*Last updated in Mar 2026*

# Chuqi Zhang

Singapore | chuqiz@u.nus.edu | chuqiz.com | Chuqi Zhang | icegrave0391

## Research Interests

My research focuses on the design of resilient and scalable system infrastructure, spanning operating systems (OS), hypervisors, and confidential computing. My goal is to make next-generation AI services (agents, copilots, SaaS/FaaS, and LLM inference endpoints) trustworthy, efficient, and scalable.

Currently, I design lightweight sandbox primitives that let AI agents and LLM training execute safely and efficiently, including a Rust-based LibOS for agent sandboxing (LiteBox), and confidential-VM containers for private data processing (Erebor). In parallel, I work on the systems layer of confidential AI infrastructure.

Previously, I built AI-based applications/evaluations, such as LLM-driven code semantics analysis for OS-level exploit analysis (Appare), and benchmarking AI agents across the software DevOps cycle (DevOpsGym). I also worked on eBPF-based efficient OS observability pipeline / system auditing 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

## Experience

**Research Scientist Intern** — *Redmond, WA, USA*
*Microsoft Research (MSFT Research)* — *June 2025 – Sept 2025*
- Worked on Rust-based OS design for sandboxing untrusted AI agents (LiteBox).
- 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.**

**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.**

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.**

Santosh Narayanan, **Chuqi Zhang**, Sangho Lee, Zhenkai Liang, Adil Ahmad

*Preprint (undersubmission) 2026.*

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

Vikram Ramaswamy, **Chuqi Zhang**, Adil Ahmad

*Preprint (undersubmission) 2026*.

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

Jianing Wang, **Chuqi Zhang**, Yuancheng Jiang, Adil Ahmad, Shanqing Guo

*Preprint (undersubmission) 2026*.

## 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