Yaxin Tu

tyx0001ash@gmail.com +86 153-9285-5299 tu-yaxin.github.io

Research Interests

I'm broadly interested in theoretical computer science, with a focus on cryptography and its interplay with other fields.

Education

◇ **B. Eng. in Computer Science and Technology, Tsinghua University** *Aug. 2019 - July 2023*

- Yao Class, Institute for Interdisciplinary Information Sciences (IIIS), led by Prof. Andrew Yao
- GPA: **3.86/4**, major GPA: **3.90/4**

Research Experience

◇ Function Secret Sharing for Multi-point Functions, FACT center, IDC Herzliya *Feb. 2022 - Present*

Advisor: Elette Boyle

- Function secret sharing for multi-point functions serves as a useful primitive of various applications with different emphases on computation time or share size.
- We proposed a new PRG-based scheme to succinctly share multi-point functions with computation time independent of the sparsity of the vector, which appears to be the practically fastest solution in most application scenarios.
- Aiming for **CCS 2023**. More updates and follow-up works on my personal website.
- Collaborate with Elette Boyle, Yuval Ishai, and Niv Gilboa.
- My contributions include brainstorming, active discussion, concrete evaluation, and writeup.

◇ Solving standard lattice problems via quantum algorithms, Tsinghua University *June 2021 - Nov. 2021*

Advisor: Yilei Chen

- The hardness of standard lattice problems lies in the core of lattice-based cryptography and is not known to be broken by any quantum attacks.
- Borrowing ideas in Regev's worst-case to average-case reduction, we attempted to solve standard lattice problems by first reducing it to some variant of quantum LWE and then solving the latter problem. We closed the first step while the second gap persists. See notes for our partial results on my personal website.
- Collaborate with Yilei Chen, Qipeng Liu, and Zihan Hu.
- My contributions include brainstorming, formula derivation, active discussion, note updates, coding, and proofreading.

Publications

◇ On the subtle nature of a simple logic of the hide and seek game *WoLLIC 2021*

Dazhu Li, Sujata Ghosh, Fenrong Liu and Yaxin Tu

- For any simple logic, it is always interesting to find the impact of adding an equality constant.
- We introduced a new member to the class of logics whose satisfiability problem suddenly becomes undecidable after being extended with equality constant.
- I applied the analysis of games to our logic and investigated the behavior of our logic extended with other operators.

Honors and awards

- Science and Technology Innovation Merit Scholarship | Tsinghua University *2022*
- Chinese Mathematical Olympiad, Gold Medal *(Preadmitted to Yao Class)* | Chinese Mathematical Society *2018*
- Chinese Women's Mathematical Olympiad, Gold Medal (*Rank 5th*) | Chinese Mathematical Society *2018*