Conference, Gaithersburg, MD.

2022 "Asynchronous Unfold/Fold Transformation for Fixpoint Logic" at the FLOPS Conference, 2022

2016 "New Complete System of Hoare's Logic with Recursive Procedures", Constructivism and Computability, JAIST Logic Workshop Series 2015, Kanazawa, Japan

Professional Membership

- Member, International Association for Cryptologic Research (IACR)
- Member, Association for Computing Machinery (ACM)
- Member, NIST Post-Quantum Cryptography Forum mailing list (2023–present)
- Reviewer, PTCC national funding call on "Formal Verification and Hardware Side-Channel Security", France, 2025

Awards Received

NII Scholarship, 2007
National Institute of Informatics, Tokyo, Japan

Imdad Sitara Khan Scholarship, 2006, *Imdad Sitara Khan Foundation, USA*
East West University, Dhaka, Bangladesh

Extra-curricular Activities

Programming Activities

Programming Contests ACM ICPC 2006, Coimbatore, India, ACM ICPC 2004, Dhaka, Bangladesh, ACM ICPC 2002, Kanpur, India

Selected Developed Software/tools

- **SLAC** A static analysis tool for detecting memory errors in C program
- **HASTOR** A graphical tool to semi-automatic image data extraction
- **FCompSynth** A graphical tool for analog VLSI layout auto arrangements and synthesis

Hobby

Arts and Photography **Solo photography** exhibition and painting of **Birangona** at the Art Competition on Liberation War at Jhenidah Cadet College, Bangladesh in 1999

Debate Participated in **Debate on environment**, at Tokyo International Exchange Center, Tokyo, Japan in 2008