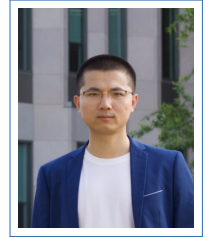# Chuan Zhao

Ph.D. in Computer Science

University of Jinan
School of Information Science and Engineering
✆ +1 (812)-671-2268
☎ +86 531 8276 7529
Skype:arronchuan
✉ ise_zhaoc@ujn.edu.cn
🖥 ujnccs.github.io/
No.336, Nanxinzhuang West Road, Jinan 250022, China

EDUCATION

Sep. 2011 – Jun. 2016
Ph.D. in Computer Science, *School of Computer Science and Technology*, Shandong University, Jinan, China.
With Prof. Qiuliang Xu

Sep. 2007 – Jun. 2011
Bachelor of Computer Science and Technology, *School of Mathematics and Computer Science*, Hunan Normal University, Changsha, China.
With Prof. Hong Liu

Exchange Student in Computer Science (Mar. 2009 – Mar. 2010), *School of Computer Science and Technology*, Korea National University of Education, Cheongju, Republic of Korea.
With Prof. Jinsoo Kim

WORK EXPERIENCE

Nov. 2018 – Present
Postdoctoral Researcher, *School of Informatics, Computing, and Engineering*, Indiana University, Bloomington, US.
With Prof. Yan Huang

Jul. 2016 – Present
Assistant Professor, *Shandong Provincial Key Laboratory for Network based Intelligent Computing, School of Information Science and Engineering*, University of Jinan, Jinan, China.
With Prof. Zhenxiang Chen

RESEARCH INTERESTS

- Applied Cryptography
- Privacy-Preserving Techniques
- Secure Multi-Party Computation
- Big Data Privacy
- Mobile Security

RESEARCH PROJECTS

Jan. 2018 – Dec. 2020
National Natural Science Foundation of China, "*Research on Efficient Secure Two-Party Computation for Privacy-Preserving Genomic Sequence Comparison*" (No. 61702218) (**Principal Investigator, PI**)

Jan. 2018 – Dec. 2020
Shandong Province Higher Educational Science and Technology Program, "*Research on Efficient and Secure Genomic Sequence Alignment in Cloud Environment*" (No. J18KA349) (**PI**)

Jan. 2019 – Dec. 2021
Project of Independent Cultivated Innovation Team of Jinan City, "*Research on Intelligent Mobile Malicious Application Behavior Detection*" (No. 2018GXRC002) (**Co-PI**)

Jan. 2016 – Dec. 2019
National Natural Science Foundation of China, "*Research on Theory of Secure Multi-Party Computation*" (No. 61572294) (**Co-PI**)

Jan. 2015 – Dec. 2017
Pre-research Project of General ∗ Department, "*Research on Efficient ∗ ∗ ∗ Computing on Encrypted Data*" (No. ∗ ∗ ∗) (**Co-PI**)

Jan. 2015 – Dec. 2017
Pre-research Project of General ∗ Department, "*Research on Keywords ∗ ∗ ∗ Querying Techniques*" (No. ∗ ∗ ∗) (**Co-PI**)

Jan. 2012 – Dec. 2015
National Natural Science Foundation of China, "*Research on Fundamental Theory of Secure Multi-Party Computation*" (No. 61173139) (**Co-PI**)

Jan. 2012 – Dec. 2014 Doctoral Fund of Ministry of Education of China, "*Research on Basic Operations of Secure Multi-Party Computation and Universally Composable Security*" (No. 20110131110027) (**Co-PI**)

SELECTED PUBLICATIONS

- Jian Qiu, Hengjian Li, **Chuan Zhao**, "*Cancelable palmprint templates based on random measurement and noise data for security and privacy-preserving authentication*". Published in *Computers & Security*. 2019.

- Minghao Zhao, Chengyu Hu, Xiangfu Song, **Chuan Zhao**, "*Towards dependable and trustworthy outsourced computing: A comprehensive survey and tutorial*". Published in *Journal of Network and Computer Applications*. 2019.

- **Chuan Zhao**, Shengnan Zhao, Minghao Zhao, Chong-Zhi Gao, Hongwei Li, Yu-an Tan. "*Secure Multi-Party Computation: Theory, Practice and Applications*". Published in *Information Sciences*. 2019.

- **Chuan Zhao**, Shengnan Zhao, Zhenxiang Chen, Bo Zhang, Mauro Conti. "*Secure Comparison under Ideal/Real Simulation Paradigm*". Published in *IEEE Access*. 2018.

- Bo Zhang, Tianqing Zhu, Chengyu Hu, **Chuan Zhao**. "*Cryptanalysis of a Lightweight Certificateless Signature Scheme for IIOT Environments*". Published in *IEEE Access*. 2018.

- Bo Zhang, Zhongtian Jia, **Chuan Zhao**. "*An Efficient Certificateless Generalized Signcryption Scheme*". Published in *Security and Communication Networks*. 2018.

- Anran Liu, Zhenxiang Chen, Shanshan Wang, Lizhi Peng, **Chuan Zhao**, Yuliang Shi. "*A Fast and Effective Detection of Mobile Malware Behavior Using Network Traffic*". Published in *The 18th International Conference on Algorithms and Architectures for Parallel Processing*. 2018.

- Shanshan Wang, Qiben Yan, Zhenxiang Chen, Bo Yang, **Chuan Zhao**, Mauro Conti. "*Detecting Android Malware Leveraging Text Semantics of Network Flows*". Published in *IEEE Transactions on Information Forensics and Security*. 2017.

- **Chuan Zhao**, Han Jiang, Qiuliang Xu, Yilei Wang, Xiaochao Wei, Shujie Cui. "*Fast Two-Output Secure Computation with Optimal Error Probability*". Published in *Chinese Journal of Electronics*. 2017.

- Hao Wang, Debiao He, Jian Shen, Zhihua Zheng, **Chuan Zhao**, Minghao Zhao. "*Verifiable Outsourced Ciphertext-Policy Attribute-Based Encryption in Cloud Computing*". Published in *Soft Computing*. 2017.

- **Chuan Zhao**, Han Jiang, Xiaochao Wei, Qiuliang Xu. "*Cut-and-Choose Bilateral Oblivious Transfer (in Chinese)*". Published in *Journal of Software*. 2017.

- Shanshan Wang, Qibei Yan, Zhenxiang Chen, Bo Yang, **Chuan Zhao**, Mauro Conti. "*TextDroid: Semantics-based Detection of Mobile Malware Using Network Flows*". Published in *2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*. 2017.

- Shanshan Wang, Zhenxiang Chen, Xiaomei Li, Lin Wang, Ke Ji, **Chuan Zhao**. "*TextDroid: Semantics-based Detection of Mobile Malware Using Network Flows*". Published in *The 13th International Conference on Intelligent Computing Theories and Application*. 2017.

- Ying Pang, Zhenxiang Chen, Xiaomei Li, Shanshan Wang, **Chuan Zhao**, Lin Wang, Ke Ji, Zicong Li. "*Finding Android Malware Trace from Highly Imbalanced Network Traffic*". Published in *2017 IEEE International Conference on Computational Science and Engineering and IEEE International Conference on Embedded and Ubiquitous Computing*. 2017.

- **Chuan Zhao**, Han Jiang, Qiuliang Xu, Xiaochao Wei, Hao Wang. "*Several Oblivious Transfer Variants in Cut-and-Choose Scenario*". Published in *International Journal of Information Security and Privacy*. 2016.

- Xiaochao Wei, Han Jiang, **Chuan Zhao**, Minghao Zhao, Qiuliang Xu. "*Fast Cut-and-Choose Bilateral Oblivious Transfer for Malicious Adversaries*". Published in *The 15th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. 2016.

- Xiaochao Wei, **Chuan Zhao**, Han Jiang, Qiuliang Xu, Hao Wang. "*Practical Server-Aided k-out-of-n Oblivious Transfer Protocol*". Published in *The 11th International Conference on Green, Pervasive and Cloud Computing*. 2016.

- Xiaochao Wei, Han Jiang, **Chuan Zhao**. "*An Efficient 1-out-of-n Oblivious Transfer Protocol with Full Simulation (in Chinese)*". Published in *Journal of Computer Research and Development*. 2016.

- **Chuan Zhao**, Han Jiang, Xiaochao Wei, Qiuliang Xu, Minghao Zhao. "*Cut-and-Choose Bilateral Oblivious Transfer and Its Application*". Published in *The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*. 2015.

- Yilei Wang, **Chuan Zhao**, Qiuliang Xu, Zhihua Zheng, Zhenhua Chen, Zhe Liu. "*Fair Secure Computation with Reputation Assumptions in the Mobile Social Networks*". Published in *Mobile Information Systems*. 2015.
- Yilei Wang, Duncan S. Wong, **Chuan Zhao**, Qiuliang Xu. "*Fair Two-Party Computation with Rational Parties Holding Private Types*". Published in *Security and Communication Networks*. 2015.
- Hao Wang, **Chuan Zhao**, Qiuliang Xu, Yilei Wang. "*Identity-Based Authenticate Key Exchange Protocol from Lattice*". Published in *The 9th International Conference on Computational Intelligence and Security*. 2013.

TALKS AND TRAINING

Paper Presentation at Helsinki, Finland

Title **Cut-and-Choose Bilateral Oblivious Transfer and Its Application**

In "*The 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications*", August 21, 2015.

Winter School at Tel Aviv, Israel

Topic **Advances in Practical Multiparty Computation**

In "*The 5th Bar-Ilan Winter School on Cryptography*", February 15-19, 2015.

Ph.D. THESIS

Title **RESEARCH ON THEORY OF PRACTICAL SECURE TWO-PARTY COMPUTATION**

Advised by Prof. Qiuliang Xu

Abstract Secure Multi-Party Computation (SMPC) focuses on the problem of cooperative computing on private data owned by several participants in a secure way in the distributed computing scenario. As a special case of SMPC, Secure Two-Party Computation (S2PC) formalizes many tasks, such as commitment schemes, zero-knowledge proof, oblivious transfer, etc. In recent years, research on practical SMPC has attracted wide attention from the international research community. In this thesis, we focus on the fundamental theory in constructing practical generic S2PC protocols with strong security. One of the most efficient methods of constructing generic protocols in malicious model is to apply cut-and-choose technique for garbled circuits. With this method, one can construct efficient generic protocols with provable security under ideal/real simulation paradigm, which proves to imply the strongest security level in reality. However, there are still many issues which are not addressed well in cut-and-choose based S2PC protocols, such as input consistency of participants, selective failure attack in oblivious transfer, two-output function computation, etc. This thesis studied the above issues and did some deep research from two aspects. First, we studied oblivious transfer, one of the most important tools of secure computation. In this thesis, the functionality of oblivious transfer was extended and two new primitives were proposed. The new proposed primitives can be applied in S2PC generic protocols so as to decrease the round complexity. Second, we studied two-output function and proposed an optimal paradigm to complete two-output secure computation. Based on this new paradigm, one can design faster two-output secure computation protocols with optimal error probability.

TEACHING

Graduate Course

- "*Network Security & Information Privacy*", School of Information Science and Engineering, University of Jinan
- "*Advanced Computer Network*", School of Information Science and Engineering, University of Jinan

Undergraduate Course

- "*Applied Cryptography*", School of Information Science and Engineering, University of Jinan
- "*Network Security Protocols*", School of Information Science and Engineering, University of Jinan
- "*Network Information Confrontation*", School of Information Science and Engineering, University of Jinan