Chuqi Zhang

Singapore chuqiz@u.nus.edu chuqiz.notion.site Chuqi Zhang icegrave0391

Research Interests

My research focuses on the design of secure system software, spanning operating systems, hypervisors, and trusted execution environments (TEEs). I aim to build trustworthy and efficient system foundations for emerging application domains, such as SaaS, FaaS, and agentic AI platforms.

Currently, I work on enhancing confidential computing architectures, particularly confidential virtual machines (CVMs) and user-land library operating systems (LibOS). My goal is to extend CVM isolation for sandboxes and confidential containers, improving the security, reliability, and efficiency of cloud infrastructures and AI code agents. In parallel, I work on virtualization-based system monitoring designs for client-side isolation and privacy, including 1) privacy-preserving secure video gaming PC architectures and 2) LLM-powered code semantics-assisted OS-level exploit detection/investigation frameworks.

Education

National University of Singapore (NUS) — *Singapore*
Ph.D., School of Computing (Computer Science) — *Aug 2021 – Present*

- Advisor: Dr. Zhenkai Liang

Arizona State University (ASU) — *Tempe, AZ, USA*
Visiting Ph.D., School of Computing and Augmented Intelligence — *Mar 2024 – Dec 2024*

- Advisor: Dr. Adil Ahmad (Since *Nov 2022*)

Huazhong University of Science and Technology (HUST) — *Wuhan, HUB, China*
B.S. in Computer Science, ACM class — *Sept 2017 – June 2021*

- GPA: 3.95/4.0
- **Thesis:** Refining Audit Provenance based on Hardware-assisted Execution-flow Tracing

Experience

Research Scientist Intern — *Redmond, WA, USA*
Microsoft Research (MSFT Research) — *June 2025 – Sept 2025*

- Worked on Rust-based Library-OS design for sandboxing untrusted AI agent execution.
- Research intern – Systems for Scalable and Reliable AI Agents.
- Mentors: Dr. Jay Bosamiya, Dr. Weiteng Chen, and Dr. Weidong Cui.

Visiting Researcher — *Shenzhen, GD, China*
Southern University of Science and Technology (SUSTech) — *May 2023 – June 2023*

- Worked on secure enclave based on ARM Confidential Computing Architecture (CCA).
- Mentor: Dr. Fengwei Zhang.

Research Assistant Intern — *Remote*
Georgia Institute of Technology (GaTech) — *Sept 2020 – Nov 2020*

- Worked on selective symbolic execution for malware & ransomware analysis.
- Mentor: Dr. Brendan Saltaformaggio.

Software Engineer Intern — *Shenzhen, GD, China*
Tencent — *Jul 2020 – Sept 2020*

- Worked on iOS QQ client application development.

- Mentor: Ace Tang.

Publications (* denotes co-first authors)

- Efficient Fine-Grained Kernel Auditing using Augmented Reference Behavior Analysis and Virtualized Selective Tracing (To Appear).

Chuqi Zhang, Spencer Faith, Feras Al-Qassas, Theodorus Wensan Februanto, Zhenkai Liang, Adil Ahmad

*IEEE Symposium on Security and Privacy (***IEEE S&P***) 2026.*

- DevOps-Gym: Benchmarking AI Agents in Software DevOps Cycle (To Appear).

Yuheng Tang*, Kaijie Zhu*, Bonan Ruan, **Chuqi Zhang**, Michael Yang, Hongwei Li, Suyue Guo, Tianneng Shi, Zekun Li, Christopher Kruegel, Giovanni Vigna, Dawn Song, William Yang Wang, Lun Wang, Yangruibo Ding, Zhenkai Liang, Wenbo Guo

*International Conference on Learning Representations (***ICLR***) 2026.*

- Enhanced Differential Testing in Emerging Database Systems.

Yuancheng Jiang, Jianing Wang, **Chuqi Zhang**, Roland Yap, Zhenkai Liang, Manuel Rigger

*ACM International Conference on the Foundations of Software Engineering (***ACM ESEC/FSE***) 2026.*

- Erebor: A Drop-In Sandbox for Private Data Processing in Untrusted Confidential Virtual Machines.

Chuqi Zhang, Rahul Priolkar, Yuancheng Jiang, Yuan Xiao, Mona Vij, Zhenkai Liang, Adil Ahmad

*European chapter of ACM SIGOPS (***ACM EuroSys***) 2025.*

- Propagation-Based Vulnerability Impact Assessment for Software Supply Chains.

Bonan Ruan, Zhiwei Lin, Jiahao Liu, **Chuqi Zhang**, Kaihang Ji, Zhenkai Liang

*IEEE/ACM International Conference on Automated Software Engineering (***IEEE/ACM ASE***) 2025.*

- Fuzzing the PHP Interpreter via Dataflow Fusion.

(Distinguished Paper Award)

Yuancheng Jiang, **Chuqi Zhang**, Bonan Ruan, Jiahao Liu, Manuel Rigger, Roland Yap, Zhenkai Liang

*USENIX Security Symposium (***USENIX Security***) 2025.*

- The HitchHiker's Guide to High-Assurance System Observability Protection with Efficient Permission Switches.

Chuqi Zhang, Jun Zeng, Yiming Zhang, Adil Ahmad, Fengwei Zhang, Hai Jin, Zhenkai Liang

*ACM Conference on Computer and Communications Security (***ACM CCS***) 2024.*

- KernJC: Automated Vulnerable Environment Generation for Linux Kernel Vulnerabilities.

(Best Practical Paper Award)

Bonan Ruan, Jiahao Liu, **Chuqi Zhang**, Zhenkai Liang

*International Symposium on Research in Attacks, Intrusions and Defenses (***ACM RAID***) 2024.*

- PalanTír: Optimizing Attack Provenance with Hardware-enhanced System Observability.

Jun Zeng*, **Chuqi Zhang***, Zhenkai Liang

*ACM Conference on Computer and Communications Security (***ACM CCS***) 2022.*

Ongoing Projects

- A Privacy-Preserving Video Gaming Architecture with Lightweight Virtualization and Graphics Rendering Passthrough.

- A Deployment-Friendly and Memory-Optimized Confidential Serverless Platform for Modern Clouds.

- Shoot the Honey, Cloak the Player: Towards Zero-Runtime-Overhead Proactive Defense and Detection for Visual Game Cheating.

Workshop Papers

- Towards Trusted Extensible Device Measurement and Management via Intra-Firmware Privilege Isolation.

Chuqi Zhang, Bonan Ruan, Vikram Ramaswamy, Zhenkai Liang, Adil Ahmad

1st Workshop on Operating System Research for Connected Intelligence (co-located with ASPLOS / EuroSys'25).

- Towards a Lightweight Key-Enforced Data Race Detector for Commodity Kernels.

Rahul Priolkar, **Chuqi Zhang**, Adil Ahmad

The Network and Distributed System Security (NDSS) Symposium 2025.

Teaching

CS5231 "System security" *NUS*

- Teaching assistant (Fall 2022; Fall 2023)

CS5331 "Web security" *NUS*

- Teaching assistant (Spring 2022; Spring 2023)

Honors and Awards

Research Achievement Award (2025/2026)	*NUS*
Usenix Security Distinguished Paper Award (2025)	*USENIX*
RAID Best Practical Paper Award (2024)	*RAID*
Outstanding Graduate (2021)	*HUST*
Dean's List Scholarship (2019)	*HUST*
Outstanding Student Scholarship (2018, 2017)	*HUST*

Invited Talks

Towards Trusted Extensible Device Measurement and Management via Intra-Firmware Privilege Isolation.

- 1st WOSCI (March 2025). *Rotterdam, Netherlands*

Erebor: A Drop-In Sandbox for Private Data Processing in Untrusted Confidential Virtual Machines.

- Microsoft Research - Security & Privacy Workshop (July 2025). *Redmond, WA, USA*
- ACM EuroSys 2025 (March 2025). *Rotterdam, Netherlands*

The HitchHiker's Guide to High-Assurance System Observability Protection with Efficient Permission Switches.

- Microsoft Research - Security Reading Group (June 2025). *Redmond, WA, USA*
- ACM CCS 2024 (October 2024). *Salt Lake City, UT, USA*

PalanTír: Optimizing Attack Provenance with Hardware-enhanced System Observability.

- ACM CCS 2022 (November 2022). *Los Angeles, CA, USA*

Services

NUS Student Area Search Committee (ASC), Chair of Security Area, 2025

PC member: TIFS'25

External reviewer: NDSS'23; USENIX Security'24; S&P'24; EuroSys'25; HPCA'25; OSDI'25; S&P'25

Sub reviewer: CODASPY'25