

# Zhenyu Lei

zhenyu.lei@163.com | (+86) 19907351616 | [Personal Homepage](#) | [GitHub](#)

## EDUCATION

**Southeast University (SEU)**, Nanjing, China

*M.S. in Cyberspace Security* GPA: 88 / 100

Jun 2026 Expected

- Awards: SEU Second Prize Postgraduate Academic Scholarship (2024), SEU Career Development Camp (1st Prize, 2024)

- Relevant Courses: New Progress on Cyber Security (Top 1%), AI & Machine Learning, Pattern Recognition

*B.S. in Cyber Science (Honors Program for Gifted Youth)* GPA: 3.66 / 4

Sep 2019 – Jul 2023

- Awards: SEU Outstanding Student (Top 15 annually, 2023), SEU Outstanding Undergraduate Thesis Award (2023), SEU Outstanding Volunteer (2022), SEU Outstanding Youth (Top 10 annually, 2021), SEU Jiao Tingbiao Scholarship (2020)

- Relevant Courses: Computer Architecture, Chip Security Attack & Protection, Operating System Design, Software Security (95), Compilation Method; Programming & Algorithmic Language (96), Probability & Statistics (93), Mathematical Analysis

## RESEARCH INTERESTS

My primary research interest lies in **Hardware Fuzzing** for **Microarchitectural Security**, aiming to 1) automate the process of finding leakage primitives, 2) exploit them via side-channels, and 3) develop defenses against these attacks. Furthermore, I am currently exploring **AI-driven approaches** to assist in the discovery of unknown microarchitectural vulnerabilities.

## PUBLICATIONS

[1] **Zhenyu Lei** and Fei Tong. “Semantics-Guided Black-Box Fuzzing for Microarchitectural Vulnerabilities in Processors”, manuscript in preparation.

[2] **Zhenyu Lei** and Fei Tong. “ParaFuzz: A Parallel Fuzzing Framework for Multi-Core Processors”, manuscript in preparation.

[3] Xiaoyu Cheng, Fei Tong, **Zhenyu Lei**, Fang Jiang, Zhe Zhou and Trevor E. Carlson. “Exploiting Hidden Resource Contention in Selective Speculation Defenses”, under review at *IEEE Symposium on Security and Privacy (S&P)*, 2026.

## RESEARCH EXPERIENCE

### I. HARDWARE FUZZING

#### Security Attack Modeling for Processor Microarchitectures

Jun 2025 – Present

*Project Lead* | Funded by the Cyber Security Association of China (¥ 60,000)

- Formulating a comprehensive **Systematization of Knowledge (SoK) on microarchitectural vulnerabilities** to address the challenge of inconsistent vulnerability abstractions in current research.
- Systematically modeling main-stream **microarchitectural vulnerability characteristics** and extracting common **exploitation principles** to establish a unified taxonomy for processor security evaluation.
- **Delivering Core Contributions**: 1) a SoK on Microarchitectural Vulnerabilities; 2) a Systematic Modeling Report defining standard attack primitives; and 3) a Portable Benchmark Suite for cross-platform security validation.

#### Semantics-Guided Black-Box Fuzzing for Microarchitectural Vulnerabilities in Processors

Mar 2025 – Present

*Master's Thesis* | Advisor: Prof. Fei Tong

- Developing a novel fuzzing framework that models **inter-instruction dependencies** to systematically discover unknown microarchitectural vulnerabilities, overcoming the coverage limitations of blind fuzzing.
- Architecting a hybrid engine that leverages **semantics-guided fuzzing** to optimize instruction sequences via both data-flow and control-flow analysis, coupled with model checking for precise **vulnerability localization**.
- **Delivering Core Contributions**: 1) a Semantics-Guided Fuzzing Strategy for efficient instruction exploration; 2) a novel Coverage Feedback Mechanism established by dynamically maintaining Side-Channel Attack Templates; and 3) Model-Checking Techniques for Vulnerability Localization.

### II. MICROARCHITECTURAL ATTACKS

#### Exploiting Hidden Resource Contention in Selective Speculation Defenses

May 2025 – Nov 2025

*Core Researcher* | Under Review at IEEE S&P 2026 | Advisor: Prof. Fei Tong

- Uncovered novel **side-channel vulnerabilities** in SOTA **selective speculation defenses** (e.g., STT, DOLMA); revealed that overlooked arithmetic instructions and predicated execution (e.g., REP MOVSB) can induce Reservation Station (RS) contention to bypass protections.
- Engineered a **custom LLVM-based leakage detection framework** utilizing novel inter-procedural taint tracking to systematically trace sensitive data propagation, thereby automating the identification of explicit and implicit RS contention gadgets within real-world software such as OpenSSL and Libgcrypt.
- Leveraged the vulnerable gadgets identified by the automated framework to **construct end-to-end side-channel exploits** on commercial hardware, successfully recovering encryption keys from the OpenSSL `aria_set_encrypt_key` function on Intel Cascade Lake (Xeon Gold 6248R) with high precision.

#### Aware+Fuzz: A Cache Side-Channel Mitigation Architecture for RISC-V Processors

Apr 2023 – Aug 2023

*Team Lead* | **3rd Prize**, National College Student Information Security Contest | Advisor: Prof. Fei Tong

- Led the development of **Aware+Fuzz**, a novel two-module architecture for **mitigating cache side-channel attacks** on RISC-V processors. Aware+Fuzz consists of an Aware Attack Module (AAM) and a Fuzz Observation Module (FOM):
  - AAM dynamically detects speculative execution-based side-channel threats;
  - FOM predicts attacker access patterns during the observation phase and proactively disrupts potential exploits through strategic data prefetching.

- Validated on RISC-V hardware and gem5, demonstrating **robust defense against Spectre attacks** with negligible overhead (<1% on SPEC CPU 2017) and seamless hardware compatibility.

### Spectre Attack Mitigation on RISC-V Processors

Dec 2022 – Jun 2023

*Undergraduate Thesis Research | Outstanding Undergraduate Thesis, Southeast University | Advisor: Prof. Fei Tong*

- Reproduced Spectre v1 attacks on RISC-V processors and systematically analyzed microarchitectural side-channel vulnerabilities.
- Introduced Flush Key Load (FKL), a **novel detection metric for identifying abnormal cache access patterns indicating Spectre-like behavior**; validated its effectiveness on gem5 and Chipyard.
- Designed a **dual-layer defense strategy** which uses FKL to trigger coordinated hardware-software mitigation; benchmark results demonstrated the strategy's **robust resistance to Spectre v1 attacks** with only ~2% performance overhead.

### III. HIGH-PERFORMANCE SYSTEMS

#### High-performance Register File Design

Apr 2025 – Jul 2025

*Team Lead | 2nd Prize (Cadence Track), China Postgraduate IC Innovation Competition | Advisor: Prof. Fei Tong*

- Designed a parallel register file (15W5R, 256×32 bit) with dual-cycle read and single-cycle write timing, implementing **address pre-decoding and parallelized priority encoding strategies** to reduce arbitration complexity for shortening the critical path.
- Established an **automated verification pipeline** to ensure RTL and gate-level consistency through cycle-accurate comparisons against reference models.
- Applied timing-driven optimizations (e.g., retiming and min-delay constraints) using **Cadence Genus and Innovus** to achieve timing closure at 300 MHz operating frequency.
- Conducted dynamic/static power analysis using **Cadence Joules** with SDF back-annotation and switching activity waveforms.

#### Design and Implementation of an In-order, Five-stage Pipelined RISC-V Processor

Sep 2022 – Jun 2023

*Independent Project | Institute of Computing Technology, Chinese Academy of Sciences*

- Designed and implemented a **tape-out ready RISC-V SoC**, key modules including Instruction Decode Unit (IDU), Arithmetic Logic Unit (ALU), data/instruction memory, General Purpose Registers (GPRs), and Control and Status Registers (CSRs).
- Optimized module interfaces and pipeline control logic to ensure **full 5-stage in-order pipeline functionality** (IF, ID, EX, MEM, WB), supporting precise exception handling and instruction flow consistency.
- Built a verification platform integrating an interactive debugger and DiffTest with NEMU to ensure cycle-level correctness, validating **system robustness** by successfully booting complex workloads like *Super Mario Bros* at 24 FPS.

#### Privacy-Preserving Cross-System Voiceprint Recognition and Protection

Aug 2022 – Jun 2023

*Researcher | Funded by Institute of Information Engineering, Chinese Academy of Sciences (¥12,000) | Advisor: Ben Niu*

- Proposed a lightweight, privacy-preserving framework to mitigate **critical biometric vulnerabilities**, including voiceprint leakage, spoofing, and identity theft in mobile environments.
- Developed a **Vector Quantization (VQ)** recognition pipeline by extracting Linear Predictive Coding (LPC) **acoustic features** and generating **user-specific voiceprint templates** via the LBG algorithm.
- Optimized **deployment for resource-constrained mobile platforms**, achieving high recognition precision with low computational and memory overhead in real-world experiments.

#### SuriVPP: A High-Performance Virtualized Intrusion Prevention System

Jul 2021 – Nov 2021

*Core Member | 1st Place, National Undergraduate Extracurricular Sci&Tech Competition | Advisor: Prof. Sanfeng Zhang*

- Engineered SuriVPP, a high-performance IPS coupling Suricata with **Vector Packet Processing (VPP)** to resolve kernel-user context switch bottlenecks, enabling high-speed user-space packet processing on ARM/x86 platforms.
- Developed a **custom zero-copy VPP plugin** that embeds the Suricata engine directly into the VPP thread, eliminating inter-process communication overhead; re-engineered memory management using **lock-free ring buffers and CPU affinity** to maximize cache locality.
- Achieved **3× native performance (6 Gbps)** with ultra-low latency (**19.89 μs**, ~22% of the national standard) on Kunpeng servers, verifying the system's stability via Dockerized cross-platform deployment.

### SKILLS & QUALIFICATIONS

**Programming Languages:** C, C++, Rust, Python, Shell, Verilog, System Verilog, Scala, Tcl

**Frameworks & Tools:** Simulators (gem5, Chipyard), Benchmarks (SPEC CPU 2017, PARSEC), EDA Tools (Cadence Genus, Innovus, Joules)

**Language:** English (Proficient), Mandarin (Native)

### LEADERSHIP & COMMUNITY SERVICE

#### Director | Academic Exchange Center, Graduate Student Union of SEU

Sep 2023 – Jun 2024

- Orchestrated 10+ high-profile academic and literacy lectures, featuring distinguished guests including Nobel laureates and academicians; managed all planning, guest coordination, hosting, and technical execution.
- Directed the exclusive pre-screening and exchange event for a film Beyond the Clouds; authored a promotional article that gained 62,000+ views, becoming the Union's top-viewed post in 2023.

#### Member | SEU Youth Volunteer Association

Sep 2020 – Jun 2021

- Devoted over 500 hours to various volunteer activities, including serving at the 9th International Congress of Chinese Mathematicians (ICCM 2022), leading campus tours, etc.

### REFERENCES

- Associate Professor Fei Tong, Southeast University Email: ftong@seu.edu.cn
- Professor Liquan Chen, Southeast University Email: lqchen@seu.edu.cn
- Associate Professor Lining Peng, Southeast University Email: pengln@seu.edu.cn