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

1. Abidha V., Barakbayeva T., **Cai, Z.**, & Goharshady, A. (2024). Gas-efficient decentralized random beacons. In IEEE ICBC.

2. Barakbayeva T., **Cai, Z.**, & Goharshady, A. (2024). SRNG: an efficient decentralized approach for secret random number generation. In IEEE ICBC.

3. **Cai, Z.**, Farokhnia, S., Goharshady, A., & Hitarth, S. (2023). Asparagus: Automated synthesis of parametric gas upper-bounds for smart contracts. In OOPSLA. Asparagus code

4. Ballweg, J., **Cai, Z.**, & Goharshady, A. (2023). PureLottery: Fair leader election without decentralized random number generation. In IEEE Blockchain. PureLottery code

5. **Cai, Z.**, & Goharshady, A. (2023). Trustless and bias-resistant game-theoretic distributed randomness. In IEEE ICBC.

6. **Cai, Z.**, & Goharshady, A. (2023). Game-theoretic Randomness for Proof-of-Stake. In MARBLE.

7. 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. Barakbayeva T., **Cai, Z.**, & Goharshady, A. Smart Contracts for Trustless Sampling of Correlated Equilibria. code - SNARK part

2. **Cai, Z.**, & Goharshady, A. Proof of Election: A Formally-Verified Democratic Blockchain Protocol.

3. Updatable batched lookup argument: polylogarithmic update cost for prover.

4. 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.

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, Go, Solidity, MATLAB, JAVA, PyTorch, HTML, LaTeX, …