Chao Yin

PhD Candidate in Computer Security

Vrije Universiteit Amsterdam & CWI Amsterdam

c.yin@vu.nl

I am a fourth-year PhD candidate in computer security. My research focuses on secure computation, SAT-based security analysis, and distributed system security. I have co-led two research projects resulting in co-first-author publications at ACM CCS 2024 and ACSAC 2022, on Byzantine fault-tolerant and privacy-preserving sensor fusion and incentive attacks in proof-of-work mining pools, respectively. In parallel, I am developing my own research directions in secure data aggregation for sensor networks and SAT-based function recovery attacks on gate-hiding garbled circuits.

For my research, I conducted large-scale AWS cloud experiments with hundreds of distributed nodes to evaluate correctness, robustness, and performance. I also run SAT experiments encoding circuits with 700+ variables to break gate-hiding schemes.

Education

Vrije Universiteit Amsterdam & CWI Amsterdam — *Amsterdam, Netherlands*
PhD in Computer Science — *Oct 2022 - present*

- Advisors: Prof. Fabio Massacci (VU, Amsterdam) and Prof. Marten van Dijk (CWI, Amsterdam)
- Daily supervisor: Dr. Chenglu Jin, Tenured Researcher (CWI, Amsterdam)

Chongqing University of Technology — *Chongqing, China*
MS in Computer Science — *Sep 2019 - Jul 2022*
BS in Computer Science — *Sep 2015 - Jul 2019*

- Advisor: Prof. Zheng Yang (currently at Southwest University)

Research Visits & Internships

Tsinghua University & Shanghai Jiao Tong University — *Beijing / Shanghai, China*
Research Visit / Intern — *Jul 2024 - Aug 2024*

- Hosted by Prof. Sisi Duan (THU), Prof. Haibin Zhang and Prof. Shengli Liu (SJTU / Yangtze Delta Institute)

Singapore University of Technology and Design (SUTD) — *Singapore*
Visiting Graduate Research Student — *Nov 2020 – May 2021*

- Advisor: Prof. Jianying Zhou

Publications

Published

Chao Yin, Haihong Tian, Zheng Yang, Haibin Zhang, Fabio Massacci, Chenglu Jin. CRSF: Collusion-Resilient Privacy-Preserving Sensor Fusion with Byzantine-Robust Participation. **ISC 26**.
First author. Proposed a collusion-resilient privacy-preserving sensor fusion protocol combining garbled circuits, Byzantine-fault-tolerant broadcast, and secret sharing. Developed a stronger adversarial model that captures collusion between malicious sensors and a malicious server, while preventing a single server from manipulating sensor participation and protecting private sensor inputs.

Chenglu Jin, **Chao Yin (co-first)**, Marten van Dijk , Sisi Duan, Fabio Massacci, Michael K. Reiter, Haibin Zhang. PG: Byzantine

fault-tolerant and privacy-preserving sensor fusion with guaranteed output delivery. **ACM CCS 24** .
Co-first author. Contributed to the theoretical formulation and security analysis of privacy-preserving sensor fusion under Byzantine faults. Co-designed and implemented two protocol variants and conducted large-scale AWS cloud experiments to evaluate correctness, robustness, and performance.

Zheng Yang, **Chao Yin (co-first and corresponding author)**, Junming Ke, Tien Tuan Anh Dinh, Jianying Zhou. If you can't beat them, pay them: Bitcoin protection racket is profitable. **ACSAC 22**.
Co-first and corresponding author. Developed the game-theoretic security analysis of incentive attacks in proof-of-work mining pools, formulated the attack profitability model, and conducted all experiments to validate the theoretical results.

Zheng Yang, **Chao Yin (corresponding author)**, Chenglu Jin, Jianting Ning, Jianying Zhou. Lightweight delegated authentication with identity fraud detection for cyber-physical systems. Cyber-Physical System Security Workshop. **ACM CPSS 21**.

Zheng Yang, Tien Tuan Anh Dinh, **Chao Yin (corresponding author)**, Yingying Yao, Dianshi Yang, Xiaolin Chang, Jianying Zhou. LARP: A lightweight auto-refreshing pseudonym protocol for V2X. **ACM SATMAT 22**.

Preprints / Under Review

Chao Yin, Zunchen Huang, Chenglu Jin, Marten van Dijk, Fabio Massacci. (2026). Function Recovery Attacks in Gate-Hiding Garbled Circuits using SAT Solving.
Proposed SAT-based function recovery attacks against gate-hiding garbled circuits, where the circuit topology is known but gate functionalities are hidden. Developed formal attack models, topology-preserving simplification techniques, and optimized attack procedure to recover the target functionality through adaptive oracle queries. Implemented the attack framework and evaluated it on benchmark circuits.

Chao Yin, Zunchen Huang, Chenglu Jin, Marten van Dijk, Fabio Massacci. Quantifying Function Privacy in XOR-Revealed Gate-Hiding Garbled Circuits.

Awards, Fellowships, & Grants

2022-2026	**China Scholarship Council PhD Fellowship** Full doctoral fellowship awarded through national competitive selection.
2021	**University Scholarship for Overseas Study** Competitive funding for a six-month overseas research visit.
2019-2021	**Graduate Academic Excellence Scholarships** Merit-based scholarships awarded annually during my master's program for academic performance within the top cohort of the department.

Teaching and Supervision

2024, 2026	**Security and Safety Engineering. Teaching Assistant** Graded assignments, assisted students with security and safety engineering concepts, and provided feedback on coursework.
2024-2026	**Master's Student Supervision: Haihong Tian, Southwest University** Supervised research on secure computation and privacy-preserving sensor fusion, including research problem formulation, literature review, and experimental design.