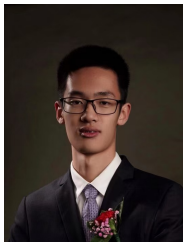

Zikuan Huang

+86-13810018850

Education

•B.E. in the Institute for Interdisciplinary Information Science, Tsinghua University *2021.9-2025.6*

Computer Science and Technology (a.k.a Yao Class)

Research Area

I am broadly interested in theoretical computer science. Mostly interested in the intersection between cryptography and quantum computation.

Publications

•On the Need for (Quantum) Memory with Short Outputs

STOC2026, by Zihan Hao, Zikuan Huang and Qipeng Liu

– In this work, we establish the first separation between computation with bounded and unbounded space, for problems with short outputs. Towards that, we introduce a problem called nested collision finding, and show that optimal query complexity can not be achieved, if one has much smaller memory comparing to the optimal algorithm.
Link: https://zikuanhuang.github.io/files/On%20the%20Need%20for%20(Quantum)%20Memory%20with%20Short%20Outputs.pdf.

•Copy-Protection From UPO, Revisited

Eurocrypt2026 and TQC2025, by Prabhanjan Ananth, Amit Berhera, Zikuan Huang, Fuyuki Kitagawa and Takashi Yamakawa

– Discussed a new construction for unclonable puncturable obfuscation and its application to copy-protections.
Link: https://eprint.iacr.org/2025/1880.pdf.

•Quantum Key-Revocable Dual-Regev Encryption, Revisited

TCC2024, by Prabhanjan Ananth Zihan Hu and Zikuan Huang

– Mainly resolve a conjecture made by a previous work (https://eprint.iacr.org/2023/325.pdf). Thus fully proved the existence of key-revocable PKE/FHE/PRF with or without classical revocation under the assumption of Learning-With-Error(LWE).
Link: https://eprint.iacr.org/2024/738.pdf.

Google Scholar Page: https://scholar.google.com/citations?user=EDJSTAcAAAAJ

Work Experience

•Winter 2025: Post-Bachelor *2025/12-now*

Post-bachelor researcher at Shanghai Qizhi Institute.

•Autumn 2024: Teaching Assistant *2024/09-2024/12*

Course: Cryptographic Protocols: Zero-Knowledge Proofs and MPC by Yifan Song at Tsinghua University.

•Feburary to August, 2024: Research Intern *2024/02-2024/07*

Jointly funded by Tsinghua and UCSB, 2024/02-2024/05 from Tsinghua and 2024/06-2024/07 from UCSB