# Zikai Zhou

zhouzk22@mails.tsinghua.edu.cn +86 172 0523 8368
https://zigzagkmp.github.io/ https://github.com/ZigZagKmp

## EDUCATION

**BS, Tsinghua University, Computer Science and Technology,** 08/2022 - Present

- **Department:** Yao Class (Institute for Interdisciplinary Information Sciences)
- **GPA:** 3.95/4.00
- **Relevant Courses:** Cryptographic Protocols: Zero-Knowledge Proofs and MPC (A-), Fundamentals of Cryptography (A), Secure Multiparty Computation: Theory and Applications (A), Quantum Communication and Cryptography (A-), Mathematics for Computer Science (A), Abstract Algebra (A).

## RESEARCH INTERESTS & SKILLS

| | |
|---|---|
| **Research Interests** | Cryptography: FHE, MPC, and ZKP |
| **Programming Languages** | Familiar with C, C++, Python; Experience with Go, Matlab, Bash. |

## ACADEMIC EXPERIENCE

**Student Research Intern @ Carnegie Mellon University** 02/2025 - 07/2025

- Research Advisor: Prof. Wenting Zheng

**Student Research Intern @ Tsinghua University** 09/2025 - present

- Research Advisor: Prof. Yifan Song

**Teaching Assistant @ Tsinghua University** 09/2024 - 01/2025

- Course: Cryptographic Protocols: Zero-Knowledge Proofs and MPC
- Class size: 20
- Course Instructor: Prof. Yifan Song
- Responsibilities: Graded and provided feedback on scribed lecture notes, graded assignments and the course project.

## RESEARCH EXPERIENCE

**Project: Optimal Bootstrapping Placement for Fully Homomorphic Encryption** 10/2024 - present

- Led the design of a novel compiler for optimizing FHE circuits, focusing on optimal bootstrapping placement.
- Developed and implemented new algorithms to accelerate the search for optimal bootstrapping placements.
- Benchmarked the compiler against state-of-the-art algorithms and integrated FHE library backends for testing.
- **Co-first author** on a manuscript in preparation for submission to the *USENIX Security Symposium 2026*.

**Project: Efficient honest majority MPC protocol with guaranteed output delivery** 09/2025 - present

- Identified the core cost trade-off between authentication tag generation and authentication key generation.
- Exploring potential improvements.

**Course Project: Continuous LWE and its application in learning theory** 04/2024 - 06/2024

*Course: Fundamentals of Cryptography*

- Reviewed the reduction from GapSVP and LWE to continuous LWE (group contribution).
- Investigated the reduction from certain learning problems to continuous LWE (CLWE).
- Generalized the cryptographic hardness of learning a cosine neuron to the hardness of learning any constant-period, constant-Lipschitz neuron.
- Unified the hardness proofs of different learning problems by summarizing the common crucial role of the homogeneous CLWE distribution (hCLWE).

## AWARDS AND HONORS

**Yao Award 2025** 09/2025
*Top* 20% *in Yao Class*

**National Scholarship** 12/2023
*Top* 0.2% *national-wide*

**Comprehensive Merit Scholarship of Tsinghua** 12/2024
*Sponsored by Ningbo Future Star Scholarship*

**Outstanding Student Leader of Tsinghua University** 10/2024

**Comprehensive Merit Scholarship of Tsinghua** 12/2023
*Sponsored by Institute for Interdisciplinary Information Core Technology Special Scholarship*

**Honorable Mention, Mathematical Contest in Modeling** 02/2023

**Gold Medalist, National Olympiad in Information Winter Camp (NOI-WC)** 02/2021
*In high school period*

**1st Prize, National High School Mathematics Olympics Competition** 11/2021
*In high school period*

## EXTRA-CURRICULAR

**Senior Q&A Assistant** 03/2023 - present
*Tsinghua Drop-in Tutoring Center*

· Assisted undergraduate students with problems in calculus, linear algebra, programming, and algorithms.

**Leadership:** Class monitor of Yao Class (2023-2024); Deputy secretary of Yao Class Youth League Committee (responsible for volunteer activities) (2024); Student Union Officer (2023-present).

**Voluntary Service:** 450+ hours of volunteer service. Organized several institution-wide volunteer activities.