

Kaiyi Zhang

✉ kzoacn@outlook.com

☎ (+86)15066099436

📄 kzoacn



Education

- Sept. 2020 – Present 📖 **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 Publications

- 1 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*, vol. 120, no. 45, e2205463120, 2023.
- 2 **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.
- 3 **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*, Springer, 2023, pp. 285–310.
- 4 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.
- 5 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.
- 6 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.
- 7 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.
- 8 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.
- 9 **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

- 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.