Zihan Hao

z1hao@ucsd.edu | ORCID

Education

- **Tsinghua University** — Beijing, China
  Bachelor of Engineering in Computer Science - IIIS (Yao Class) — *Aug. 2020 - Jul. 2024*
  - GPA: 3.88/4.00 (Major GPA: 3.93/4.0)
  - Selected courses with A/A+: General Physics(1), General Physics(2), Theory of Computation, Fundamentals of Cryptography, Advanced topics in cryptography, Quantum complexity theory

- **Northeastern University** — MA, United States
  Research Intern, supervised by Prof. Daniel Wichs — *Mar. 2023 - Aug. 2023*

- **University of California, San Diego** — CA, United States
  PhD student in Computer Science and Engineering, supervised by Prof. Qipeng Liu — *Sept. 2024 - present*

Publications

- **[1]**= Fangqi Dong, **Zihan Hao**, Ethan Mook, Hoeteck Wee, Daniel Wichs: **Laconic Function Evaluation and ABE for RAMs from (Ring-)LWE**, *CRYPTO2024 accepted*, ePrint:2024/897

- **[2]**= Fangqi Dong, **Zihan Hao**, Ethan Mook, Daniel Wichs: **Laconic Function Evaluation, Functional Encryption and Obfuscation for RAMs with Sublinear Computation**, *Eurocrypt2024 accepted*, ePrint:2024/068

- **[3]** Zhenhuan Liu, **Zihan Hao**, Hong-Ye Hu: **Predicting Arbitrary State Properties from Single Hamiltonian Quench Dynamics**, Phys. Rev. Research 6, 043118, *QCTIP24 poster*

=: authors are alphabetically-ordered.

Research Experience

- **Quantum Crypotgraphy** — *University of California, San Diego, CA*
  Supervised by Prof. Qipeng Liu

  Time-space tradeoff for search problems — Sept. 2024 - present
  - Topic: Quantum Time-space tradeoff, Compressed oracle, QROM
  - Develop the first classical time-space lower bound for search problems with short output.
  - Attempt to derive a union bound for query algorithms combined in a non-uniform pattern.
  - Aim to derive a quantum time-space lower bound, showing a gap between space-bounded quantum algorithms and classical algorithms.

- **Quantum Computation** — *Tsinghua University, Beijing*
  Supervised by Prof. Xiongfeng Ma

  Applying Hamiltonian Shadow in Optical Lattices — Nov. 2023 - Jul. 2024
  - Topic: Randomized Measurement, Entanglement Detection
  - Explore the advantage of Hamiltonian Shadow in predicting properties in an optical lattice, especially fidelity.
  - Enable the prediction of asymmetric properties such as fidelity in optical systems for the first time.

  Predicting State Properties from Single Hamiltonian Dynamics [3] — Sep. 2023 - Jan. 2024
  - Topic: Randomized Measurement, Analog Quantum Simulation, Quantum tomography
  - Proposed the *Hamiltonian Shadow* protocol, which extracts complete information of the target state, using only a single Hamiltonian evolution without any ancillary systems.
  - Derived sample complexity of our protocol and showed comparable performance to the classical shadow method.
  - Conducted simulations on Rydberg atom arrays under realistic parameter settings, showing that our protocol is universally applicable to various analog quantum systems.
  - Progressed substantially in addressing the measurement difficulty of analog quantum simulators.

  Predicting Quantum Moments with Shallow Random Clifford Circuits — Nov. 2022 - Apr. 2023
  - Topic: Randomized Measurement, Shallow Clifford Circuits
  - Proposed a randomized measurement protocol to estimate quantum moments, $\mathrm{Tr}(\rho^k)$, which employs the statistical correlation between results, and only uses shallow clifford circuits.

- Explored how the depth of random clifford circuits influences the measuring capability and performance of the protocol.
- Presented an efficient way of predicting high-order moments with Near-Term Quantum Computation.

- **Advanced Cryptography Primitives** *Northeastern University, MA*
  Supervised by Prof. Daniel Wichs

  Laconic Function Evaluation for RAMs from (Ring-)LWE [1] Jul. 2023 - Feb. 2024
  - Topic: Laconic Function Evaluation, Attribute-Based Encryption, RAM Circuit
  - Developed a construction for RAM-LFE primitive based on (Ring-)LWE assumption and proved its security, achieving a client runtime that is sublinear in the database size and independent of the secret program runtime.
  - Showed that our method can be generally adapted to obtain constructions for a variety of primitives, including Functional Encryption for RAM and attribute-based Encryption for RAM.

  Laconic Function Evaluation for RAMs [2] Mar. 2023 - Oct. 2023
  - Topic: Laconic Function Evaluation, Functional Encryption, RAM model
  - Introduced the primitive of Laconic Function Evaluation for the RAM computation model (RAM-LFE), where a client delegates a secret RAM program to a server, asking it to run on a public large database and return the output, while not leaking any information of the program except the output.
  - Developed two different constructions for the RAM-LFE primitive and presented proof of security, based on Ring-LWE assumption and indistinguishability obfuscation(iO) respectively. Both achieve a client runtime that is sublinear in the database size and in the construction with iO, the client runtime is also sublinear in the runtime of the secret program.

Services

Asiacrypt 2024, external reviewer Jun. 2024

Honors and Awards

The prestigious Jacob School of Engineering fellowship, University of California, San Diego Mar. 2024
Science and Technology Innovation Excellence Award, Tsinghua University Oct. 2023
Academic Excellence Award, Tsinghua University Oct. 2023
Athletic Excellence Award, Tsinghua University Oct. 2022
Volunteer and Public Welfare Excellence Award, Tsinghua University Oct. 2022
Five-Star Volunteer Honor (with volunteering hours 300+), Tsinghua University Jun. 2022
1^{st} *Prize of Beijing in the National High School Mathematics League*, Chinese Mathematical Society Sept 2019
1^{st} *Prize of Beijing in the National High School Mathematics League*, Chinese Mathematical Society Sept 2018
1^{st} *Prize of the Beijing High School Mechanics Competition*, Beijing Physical Society May 2018
Bronze Medal in the Chinese Earth Science Olympiad, Seismological Society of China May 2018

Teaching, Leadership & Volunteering

TA in General Physics(1) Feb. 2024 - Jul. 2024
Core member of the Student Union Sports Department of IIIS Mar. 2022 - Jul. 2024
Volunteer for The 2021 College Admission(Undergraduate) of Tsinghua University Jun. 2022 - Jul. 2022
Volunteer in *The Beijing 2022 Winter Olympic Games* Feb. 2022
Volunteer in The Inspire Letter Program, exchanged letters with kids from the less developed areas Oct. 2020 - Jan. 2022
Volunteer for The 2021 College Admission(Undergraduate) of Tsinghua University Jun. 2021 - Jul. 2021

Skills

- **Programming Languages and Tools**: Python (with PyTorch and Qiskit), Go, C/C++, Verilog, Git, LaTeX
- **TOEFL**: 108/120. Reading: 29, Listening: 29, Speaking: 23, Writing: 27 (*MyBest*: 29)
- **GRE**: 327/340. Quantitative: 170/170, Verbal: 157/170, Analytical Writing: 4.0/6.0
- **Miscellaneous**: Taekwondo, Electronic organ piano, Photography, Skateboard