张凯羿

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



工作经历

2025 年 7 月 – 至今 **清华大学**
高等研究院 水木学者博士后
博士后导师：王小云院士

教育经历

2020 年 9 月 – 2025 年 6 月 **上海交通大学**
计算机科学与技术 博士
导师：郁昱教授.

2016 年 9 月 – 2020 年 6 月 **上海交通大学**
计算机科学与技术 学士
毕业于致远学院 *ACM* 班.

研究方向

当前研究方向 **人工智能**
AI for Science、AI for Math、具身智能

此前研究方向 **后量子密码**
发表多篇学术论文，其中以第一作者发表于 CRYPTO,ASIACRYPT 各一篇
参与美国 NIST 后量子密码标准征集 SPHINCS-ALPHA [Link]

其他研究方向 **量子信息**
以第一作者或共同第一作者发表于 PNAS,npj quantum inf. 三篇
零知识证明、安全多方计算
发表若干学术论文

科研项目

2027 年 – 2029 年 **国家自然科学基金青年科学基金项目**
面向算术化对称原语的代数安全性分析
项目批准号：62602352

个人技能

专业能力

编程能力

熟悉 C++, Python

曾参与程序设计竞赛，熟悉各类常见算法、数据结构

熟悉 Linux 系统常用操作

熟悉密码学项目工程，所有参与的学术论文的代码实现均由我本人完成 [GitHub]

其他能力

论文撰写

熟悉 LaTeX, 撰写并发表过多篇学术论文

语言

母语汉语，英语流利

发明专利

2024 **量子不经意传输方法、系统、服务器及存储介质**

申请人：国科量子通信网络有限公司

申请号：2024105973684

2022 **适用于闪烁探测器的低中放固废 γ 能谱解析方法及系统**

申请人：上海交通大学

申请号：2022115643272

帮助核物理舍友完成了相关代码实现

学术论文

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.

研究经历

2019 年 8 月 – 2019 年 12 月　**美国西北大学**
实习，导师：汪骁教授
主要研究内容为安全多方计算

2018 年 7 月 - 2020 年 9 月　**上海交通大学**
实习，导师：郁昱教授

成就与奖项

2025 **博士学位论文激励计划（原优博）**, 中国计算机学会.

2020 **一等奖**, 2020 年金融密码杯全国密码应用和技术创新大赛.

2017 **金牌**, 2017 年中国大学生程序设计竞赛 (CCPC) 决赛.

金牌, 2017 年国际大学生程序设计竞赛 (ICPC) 东大陆决赛.

金牌, 2017 年国际大学生程序设计竞赛 (ICPC) 香港站.

金牌, 2017 年中国大学生程序设计竞赛 (CCPC) 秦皇岛站.

金牌, 2017 年国际大学生程序设计竞赛 (ICPC) 沈阳站.

2016 **金牌**, 2016 年国际大学生程序设计竞赛 (ICPC) 仰光站.

金牌, 2016 年中国大学生程序设计竞赛 (CCPC) 合肥站.

金牌, 2016 年国际大学生程序设计竞赛 (ICPC) 青岛站.

2015 **铜牌**, 第 32 届全国青少年信息学奥林匹克竞赛 (NOI).

教学经历

2019 年春季 **(SJTU MS208) 编译原理**
助教

2018 年秋季 **上海交通大学 ACM-ICPC 队**
教练

2018 年春季 **(SJTU CS147) 数据结构**
助教

其他经历

2019 年 7 月 **第 36 届全国青少年信息学奥林匹克竞赛 (NOI)**
裁判、命题人