ZIHAN HAO

haozh02@hotmail.com | (+86) 13681184210 | Personal Website

Education

- **Tsinghua University** — Beijing, China
  Bachelor of Engineering in Computer Science - IIIS (Yao Class) — *Aug. 2020 - (Expected) July 2024*
  - GPA: 3.86/4.00
  - Selected courses with A/A+: General Physics(1), General Physics(2), Theory of Computation, Fundamentals of Cryptography, Advanced topics in cryptography
- **Northeastern University** — MA, United States
  Research Intern, supervised by Prof. Daniel Wichs — *Mar. 2023 - Aug. 2023*

Publications

- **[1]** Zhenhuan Liu, **Zihan Hao**, Hong-Ye Hu: **Predicting Arbitrary State Properties from Single Hamiltonian Quench Dynamics**, arXiv preprint arXiv:2311.00695
- **[2]**= Fangqi Dong, **Zihan Hao**, Ethan Mook, Daniel Wichs: **Laconic Function Evaluation, Functional Encryption and Obfuscation for RAMs with Sublinear Computation**, *Eurocrypt2024 in submission*

=: authors are alphabetically-ordered

Research Experience

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

  Quantifying Memory Effect for Open Quantum System Evolutions — Nov. 2023 - present
  - Topic: Open Quantum System, Non-Markovian Quantum Process, Randomized Measurement
  - Propose a measure for the memory effect in open quantum system evolutions, with a discrete setting and from the perspective of quantum information.
  - Provide a new way to estimate the dimension of a quantum system or subsystem with the tool of Randomized Measurement.

  Predicting State Properties from Single Hamiltonian Dynamics [1] — Sep. 2023 - Nov. 2023
  - 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 — July 2023 - present
  - 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 - June 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.

Honors and Awards

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	June 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

Leadership & Volunteering

Core member of the Student Union Sports Department of IIIS	Mar. 2022 - present
Volunteer for The 2021 College Admission(Undergraduate) of Tsinghua University	June. 2022 - July. 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	June. 2021 - July. 2021

Skills

- **Programming Languages and Tools**: Python (with PyTorch and Qiskit), Go, C/C++, Verilog, Git, LaTeX
- **English**: TOEFL: 108(Speaking 23), GRE: 327+4.0, C2 Proficiency: 211
- **Miscellaneous**: Taekwondo, Electronic organ piano, Basketball, Science fiction writing, Astronomical observation