Xufeng Zhang

Last updated: February 2026

xufengzhang.crypto@gmail.com

Master's Student - Beijing Institute of Technology, China

Research Summary and Interests

- My previous research explores the interplay between cryptography and distributed computing from both directions. It applies cryptographic techniques to improve the complexity and security of distributed protocols, and leverages distributed techniques to enhance the scalability and decentralization of secure cryptographic primitives. Overall, my work aims to organically integrate these two fields to design provably secure and efficient distributed cryptographic protocols.
- My current research interests lie in theoretical cryptography, particularly in secure protocols, including multi-party computation (*MPC*), zero-knowledge proofs (*ZKP*), Byzantine agreement and broadcast, and threshold cryptography.

Education

- **Beijing Institute of Technology** *Sept. 2023 - Present*
  M.S. in Cyberspace Science and Technology *(Advisor: Haibin Zhang and Sisi Duan)* Beijing, China
  - GPA: 90.46/100
- **Qinghai University** *Sept. 2019 - Jun. 2023*
  Bachelor of Engineering in Computer Science and Technology Xining, Qinghai, China
  - GPA: 4.2/5.0 (89.81/100), Rank: 2nd/176

Publications and Patents

[1] **Randomized vs. Deterministic? Practical Randomized Synchronous BFT in Expected Constant Time** *SRDS 2025*
Xufeng Zhang, Baohan Huang, Sisi Duan, Haibin Zhang [DOI] [eprint]
IEEE Symposium on Reliable Distributed Systems (SRDS; annual since 1981)

[2] **Enhancing Permissioned Blockchains with Controlled Data Authorization** *ACISP 2024*
Qichang Liu, **Xufeng Zhang**, Sisi Duan, Haibin Zhang [DOI]

Research Experience

- **ARiMS, Beijing Institute of Technology** *Sept. 2025 - Present*
  Supervised by Dr. Haibin Zhang Beijing, China
  - Studying on information-theoretically secure asynchronous multi-party computation (AMPC) and asynchronous complete secret sharing (ACSS).
- **ARiMS, Beijing Institute of Technology** *Jan. 2024 - Sept. 2025*
  Supervised by Dr. Haibin Zhang and Dr. Sisi Duan Beijing, China
  - **Paper:** Randomized vs. Deterministic? Practical Randomized Synchronous BFT in Expected Constant Time *(First Author; SRDS 2025, a long-standing conference on distributed computing)*
  - Proposed a randomized, expected $O(1)$ time synchronous Byzantine fault-tolerant (BFT) paradigm, achieving $O(n)$ amortized message complexity per block proposal.
  - Built a practical synchronous BFT system, outperforming existing state-of-the-art protocols in both latency and throughput under failure-free scenarios.
  - Designed a synchronous binary Byzantine agreement (BA) and a multi-valued Byzantine agreement (MBA) protocol with expected $O(1)$ time, $O(n^2)$ message, and fewer steps than the corresponding state-of-the-art.
- **ARiMS, Beijing Institute of Technology** *Jun. 2023 - Jan. 2024*
  Supervised by Dr. Haibin Zhang and Dr. Sisi Duan Beijing, China
  - **Paper:** Enhancing Permissioned Blockchains with Controlled Data Authorization *(ACISP 2024)*
  - To achieve confidentiality with fine-grained access control for permissioned blockchains or distributed systems, proposed the threshold encryption with controlled authorization.
  - Leveraging verifiable secret sharing, threshold proxy re-encryption and non-interactive zero-knowledge.

- Before delegation, even if the number of corrupted parties goes beyond the threshold, the privacy still maintained. Supports dynamically delegation revocation.

- **ARiMS, Beijing Institute of Technology** *Aug. 2024 - Nov. 2024*
  Supervised by Dr. Haibin Zhang and Prof. Shengli Liu Beijing, China
  - **Competition:** 2024 "Financial Cryptography Cup" Innovation Competition
  - Based on the expected $O(1)$ time asynchronous distributed key generation (ADKG) and the asynchronous distributed key refreshment (ADKR), designed a distributed secure digital wallet solution for mobile terminals for e-cash.
- **Dept. of IT, Yangtze Delta Region Institute of Tsinghua University** *Oct. 2024 - Jan. 2025*
  Supervised by Dr. Haibin Zhang Remote
  - Assisted in building *Tianshu* Trusted Data Space Platform, a full-stack solution for trusted, secure and reliable data sharing and utilizing among distrusted entities.
  - Developed and deployed the core consensus mechanisms as well as the distributed fine-grained access control and encryption module.
- **School of CS, Qinghai University** *Oct. 2022 - Mar. 2023*
  Supervised by Dr. Rujia Li and Prof. Yong Xie Xining, Qinghai, China
  - **Bachelor's Thesis:** Research and Design on Accountable Decryption Based on Intel SGX
  - Designed and developed a distributed accountable decryption system based on trusted execution environment (TEE), ensuring every decryption leaves a tamper-resistant record. [Open Sourced]

Honors and Awards

- **Postgraduate Student Scholarship** 2023 - 2025
  Awarded by Beijing Institute of Technology (awarded for two times)
- **Outstanding Student Scholarship** 2020 - 2022
  Awarded by Qinghai University (awarded for two times)
- **Third Group Prize of 2024 "Financial Cryptography Cup" Innovation Competition** *Nov. 2024*
  Awarded by the Central Bank of the People's Republic of China
  - "Financial Cryptography Cup" is the highest level financial cryptography competition in China, hosted by the Digital Currency Research Institute of the Central Bank of the People's Republic of China.
- **Second Group Prize in the First Gansu Provincial University Competition on Blockchain Technology Application for Talent Employment and Entrepreneurship** *Jun. 2021*
  Awarded by Education Department of Gansu Province, China

Skills

- **Relevant Courses and Knowledge Areas:** Cryptography, Distributed Computing, Provable Security, Blockchain, Privacy Enhancing Technologies, Abstract Algebra, Discrete Mathematics
- **Programming Languages:** Golang, Python, C/C++, Java, SQL
- **Tools & Technologies:** LaTeX, Git, AWS Cloud Deployment, MATLAB