LUDIVINE ESTHER MOOH

Busan, South Korea

esther.ludivine@gmail.com | github.com/Ludest27/Portfolio

Summary

Master's student in Information Security with experience in post-quantum cryptography, and implementation-level optimization. Presented research on ML-KEM and lightweight cryptography at international venues. Research interests include post-quantum cryptography, secure multiparty computation, and privacy-preserving cryptographic protocols.

Education

Master of Science in Information Security

Pukyong National University, South Korea | Sep 2023 – Aug 2025 (expected)

GPA: 4.4 / 4.5 Scholarship: Global Korea Scholarship

- **Thesis:** Toward Practical Post-Quantum Cryptography for IoT: Ascon and Macro-based Optimization of ML-KEM
- **Relevant coursework:** Cryptography on Chip, Finite Field Theory, PKI, Digital Forensics, Advanced System Programming, Data Structures & Algorithms

Graduate Certificate in Cybersecurity

La Trobe University, Australia (Online) | 2020 – 2021

Network Security, Cryptography, Penetration Testing, Cyber Law

Bachelor of Science in Political Science

University of Nebraska Omaha, USA | 2015 – 2017

GPA: 3.5 / 4.0, Cum Laude Scholarships: International Student, Miller Family

- Summer Program: Cybersecurity and Cyberwarfare, Leiden University, The Hague (2016)

Research & Experience

Student Researcher – Security System Semiconductor Lab

Pukyong National University | Sep 2023 – Present

- **ML-KEM Performance Optimization Research**
  - Investigated optimization methods for ML-KEM, identifying modular reduction as a performance bottleneck
  - Implemented optimization by replacing modular reduction function calls with macros to reduce execution overhead

- Achieved performance improvements, reducing latency by 18-21% in key generation, encapsulation, and decapsulation
- Used Valgrind profiling, C/C++, and Linux-based environments for performance analysis
- Analyzed security vulnerabilities in Falcon and Kyber, including fault injection and constant-time attack risks in compilers like Clang

- **ML-KEM Optimization for Resource-Constrained Environments**

  - Focused on optimizing ML-KEM for use in IoT and embedded devices
  - Replaced Keccak with Ascon , reducing code size and memory usage by 24%
  - Worked with cryptographic libraries such as PQM4 and OpenSSL, testing implementations in a Linux environment

Contributor – Agence Nationale de la Cybersécurité (ANCy)
Togo (Remote) | Jan 2024 – Present

- Contributed to the development of national cybersecurity audit and qualification frameworks
- Authored incident response guides and supported diaspora expert consultations

Legal Research Intern – Cabinet Maître Moreira
Lomé, Togo | Mar 2018 – Aug 2018

- Conducted research on cyber harassment and digital privacy law
- Analyzed threat patterns and drafted memoranda for legal teams

Publications & Presentations

- “Enhancing ML-KEM Performance Through Macro-Based Modular Reduction Optimization,” MITA 2024, Taipei – Main Author & Presenter
- “ECC Accelerator Using Faster Montgomery Ladder on FPGA Devices,” Busan Cybersecurity Conference 2024 – Presenter

Technical Skills

- Languages: C/C++, Bash, Python
- Cryptography: ML-KEM, RSA, ECC, Ascon (lightweight cryptography)
- Security Tools: Wireshark, FTK Imager, Nmap, Autopsy, Volatility, John the Ripper
- Development Tools: Git, Valgrind, OpenSSL, Docker, GDB
- Platforms: Linux (Ubuntu, WSL), Windows
- Hardware & Optimization: PQM4 framework, STM32, cycle-level benchmarking

- Analysis: Timing analysis, compiler-induced leakage, side-channel testing, fault injection

Security Training

TryHackMe (25+ rooms completed)

- Memory Forensics (Digital Forensics)
- Linux Privilege Escalation (System Security)
- Tor Investigation (Privacy/Anonymity)
- OWASP Top 10 (Web Security)
- Red Team Recon (Penetration Testing Basics)

Languages

French (Native) | Mina (Native) | English (Fluent) | Korean (Intermediate) | Spanish (Beginner-Intermediate)