Zihan Hu

☎ +86 19801260391 ✉ huzihan423@gmail.com 🏠 zihanhu.cn

Research Interests

- **Theoretical Computer Science (TCS)**, especially quantum computing, cryptography and complexity theory.

Education

- **Tsinghua University** *Aug. 2019 - June 2023*

  Bachelor in Computer Science Beijing, China

  - Yao Class, Institute for Interdisciplinary Information Sciences (IIIS), led by Prof. Andrew Yao
  - GPA: **3.98/4.0**, Rank: **2/91**
  - TOEFL: 106, GRE: 331

Work Experience

- Research Intern | Shanghai Qi Zhi Institute *Sep. 2023 - Present*

  Advisor: Yilei Chen Shanghai, China

  - Zero-knowledge protocols are vital components in constructing cryptographic primitives. The round complexity is a crucial metric for these protocols.
  - I am working on developing a new relaxed notion of zero knowledge and constructing round-efficient protocols that satisfy the new notion. This is an ongoing project (remotely) with Elaine Shi, Aayush Jain and Pratik Soni.

- Teaching Assistant for Theory of Computation *Feb. 2023 - June 2023*

  Instructor: Ran Duan Beijing, China

  - Provide guidance and support to students by answering their questions.
  - Evaluate assignments and offer tutorial sessions focused on common issues arising from assignments.

Research Experience

- Black-Box Separation for Public-Key Quantum Money *Jan. 2022 - Sep. 2022*

  Advisors: Prabhanjan Ananth and Henry Yuen UCSB (Remote)

  - Public-key quantum money scheme is a cryptographic protocol that allows a bank to issue banknotes that are publicly verifiable yet resistant to counterfeiting due to the laws of the physics. However, constructing provably secure public-key quantum money schemes based on well-studied assumptions remains challenging.
  - We ruled out the class of black-box constructions from collision-resistant hash functions to public-key quantum money schemes where the verification algorithm only makes classical queries to the hash functions.
  - My contribution includes extending our result to a more general case, deriving formal proofs, and writing.

- Attempts to Quantumly Solve Standard Lattice Problems *June 2021 - Nov. 2021*

  Advisor: Yilei Chen Tsinghua University

  - A wide range of cryptographic protocols are based on the hardness of lattice problems. Despite a large number of studies, the quantum hardness of lattice problems remains obscure.
  - We modified Regev's reduction to reduce standard lattice problems to a variant of learning with errors problem called $\mathsf{S}|\mathsf{LWE}\rangle$ where the noise amplitude is gaussian with an unknown phase, and showed a subexponential algorithm for $\mathsf{S}|\mathsf{LWE}\rangle$ where the noise amplitude is known, which suggests that to solve standard lattice problems more efficiently, it suffices to handle the unknown phase better.
  - My contribution includes brainstorming, formula derivation, and writing.

Publications

*In theoretical computer science, the authors are usually listed in alphabetical order.

- On the (Im)plausibility of Public-Key Quantum Money from Collision-Resistant Hash Functions

  Prabhanjan Ananth, Zihan Hu, Henry Yuen *Asiacrypt 2023*

- On the Hardness of $\mathsf{S}|\mathsf{LWE}\rangle$ with Gaussian and Other Amplitudes

  Yilei Chen, Zihan Hu, Qipeng Liu, Han Luo, Yaxin Tu *In Submission*

Honors and Awards

- Yao Award, Recognition Prize | IIIS, Tsinghua University *2022*
- Comprehensive Excellence Award | Tsinghua University *2021*
- Academic Excellence Award | Tsinghua University *2020, 2022*
- Sports Excellence Award | Tsinghua University *2020*
- Chinese Mathematical Olympiad, Silver Medal | Chinese Mathematical Society *2018*
- Chinese Girls' Mathematical Olympiad, Gold Medal (Rank 3) | Chinese Mathematical Society *2018*

Extracurricular Activities

- Class Leader | Yao Class 91, Tsinghua University *Sep. 2020 - Sep. 2021*
- Keen on a variety of sports, especially middle-distance and long-distance running.