

LUO, HAN

luohan23@mails.tsinghua.edu.cn ◇ (+86) 18800128126 ◇ Homepage

EDUCATION

Institute for Interdisciplinary Information Sciences, Tsinghua University Ph.D. student majored in Computer Science, advisor Prof. Yilei Chen	<i>Beijing, China</i> 2023 -
Institute for Interdisciplinary Information Sciences, Tsinghua University Bachelor's degree in Computer Science	<i>Beijing, China</i> 2019 - 2023

RESEARCH EXPERIENCE

Lattice-based Cryptography. In IIIS, Tsinghua university. *Spring 2021 -*
Supervisor(s): Prof. Yilei Chen.

- We aim to find new classical or quantum algorithms for solving variants of lattice problems, including the quantum version of LWE and the extrapolated dihedral coset problems, etc. Our goal is to use these problems as a bridge to develop subexponential (or even polynomial) quantum algorithms for standard lattice problems.
- We also aim to prove new hardness results or reductions for variants of lattice problems. Based on these problems, we plan to design new constructions of cryptographic primitives, such as quantum money, witness encryption, etc.

AI + Cryptography. In IIIS, Tsinghua university. *Spring 2025 -*
Supervisor(s): Prof. Yilei Chen, Prof. Tianxing He.

- We ultimately aim to use large language models to evaluate cryptography papers. As a first step, we focus on testing their ability of understanding mathematical contents, and explore how fine-tuning can improve this capability.

Quantum Algorithm. In QUARK Lab, CFCS, Peking University. *Spring 2022 -*
Supervisor(s): Prof. Tongyang Li.

- We aim to develop novel quantum algorithms that can accelerate the estimation of fundamental statistical properties of data, specifically the mean and covariance, which are critical for various tasks in data analysis and machine learning.
- We also aim to design new quantum algorithms for classical problems in number theory and combinatorics (e.g. integer factorization, submodular maximization, etc.), to further reducing their time and space complexity. In addition, we explore the possibility of establishing new lower bounds on quantum complexity for these problems.

Quantitative Researcher (Intern). In Jump Trading Shanghai Office *Summer 2022*

- We apply methods from statistical learning and machine learning to deeply explore the mathematical patterns in financial data. Based on these insights, we design and develop new trading strategies, which are then evaluated through rigorous back-testing to assess their effectiveness and robustness.

PUBLICATIONS

LWE with Quantum Amplitudes: Algorithm, Hardness, and Oblivious Sampling

By Yilei Chen, Zihan Hu, Qipeng Liu, **Han Luo**, Yaxin Tu

In CRYPTO 2025

AICrypto: A Comprehensive Benchmark For Evaluating Cryptography Capabilities of Large Language Models

By *Yu Wang, *Yijian Liu, *Liheng Ji, ***Han Luo**, *Wenjie Li, Xiaofei Zhou, Chiyun Feng, Puji Wang, Yuhan Cao, Geyuan Zhang, Xiaojian Li, Rongwu Xu, Yilei Chen, Tianxing He

In submission

HONORS & AWARDS

Comprehensive Excellence Scholarship	2021
Freshmen Scholarship	2019

OTHER EXPERIENCE

High School Mathematics Olympiad *Winter 2018*

- I win the gold medal in 34th Chinese Mathematical Olympiad (CMO), and was selected into the Chinese national training team.

Reviewer Service

- CRYPTO 2024, CRYPTO 2025.