YIDING ZHANG

zhangyd19@mails.tsinghua.edu.cn
+86 18851069946 Homepage
Beijing, China, 100084

EDUCATION

Tsinghua University *Sept. 2019 - Present*

- Institute for Interdisciplinary Information Sciences (Yao Class, founded by Prof. Andrew C. Yao in 2005)
- Overall GPA 3.77/4.00
- Relevant courses: Theory of Computation, Fundamentals of Cryptography, Design and Analysis of Algorithms, Mathematics for Computer Science, Linear Algebra

RESEARCH INTERESTS

Cryptography, complexity theory, algorithms.

RESEARCH EXPERIENCE

Tsinghua University *Beijing China*
Mentor: Yilei Chen *Feb. 2021 - Present*

- Lattice-based cryptography
- Theory and applications of the Fiat-Shamir heuristic

Technion - Israel Institute of Technology *Haifa, Israel*
Host Professor: Ron Rothblum *Feb. 2022 - July 2022*

- PPAD hardness from plain LWE
- SNARGs for P based on more cryptographic assumptions

PROJECTS

Towards better SNARGs for P from Fiat-Shamir
Advisor: Prof. Ron Rothblum Course project of *Research Immersion Training*

- In this project, we focused on a recent LWE-based construction of succinct non-interactive arguments (SNARGs) for the complexity class P. We showed that somewhere extractable commitment - a crucial component in the SNARG construction - is closely related to (and almost the same as) private information retrieval, a much more well-studied tool in cryptography. We also showed some progress and challenges in constructing DDH-based SNARGs through the same technique.

Fiat-Shamir for arguments (ongoing)
Advisor: Prof. Yilei Chen Course project of *Research Practice*

- This project aimed to study the possibility of securely instantiating Fiat-Shamir on a broader class of arguments (either positively or negatively). We first studied some known impossibility results about Fiat-Shamir to see if there are some limitations in these counterexamples. Then starting from the limitations, we tried to either strengthen or bypass the impossibility results. Due to the new techniques and progress in some cryptographic tools (e.g., indistinguishability obfuscation), stronger positive results about Fiat-Shamir might be achievable.

Hardness of sequence alignment from fine-grained complexity
Joint work with Tianqi Yang Course project of *Computational Biology*

- Sequence alignment is a fundamental problem in computational biology. In this project, we showed the hardness of this problem in the context of data structure lower bounds. More precisely, we studied some known results about the hardness of nearest neighbour search under the Orthogonal Vectors Conjecture, and then showed that the same technique can also lead to the hardness of (online) sequence alignment.

AWARDS

China Collegiate Programming Contest (CCPC) *Oct. 2019*

- Gold medal (5^{th} place) in the CCPC Xiamen Regional Contest

Tsinghua Xuetang Scholarship *Sept. 2019*

Second-Level Scholarship for Freshman *Sept. 2019*

National Olympiad in Informatics (NOI) *July 2018*

- Gold medal and entering the national training team

SKILLS

Programming skills: C, C++, Python, Go, Java, SQL, Matlab.
Tools and frameworks: LaTeX, Git, MySQL.
Language skills: Chinese (native), English (TOEFL 103, GRE 323+3.5).
Hobbies: tennis, table tennis, badminton.