

CONG ZHANG

Beijing, China

zhangcong@mail.tsinghua.edu.cn ♦ github.com/zhangcong12343

INTRODUCTION

I am currently a postdoctoral fellow at the Institute for Advanced Study, Tsinghua University, Beijing, China. My collaborating supervisor is Prof. Xiaoyun Wang. Prior to this, I received my Bachelor's degree in mathematics from Shandong University China in 2018 and obtained my Ph.D. degrees in Institute of Information Engineering, Chinese Academy of Sciences in 2023.

My main research focus is on cryptographic protocols for secure computation. I am interested in both theoretical and practical aspects of secure computation techniques. More specifically:

- **General Multi-Party Computation Protocols**, especially Garbled Circuit (GC) and Secret Sharing based protocols.
- **Specific Protocols**, especially Private Set Operations (PSO), Private Information Retrieval (PIR) etc.

EXPERIENCE

Institute for Advanced Study, Tsinghua University	2024.01- Now
Postdoctoral researcher. Advisor: Prof. Xiaoyun Wang	
Alibaba Group	2023.07 - 2023.10
Research Intern, with Dr. Weiran Liu and Dr. Liqiang Peng	

EDUCATION

Ph.D. , Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China	2018 - 2023
<ul style="list-style-type: none">• Research directions: Cryptographic Protocols for Secure Computation• Thesis: Research on Secure Multiparty Computation for Privacy Protection	
Bachelor , Shandong University, Shandong, China	2014 - 2018

PUBLICATIONS

- **Cong Zhang**, Shuaishuai Li, and Dongdai Lin. Amortizing Division and Exponentiation. In the 18th International Conference on Information Security and Cryptology, Inscrypt 2022.
- **Cong Zhang**, Yu Chen, Weiran Liu, Min Zhang, and Dongdai Lin. Linear Private Set Union from Multi-Query Reverse Private Membership Test. In 32nd USENIX Security Symposium 2023.
- **Cong Zhang**, Weiran Liu, Bolin Ding, and Dongdai Lin. Efficient Private Multiset ID Protocols. In the 25th International Conference on Information and Communications Security, ICICS 2023.
- **Cong Zhang**, Yu Chen, Weiran Liu, Liqiang Peng, Meng Hao, Anyu Wang and Xiaoyun Wang. Unbalanced Private Set Union with Reduced Computation and Communication. In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security, CCS 2024.
- **Cong Zhang**, Liqiang Peng, Weiran Liu, Shuaishuai Li, Meng Hao, Lei Zhang, and Dongdai Lin. Charge Your Client: Payable Secure Computation and Its Applications. In IEEE Transactions on Information Forensics and Security, TIFS 2025.
- Shuaishuai Li, **Cong Zhang**, and Dongdai Lin. Secure Multiparty Computation with Lazy Sharing. In Proceedings of the 2024 ACM SIGSAC Conference on Computer and Communications Security, CCS 2024.
- Shuaishuai Li, **Cong Zhang**, and Dongdai Lin. Oblivious Transfer from Rerandomizable PKE. In the 25th International Conference on Information and Communications Security, ICICS 2023.

- Rui Zhang, Huan Zou, **Cong Zhang**, Yuting Xiao, and Yang Tao. Distributed Key Generation for SM9-based Systems. In the 16th International Conference on Information Security and Cryptology, Inscrypt 2020.
- Binbin Tu, Yu Chen, Qi Liu, and **Cong Zhang**. Fast Unbalanced Private Set Union from Fully Homomorphic Encryption. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security, CCS 2023.
- Yu Chen, Min Zhang, **Cong Zhang**, Minglang Dong, and Weiran Liu. Private Set Operations from Multi-Query Reverse Private Membership Test. In Public Key Cryptography, PKC 2024.
- Meng Hao, Weiran Liu, Liqiang Peng, Hongwei Li, **Cong Zhang**, Hanxiao Chen, and Tianwei Zhang. Unbalanced Circuit-PSI from Oblivious Key-Value Retrieval. In 33rd USENIX Security Symposium 2024.
- Xiangling Zhang, **Cong Zhang**, Weiran Liu, and Yu Chen. A Survey on Key Data Structures in Private Set Operation. Journal of Cryptologic Research, 2024, 11(2): 263–281. [DOI: 10.13868/j.cnki.jcr.000679]
- Minglang Dong, **Cong Zhang**, Yujie Bai, and Yu Chen. Efficient Multi-Party Private Set Union Without Non-Collusion Assumptions. In 34th USENIX Security Symposium 2025.
- Binbin Tu, Yujie Bai, **Cong Zhang**, Yang Cao, and Yu Chen. Fast Enhanced Private Set Union in the Balanced and Unbalanced Scenarios. In 34th USENIX Security Symposium 2025.
- Meng Hao, Weiran Liu, Liqiang Peng, **Cong Zhang**, Pengfei Wu, Lei Zhang, Hongwei Li, and Robert H. Deng. Practical Keyword Private Information Retrieval from Key-to-Index Mappings. In 34th USENIX Security Symposium 2025.
- Shuaishuai Li, Liqiang Peng, Weiran Liu, **Cong Zhang**, Zhen Gu, and Dongdai Lin. BitBatSPIR: Efficient Batch Symmetric Private Information Retrieval from PSI. In IEEE Transactions on Dependable and Secure Computing, TDSC 2025.

PROFESSIONAL ACTIVITIES

External Reviewer: Inscrypt (2019,2022,2024), Asiacrypt (2020,2021,2023), ESORICS (2021,2022), PKC 2022, CCS 2022, ICICS 2023, NDSS 2025.

SELECTED AWARDS

- 2022 Fincrypto National Competition: Outstanding Winner
- 2023 Director Excellence Award of Institute of Information Engineering, Chinese Academy of Sciences
- 2024 Outstanding Graduates of Institute of Information Engineering, Chinese Academy of Sciences
- 2024 Distinguished Doctoral Dissertation Award of Chinese Association for Cryptologic Research

TALKS

Design of Two-Party Private Set Union Protocols

- Seminar on Cryptographic Algorithms for Confidential Computing, Institute of Information Engineering, Chinese Academy of Sciences, 2024.11
- Cross Forum of Young Scholars at Institute of Advanced Study, Tsinghua University, 2024.11

Unbalanced Private Set Union with Reduced Computation and Communication.,

- ACM CCS 2024, Salt Lake City, U.S.A., 2024.10

Secure Multiparty Computation with Lazy Sharing.,

- ACM CCS 2024, Salt Lake City, U.S.A., 2024.10

Efficient Private Multiset ID Protocols.,

- ICICS 2023, Nankai University, Tianjin, China, 2023.11

Linear Private Set Union from Multi-Query Reverse Private Membership Test.,

- USENIX Security 2023, Anaheim, CA, U.S.A., 2023.8

Amortizing Division and Exponentiation.,

- Inscrypt 2022, Online, 2022.12

SELECTED FUNDED PROGECTS

- “Research on Key Cryptographic Protocol in Privacy Computing” from NSFC (No. 62402272), 2025.01 - 2027.12, Total award: 30K RMB.