Kaiyi Zhang

kaiyizhang@tsinghua.edu.cn (+86)15066099436
kzoacn Kaiyi Zhang Kaiyi Zhang



Work Experience

Jul. 2025 – Present **Tsinghua University**
Postdoctoral Researcher (Shuimu Tsinghua Scholar Program) at IAS
Hosted by Professor Xiaoyun Wang.

Education

Sept. 2020 – June 2025 **Shanghai Jiao Tong University**
Doctor of Philosophy (Ph.D.) in Computer Science
Advised by Professor Yu Yu.

Sept. 2016 – June 2020 **Shanghai Jiao Tong University**
Bachelor of Engineering (B.Eng.) in Computer Science
*Member of **ACM Honors Class**, which is an elite CS program for talented students.*

Research Interests

Current Focus **Artificial Intelligence**
AI for Science, AI for Math, and Embodied Intelligence.

Previous Research **Post-Quantum Cryptography**
Published multiple academic papers, including first-authored papers at CRYPTO and ASIACRYPT.
Participated in the U.S. NIST Post-Quantum Cryptography Standardization project SPHINCS-ALPHA [Link].

Other Research **Quantum Information**
First- or co-first-authored papers published in PNAS and npj Quantum Information.
Zero-Knowledge Proofs, Secure Multi-Party Computation
Published several academic papers.

Research Funding

2027 – 2029 **Young Scientists Fund**
National Natural Science Foundation of China
Algebraic Cryptanalysis of Arithmetization-Oriented Symmetric Primitives
Grant No. 62602352

Research Publications

1. C. Baum, J. Berlips, W. Chen, *et al.*, "A system capable of verifiably and privately screening global DNA synthesis," ***National Science Review***, vol. 13, no. 14, nwag103, 2026. DOI: 10.1093/nsr/nwag103.
2. **K.-Y. Zhang**, A.-J. Huang, K. Tu, *et al.*, "Experimental secure multiparty computation from quantum oblivious transfer with bit commitment," ***npj Quantum Information***, vol. 12, 76, 2026. DOI: 10.1038/s41534-026-01219-w.

3. Q. Feng, K. Yang, **K. Zhang**, X. Wang, Y. Yu, and X. Xie, "Stateless deterministic multi-party EdDSA signatures with low communication," in *Public-Key Cryptography – **PKC 2025**, Part V*, Springer Nature Switzerland, 2025, pp. 268–297. DOI: 10.1007/978-3-031-91832-2_9.

4. H. Cui, H. Liu, D. Yan, K. Yang, Y. Yu, and **K. Zhang**, "ReSolveD: Shorter signatures from regular syndrome decoding and VOLE-in-the-head," in *IACR International Conference on Public-Key Cryptography **(PKC 2024)***, Springer, 2024, pp. 229–258.

5. C.-L. Li, **K.-Y. Zhang**, X. Zhang, *et al.*, "Device-independent quantum randomness–enhanced zero-knowledge proof," *Proceedings of the National Academy of Sciences **(PNAS)***, vol. 120, no. 45, e2205463120, 2023.

6. **K. Zhang**, H. Cui, and Y. Yu, "Revisiting the constant-sum Winternitz one-time signature with applications to SPHINCS+ and XMSS," in *Advances in Cryptology – **CRYPTO 2023***, H. Handschuh and A. Lysyanskaya, Eds., ser. Lecture Notes in Computer Science, Cham: Springer Nature Switzerland, 2023, pp. 455–483, ISBN: 978-3-031-38554-4. DOI: 10.1007/978-3-031-38554-4_15.

7. **K. Zhang**, Q. Wang, Y. Yu, C. Guo, and H. Cui, "Algebraic attacks on round-reduced RAIN and full AIM-III," in *International Conference on the Theory and Application of Cryptology and Information Security **(ASIACRYPT 2023)***, Springer, 2023, pp. 285–310.

8. Y. Xu, **K. Zhang**, and Y. Yu, "GRUZ: Practical resource fair exchange without blockchain," in *Information Security: 25th International Conference, **ISC 2022**, Bali, Indonesia, December 18–22, 2022, Proceedings*, Springer, 2022, pp. 214–228.

9. H. Cui and **K. Zhang**, "A simple post-quantum non-interactive zero-knowledge proof from garbled circuits," in *Information Security and Cryptology: 17th International Conference, **Inscrypt 2021**, Virtual Event, August 12–14, 2021, Revised Selected Papers 17*, Springer, 2021, pp. 269–280.

10. H. Cui, **K. Zhang**, Y. Chen, Z. Liu, and Y. Yu, "MPC-in-Multi-Heads: A multi-prover zero-knowledge proof system: (or: How to jointly prove any NP statements in ZK)," in *Computer Security–**ESORICS 2021**: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part II 26*, Springer, 2021, pp. 332–351.

11. L.-J. Wang, **K.-Y. Zhang**, J.-Y. Wang, *et al.*, "Experimental authentication of quantum key distribution with post-quantum cryptography," ***npj Quantum Information***, vol. 7, no. 1, p. 67, 2021.

12. Y.-H. Yang, P.-Y. Li, S.-Z. Ma, *et al.*, "All optical metropolitan quantum key distribution network with post-quantum cryptography authentication," ***Optics Express***, vol. 29, no. 16, pp. 25 859–25 867, 2021.

13. **K. Zhang**, H. Cui, and Y. Yu, "Facial template protection via lattice-based fuzzy extractors," *Cryptology ePrint Archive*, 2021.

Research Experience

Aug. 2019 – Dec. 2019 — **Northwestern University**
Advised by Professor Xiao Wang

July 2018 - Sept. 2020 — **Shanghai Jiao Tong University**
Advised by Professor Yu Yu

Honors and Awards

2025 **Outstanding Doctoral Dissertation**, China Computer Federation

2020 **First Prize**, The 2020 Financial Cryptography Contest.

2017 **Gold Medal**, The 2017 CCPC China Final Contest.

Gold Medal, The 2017 ACM ICPC East Continent League Final.

Gold Medal, The 2017 ACM ICPC Asia Hong Kong Contest.

Gold Medal, The 2017 CCPC Qinhuangdao Contest.

Gold Medal, The 2017 ACM ICPC Asia Shenyang Regional Contest.

2016 **Gold Medal**, The 2016 ACM ICPC Asia Yangon Regional Contest.

Gold Medal, The 2016 CCPC Hefei Contest.

Gold Medal, The 2016 ACM ICPC Asia QingDao Regional Contest.

2015 **Bronze Medal**, The 32nd China National Olympiad in Informatics.

Teaching Experience

Spring 2019 **(SJTU MS208) Compiler Design and Implementation**
Lead Teaching Assistant

Fall 2018 **SJTU ACM-ICPC Team**
Coach

Spring 2018 **(SJTU CS147) Data Structures**
Teaching Assistant

Other Experience

July 2019 **The 36th China National Olympiad in Informatics**
Referee
Provided several problems to the contest committee.