TUNG LE, PhD Candidate

Last update: March 19, 2025

Contact Information

Gilbert Place, Room 4306
220 Gilbert Street
Blacksburg, VA, 24060

Email: tungle@vt.edu
Cell: (+1) 540-876-9641
LinkedIn: https://linkedin.com/in/thanhtungle/

Research Interests

My Ph.D. research focuses on Applied Cryptography, Security, and Privacy with special interests in Searchable Encryption (SE), Multiparty Computation (MPC), Oblivious RAM (ORAM), and Proof of Retrievability (PoR). I am also passionate about designing hardware accelerators using FPGA and GPU technologies, particularly for applications in AI and Cryptography.

Education

Virginia Tech, Blacksburg, Virginia, United States — Aug 2021 – May 2026 (Expected)
PhD student, Computer Science
- Dissertation: Trustworthy, Privacy-Preserving and Functional Data Outsourcing Systems
- Advisor: Dr. Thang Hoang
- GPA: 3.96/4

Hanoi University of Science and Technology (HUST), Hanoi, Vietnam — Aug 2014 – June 2019
Engineer's Degree (equivalent to BS degree), School of Information and Communications Technology (SoICT)
- Thesis: *Research and Implementing Fusion Algorithms on FPGA*
- GPA: 3.83/4 – Valedictorian Graduation Honor (Ranked 1st out of 626)

Professional Experiences

Graduate Research Assistant, Computer Science, Virginia Tech, Blacksburg, VA — Aug 2021 – current

Graduate Teaching Assistant, Computer Science, Virginia Tech, Blacksburg, VA — Aug 2021 – current

Ph.D. SWE Intern, Meta Platforms, Inc., Menlo Park, CA, USA — May 2025 – Aug 2025

FPGA Engineer, Viettel High Tech Industries Corp., Hanoi, Vietnam — Aug 2019 – July 2021

FPGA Engineer Intern, Viettel High Tech Industries Corp., Hanoi, Vietnam — July 2018 – June 2019

Embedded Engineer Intern, Viettel High Tech Industries Corp., Hanoi, Vietnam — July 2017 – Dec 2017

Publications

[1] **Tung Le** and Thang Hoang, "Hermes: Efficient and Secure Multi-Writer Encrypted Database", in *The 46th IEEE Symposium on Security and Privacy* (IEEE S&P 2025), May 2025, San Francisco, CA, USA. (*Acceptance rate: 14.8%*)

[2] **Tung Le**, Rouzbeh Behnia, Jorge Guajardo, and Thang Hoang, "MUSES: Efficient Multi-User Searchable Encrypted Database", in *The 33rd USENIX Security Symposium* (USENIX Security 2024), August 2024, Philadelphia, PA, USA. (*Acceptance rate: 18.3%*)

[3] **Tung Le** and Thang Hoang, "MAPLE: A Metadata-Hiding Policy-Controllable Encrypted Search Platform with Minimal Trust", in *The 23rd Privacy Enhancing Technologies Symposium* (PETS 2023), July 2023, Lausanne, Switzerland. (*Acceptance rate: 21.8%*)

[4] **Tung Le**, Pengzhi Huang, Attila A. Yavuz, Elaine Shi, and Thang Hoang, "Efficient Dynamic Proof of Retrievability for Cold Storage", in *The 30th Annual Network and Distributed System Security Symposium* (NDSS 2023), February 2023, San Diego, CA, USA. (*Acceptance rate: 16.2%*)

[5] **Tung Le**, Bang Le, Thuy Pham, Hoan Nguyen, and Huy Vuong, "Implement Detail Enhancement Algorithm on FPGA for Real-Time and Energy-Efficient Embedded Systems", in *The 8th IEEE International Conference on Communications and Electronics* (IEEE ICCE 2020), January 2021, Phu Quoc, Kien Giang, Vietnam. (*Acceptance rate: 49.7%*)

Awards and Honors

- 2023 CCI SWVA Cyber Innovation Scholar 2023
- Advanced Labor Performance, Viettel High Tech Industries Corp., Hanoi, Vietnam 2020
- SoICT Valedictorian Graduation Honor, HUST, Hanoi, Vietnam 2019
- Best Presentation Award in Thesis Defense, SoICT, HUST, Hanoi, Vietnam 2019
- HUST Excellence Scholarship Award for AY 2018–2019, HUST, Hanoi, Vietnam 2018
- HUST Excellence Scholarship Award for AY 2017–2018, HUST, Hanoi, Vietnam 2017
- Excellent Student Award in AY 15-16, HUST, Hanoi, Vietnam (Top 20 out of 25k students) 2016
- Scholarships for Excellent Academic Record, HUST, Hanoi, Vietnam 2014–2016

Teaching Experience

I have instructed students and graded assignments and exams in the following courses at Virginia Tech:

- CS5594 - Blockchain Technologies (Graduate Level): Spring 2024 (53 students)
- CS5584 - Network Security (Graduate Level): Fall 2023 (46 students)
- CS1044 - Introduction to Programming in C (Undergraduate Level): Spring 2022 (69 students)
- CS3114 - Data Structures and Algorithms (Undergraduate Level): Fall 2021 (414 students), Fall 2024 (481 students)

Professional Services

Conference Reviewer: ACSAC (2022–2024), PETS (2024), USENIX (2025)

Journal Reviewer: IEEE Transactions on Information Forensics and Security (2024), IEEE Transactions on Dependable and Secure Computing (2025)

Talks

Trustworthy, Privacy-Preserving and Functional Data Outsourcing Systems

- Ph. D. Preliminary Exam, Virginia Tech — Blacksburg, VA, USA, Dec 2024

MUSES: Efficient Multi-User Searchable Encrypted Database

- Presented at USENIX Security 2024 — Philadelphia, PA, USA, Aug 2024

MAPLE: A Metadata-Hiding Policy-Controllable Encrypted Search Platform with Minimal Trust

- Presented at PETS 2023 — Remote, July 2023

Poster: Efficient Dynamic Proof of Retrievability for Cold Storage

- Presented at CCI Student Researcher Showcase 2023 — Blacksburg, VA, USA, Apr 2023

Efficient Dynamic Proof of Retrievability for Cold Storage

- Presented at ISOC NDSS 2023 — San Diego, CA, USA, Mar 2023

Implement Detail Enhancement Algorithm on FPGA for Real-Time and Energy-Efficient Embedded Systems

- Presented at IEEE ICCE 2020 — Phu Quoc, Kien Giang, Vietnam, Jan 2021

Research Experience

Graduate Research Assistant 2021–Present

Department of Computer Science, Virginia Tech, Blacksburg, VA

- Develop algorithms and implement searchable encrypted systems using C/C++ including:
  - Hermes: a multi-writer searchable encrypted database that can prevent keyword-guessing attacks, optimal search complexity (sublinear in the size of keyword set) and forward privacy with user efficiency. My developed source code is publicly available at https://github.com/vt-asaplab/Hermes.
  - MUSES: a multi-server searchable encrypted system with multi-writer support. It hides all statistical information including search, result and volume patterns while achieving a minimal user overhead for keyword search and key rotation. My artifact has been awarded all three badges (available, functional, reproducible) in USENIX Security 2024: https://secartifacts.github.io/usenixsec2024/results.
  - MAPLE: a multi-server searchable encryption design attaining a high level of security. It protects search, result and volume patterns with malicious security, supports multiple users, also optimizes server computation complexity. My developed library is publicly available at https://github.com/vt-asaplab/MAPLE.
- Develop and implement Porla using MATLAB, C/C++ and Golang. Porla is a proof of retrievability protocol using error-correcting code and verifiable computation techniques, including Bulletproofs and KZG. My developed library is publicly available at https://github.com/vt-asaplab/porla.

FPGA Engineer 2019–2021

Viettel High Technology Industries Corporation, Hanoi, Vietnam

- Develop, integrate and write testbenches for IP cores of 5G Physical layer: implement IP core for resource mapping of PDCCH; integrate Xilinx Polar encoder to accelerate bit processing of PBCH and PDCCH; optimize, test and debug the overall 5G downlink system including PBCH, PDCCH, PDSCH and CSI-RS on boards VCU-118 (Xilinx) and 21DR (Viettel) (achieved download speed ≈ 1 Gbps and supported 8 concurrent users per time slot); test and debug IP cores and the overall system using Xilinx's tools: Vivado Simulator, Virtual Input/Output (VIO) and Integrated Logic Analyzer (ILA).
- Develop IP core for Digital Detail Enhancement algorithm to enhance the quality of infrared images, including multiple stages of convolutions and computations based on the histogram of the input image; test and debug on Xilinx Zedboard/Zybo Z7.
- Develop IP core interfacing with Quad SPI Flash module to read data from flash memory and write it to DRAM directly, which can speed up the system booting process by approximately 5× (delay decreases from 42s to 8s); test and debug on board Neso Artix 7.
- Adapt Linux kernel modules and C libraries from Intel x86 architecture to ARMv8 platform of NXP.

Research Student 2018–2019

Computer System Lab, SoICT, HUST, Hanoi, Vietnam

- Implement Fusion Algorithms on FPGA, test and debug on boards DE2i-150 and DE1-SoC.
- Develop Linux device driver on Ubuntu 14.04 for board DE2i-150 to transfer data between FPGA and DRAM memory (Intel Atom Processor) via PCIe bus using DMA/SG-DMA.
- Develop IP core to transfer data from GNSS receiver circuit to PC via EZ-USB FX2LP module.

Technical Skills

- **Programming Languages**: C/C++, Python, MATLAB, Golang, Verilog, Git, Bash, LaTeX
- **Embedded System Development**: Microcontroller programming (PIC, AVR), Digital design
- **Operating System/Software**: Linux (Ubuntu/CentOS), Vivado, HLS, System Generator, Tcl script, Quartus, Altera DSP Builder, Simulink, GDB
- **Algorithm Design**: Searchable Encryption, Verifiable Computation, Multiparty Computation
- **Network Programming and Multithreading/IPC**: TCP/UDP, Mutex/Semaphore, Shared Memory/Message Queue (POSIX and System V)