

Hongrui Cui

✉ rickfreeman@sjtu.edu.cn 📞 (+86)-15821879068
🌐 <https://rickfreemancui.github.io>




Education

- | | |
|------------------------|--|
| Mar. 2022 – Present | 📖 Shanghai Jiao Tong University
Ph.D. in Computer Science and Technology. |
| Sept. 2019 – Mar. 2022 | 📖 Shanghai Jiao Tong University
M.Sc. in Computer Science and Technology.
Thesis: <i>Design and Implementation of Multi-Prover Zero-Knowledge Systems.</i> |
| Sept. 2015 – Mar. 2019 | 📖 Shanghai Jiao Tong University
B.Sc. in Information Security.
Thesis: <i>Improvement and Optimization of Private Set Intersection in Stronger Security Models.</i> |

Research Publications

Conference Proceedings

- 1 **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,” ser. Lecture Notes in Computer Science, Springer, 2024.
🔗 URL: <https://eprint.iacr.org/2024/040>.
- 2 **H. Cui**, X. Wang, K. Yang, and Y. Yu, “Actively secure half-gates with minimum overhead under duplex networks,” in *Advances in Cryptology - EUROCRYPT 2023 - 42nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Lyon, France, April 23-27, 2023, Proceedings, Part II*, C. Hazay and M. Stam, Eds., ser. Lecture Notes in Computer Science, vol. 14005, Springer, 2023, pp. 35–67. 🔗 DOI: 10.1007/978-3-031-30617-4_2.
- 3 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 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part V*, H. Handschuh and A. Lysyanskaya, Eds., ser. Lecture Notes in Computer Science, vol. 14085, Springer, 2023, pp. 455–483. 🔗 DOI: 10.1007/978-3-031-38554-4_15.
- 4 K. Zhang, Q. Wang, Y. Yu, C. Guo, and **H. Cui**, “Algebraic attacks on round-reduced rain and full AIM-III,” in *Advances in Cryptology - ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Guangzhou, China, December 4-8, 2023, Proceedings, Part III*, J. Guo and R. Steinfeld, Eds., ser. Lecture Notes in Computer Science, vol. 14440, Springer, 2023, pp. 285–310. 🔗 DOI: 10.1007/978-981-99-8727-6_10.
- 5 L. Zhou, Z. Wang, **H. Cui**, Q. Song, and Y. Yu, “Bicopter: Two-round secure three-party non-linear computation without preprocessing for privacy-preserving machine learning,” in *44th IEEE Symposium on Security and Privacy, SP 2023, San Francisco, CA, USA, May 21-25, 2023*, IEEE, 2023, pp. 534–551.
🔗 DOI: 10.1109/SP46215.2023.10179449.
- 6 **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*, Y. Yu and M. Yung, Eds., ser. Lecture Notes in Computer Science, vol. 13007, Springer, 2021, pp. 269–280. 🔗 DOI: 10.1007/978-3-030-88323-2_14.

- 7 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*, E. Bertino, H. Schulmann, and M. Waidner, Eds., ser. Lecture Notes in Computer Science, vol. 12973, Springer, 2021, pp. 332–351.  DOI: 10.1007/978-3-030-88428-4_17.

Skills

Languages	Reading, writing and speaking competencies for English and Mandarin Chinese.
Standard Tests	TOEFL: Total 108 (Reading 29, Listening 30, Speaking 22, Writing 27) GRE: Verbal – 162 (91% percentile) Quantitative – 170 (97%) Analytical Writing – 4.0
Coding	Python, C++, and \LaTeX .

Miscellaneous Experience

Awards and Achievements

- 2020  **First Prize (3 in total)**, Financial Crypto Cup (Initiated by the People's Bank of China).

Academic Experience

- 2024  **PKC**. Hosted in Sydney, Australia.
- 2023  **CHINACRYPT**. Hosted in Guangzhou, China.
 **ASIACRYPT**. Hosted in Guangzhou, China.
 **CRYPTO**. Hosted in Santa Barbara, United States.
 **EUROCRYPT**. Hosted in Lyon, France.
- 2021  **ESORICS**. Virtual.
 **INSCRYPT**. Virtual.
- 2019  **Crypto Innovation School**. Hosted in Shanghai, China.
- 2018  **Crypto Innovation School**. Hosted in Shenzhen, China.