Zhuo Cai ✉ zcaiam@connect.ust.hk
🌐 https://zhuocai.github.io

Education

2023 – Now

Hong Kong University of Science and Technology, Hong Kong
PhD in Computer Science and Engineering
Co-Supervised by Amir Goharshady & Dimitris Papadopoulos
Research Interest: Cryptography, Distributed Systems, Formal Verification, Mechanism Design, Theoretical Computer Science.

2021 – 2023

Hong Kong University of Science and Technology, Hong Kong
Master of Philosophy in Computer Science and Engineering
Supervisor: Amir Goharshady
GPA: 3.88/4.0

2017 – 2021

Tsinghua University, Beijing
Bachelor of Automation
GPA: 3.81/4, GPA Ranking: 17/168

2019 Fall

National University of Singapore, Singapore
Visiting Undergraduate Researcher
GPA: 4.0/4

Research Publications

Note: (1) My advisor Amir Goharshady adopts the convention in theoretical computer science to order authors alphabetically. (2) '*' indicates a co-first author.

Publications using Alphabetical Order

1. Barakbayeva, T., **Cai, Z.**, Goharshady, A. & Keypoor K. (2025). Smart Contracts for Trustless Sampling of Correlated Equilibria. In IJCAI. code - SNARK part
2. Abidha V., Barakbayeva T., **Cai, Z.**, & Goharshady, A. (2024). Gas-efficient decentralized random beacons. In IEEE ICBC.
3. Barakbayeva T., **Cai, Z.**, & Goharshady, A. (2024). SRNG: an efficient decentralized approach for secret random number generation. In IEEE ICBC.
4. **Cai, Z.**, Farokhnia, S., Goharshady, A., & Hitarth, S. (2023). Asparagus: Automated synthesis of parametric gas upper-bounds for smart contracts. In OOPSLA. Asparagus code
5. Ballweg, J., **Cai, Z.**, & Goharshady, A. (2023). PureLottery: Fair leader election without decentralized random number generation. In IEEE Blockchain. PureLottery code
6. **Cai, Z.**, & Goharshady, A. (2023). Trustless and bias-resistant game-theoretic distributed randomness. In IEEE ICBC.
7. **Cai, Z.**, & Goharshady, A. (2023). Game-theoretic Randomness for Proof-of-Stake. In MARBLE.

Publications using Contribution Order

1. He, X.*, **Cai, Z.** *, Wei, W., Zhang, Y., Mou, L., Xing, E., & Xie, P. (2021). Towards visual question answering on pathology images. In ACL.

Manuscripts in submission & Ongoing projects

1. **Cai, Z.**, & Goharshady, A. Proof of Election: A Formally-Verified Democratic Blockchain Protocol.
2. Updatable batched lookup argument: polylogarithmic update cost for prover.
3. Efficient parallel smart contracts in DAG consensus.

Miscellaneous Experience

Awards and Achievements

2023 — **Hong Kong PhD Fellowship**

Young Researcher, 10th Heidelberg Laureate Forum

Research Travel Grant, HKUST

2019 — **Honor of Academic Excellency**, Tsinghua University.
Awarded to top 10% students.

2018 — **Honor of Academic Excellency**, Tsinghua University.

2016 — **1st Level in National High School Mathematics League**, the Chinese Mathematical Society.
Ranked within the top 2% in the provice of Anhui.

Academic Service

2025 — Reviewer for MARBLE'2025.

Extracurricular Experience

Dec 2019 - May 2021 — President of iOS Club, Tsinghua University.

Aug 2018 - Aug 2019 — Leader of the Students' Association of Science and Technology (Competition Branch), Department of Automation, Tsinghua University.

Teaching

2025 Spring, TA — **Hong Kong University of Science and Technology**
COMP5631: Cryptography and Security

2024 Spring, TA — **Hong Kong University of Science and Technology**
COMP 4541: Blockchains, Cryptocurrencies and Smart Contracts

2022 Spring & Fall, TA — **Hong Kong University of Science and Technology**
COMP 2012: Object-Oriented Programming and Data Structures

Skills

Languages — Native in Mandarin Chinese, proficient in English (TOEFL:106, GRE:158+170).

Coding — C/C++, Python, Rust, Go, Solidity, MATLAB, JAVA, PyTorch, HTML, …