Phong Le

Cryptographer/Security Researcher

Experienced cryptographer 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
Publications
Email: leducphong@gmail.com
Phone: (506)471-4591

Education

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

B.S. in Computer Science
National University of Vietnam

Skills

Cryptography

Zero-Knowledge Proof

MPC, FHE, ECC

C/C++/Python/Rust/

Solidity

Strengths

Critical thinking

Self-motivated

Prioritizing

Collaboration

Experience

Bank of Canada / Cryptographer

2021 - present

- Bringing cryptographic expertise to security and privacy of digital currencies, including MPC, ZKP, signatures, post-quantum and white-box cryptography
- Introducing security & privacy principles in designing a secure CBDC system
- Introduced privacy-preserving post-quantum credentials

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)
- Developed a fault attack against lightweight block ciphers: DFA_Simeck
- Introduced a new multisignature scheme for blockchain
- Mentored junior researchers and developers in the projects

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: BIFF
- Analyzed the security of block ciphers Present, Speck, SIMON

UL Transaction Security / Senior Cryptanalyst

2016 – 2017

- Evaluated the security of cryptographic implementations on payment smartcards under EMVCo framework.

National University of Singapore / Research Scientist

2010 – 2016

- Conducted research on paring-based and elliptic curve cryptography.
- Designed algorithms to prevent side-channel analysis. publications
- Designed and implemented secure implementation of ECDSA

University of Caen / Postdoctoral Fellow

2009 – 2010

- Conducted research on paring-based e-cash.