Phong Le

Cryptographer/Software Developer

Experienced cryptographer, security researcher with extensive knowledge in the security and privacy aspects in the payment industry. Interested in bridging the gap between research and applied cryptography.

Personal Website
GitHub
Google Scholar
Email: leducphong@gmail.com
Phone: +1 (506)471-4591

Education

PhD. in Applied cryptography
University of Pau et des Pays de l'Adour

Skills

Cryptography
Data Security
Data Privacy
Java, C/C++,
Python

Strengths

Critical thinking
Self-starter
Attention to details
Prioritizing
Collaboration

Experience

Nokia / Senior Software Engineer
2025 – present

Bank of Canada / Cryptographer
2021 - 2024

- Bringing cryptographic expertise to security and privacy of digital currencies, including MPC, ZKP, post-quantum cryptography, white-box cryptography and Hardware security
- Introducing security & privacy principles in designing a secure CBDC system
- Published: privacy-preserving post-quantum credentials, Blockchain-based Fintech

Canadian Institute for Cybersecurity / Research Team Lead
2019 – 2021

- Led a R&D team working on cybersecurity R&D projects: anomaly detection (with IBM Canada), and evaluation of synthetic data (with TD Bank) by developing relevant statistical methods and AI models
- Developed a fault attack against lightweight block ciphers: DFA_Simeck
- Introduced a new multisignature scheme for blockchain

Institute for Infocomm Research (I2R) / Scientist II
2017 – 2019

- Designed and implemented a blockchain-based assets and processes tracking. Introduced a blockchain-based IOT forensics framework
- Cryptanalyzed the block ciphers Present, SIMON using algebraic and fault analysis attacks

UL Transaction Security / Senior Cryptanalyst
2016 – 2017

- Evaluated the security of cryptographic implementations (ECC, RSA, MAC Algo 3) on payment smartcards under EMVCo framework. Delivered 10+ security evaluation projects
- Implemented t-test assessing side-channel leakage of a cryptographic implementation

National University of Singapore / Research Scientist
2010 – 2016

- Conducted research on paring-based and elliptic curve cryptography by introducing new efficient algorithms, generating new (pairing-friendly) elliptic curves
- Designed and implemented algorithms to prevent side-channel analysis, e.g., ECDSA

University of Caen / Postdoctoral Fellow
2009 – 2010

- Conducted research on paring-based e-cash
- Introduced a novel algorithm to compute cryptographic pairing