

# **Yaxi Yang, Ph.D.**

✉ yxyangjnu@gmail.com  
LinkedIn <https://www.linkedin.com/in/yaxi-yang-722bb9236/>

## **Employment History**

- 2025.10 – ··· ··· Nanyang Technological University, Research Fellow  
2023.07 – 2025.10 Singapore University of Technology and Design, Research Fellow

## **Education**

- 2017 – 2023 Ph.D., Jinan University, Guangzhou, China  
Information Security. Supervised by: Jian Weng  
2022.09 – 2022.12 Visiting, University of Surrey, Guildford, UK  
Supervised by: Liqun Chen  
2021.12 – 2022.09 Visiting, Newcastle University, Newcastle, UK  
Supervised by: Changyu Dong  
2013 – 2017 B.Sc., Jinan University, Guangzhou, China  
Information Security.

## **Research Publications**

### **Conference Proceedings**

- 1 Fangyuan Sun, **Yaxi Yang**, Jia Yu, and Jianying Zhou, “Pacs: Privacy-preserving attribute-driven community search over attributed graphs,” in *Proceedings of the 33rd Annual Network and Distributed System Security Symposium (NDSS)*, 2026.
- 2 Ye Dong, Xudong Chen, Xiangfu Song, **Yaxi Yang**, Tianwei Zhang, and Jin-Song Dong, “Mizar: Boosting secure three-party deep learning with co-designed sign-bit extraction and gpu acceleration,” in *Annual Computer Security Applications Conference (ACSAC)*, 2025.
- 3 Weizhan Jing, Xiaojun Chen, Xudong Chen, Ye Dong, **Yaxi Yang**, and Qiang Liu, “Vcr: Fast private set intersection with improved vole and crt-batching,” in *24th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (Trustcom)*, 2025.
- 4 **Yaxi Yang**, Ivan Christian, Zeyu Yang, Jiaqi Yang, Huibin Wang, Zheng Yang, and Jianying Zhou, “Authplc: Authenticating plc communication using st-based extended cryptographic library,” in *Proceedings of the 11th ACM Cyber-Physical System Security Workshop (CPSS)*, 2025, pp. 19–30.
- 5 **Yaxi Yang**, Xiaojian Liang, Xiangfu Song, Ye Dong, Linting Huang, Hongyu Ren, Changyu Dong, and Jianying Zhou, “Maliciously secure circuit private set intersection via spdz-compatible oblivious prf,” in *Privacy Enhancing Technologies Symposium (PETS)*, 2025.
- 6 **Yaxi Yang**, Jian Weng, Yufeng Yi, Changyu Dong, Leo Yu Zhang, and Jianying Zhou, “Predicate private set intersection with linear complexity,” in *International Conference on Applied Cryptography and Network Security (ACNS)*, Springer, Kyoto, Japan, 2023, pp. 143–166.

### **Journal Articles**

- 1 **Yaxi Yang**, Jian Weng, Yao Tong, Jia-Nan Liu, Zhenghao Wu, Leo Yu Zhang, and Anjia Yang, “Prigenx: Privacy-preserving query with anonymous access control for genomic data,” *IEEE Transactions on Dependable and Secure Computing*, 2024.

- 2 Caiqin Dong, Jian Weng, Jia-Nan Liu, Anjia Yang, Zhiqian Liu, **Yaxi Yang**, and Jianfeng Ma, "Maliciously secure and efficient large-scale genome-wide association study with multi-party computation," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1243–1257, 2022.
- 3 **Yaxi Yang**, Yao Tong, Jian Weng, Yufeng Yi, Yandong Zheng, Leo Yu Zhang, and Rongxing Lu, "Prirange: Privacy-preserving range-constrained intersection query over genomic data," *IEEE Transactions on Cloud Computing*, 2022.
- 4 Yufeng Yi, Wuzheng Tan, and **Yaxi Yang**, "Efficient privacy-preserving non-exhaustive nearest neighbor search of large-scale databases," *Journal of Information Security and Applications*, vol. 70, p. 103 335, 2022.
- 5 Wenjie Yang, Jian Weng, Anjia Yang, Congge Xie, and **Yaxi Yang**, "Notes on a provably-secure certificate-based encryption against malicious ca attacks," *Information Sciences*, vol. 463, pp. 86–91, 2018.

## Books and Chapters

- 1 Lulu Han, Wenli Xie, and **Yaxi Yang**, *Real-World Cryptography*. Posts & Telecommunications Press, 2022. ↗ URL: <https://book.douban.com/subject/36179106/>.

## Skills

- |                |                                                                                              |
|----------------|----------------------------------------------------------------------------------------------|
| Languages      | Strong reading, writing and speaking competencies for English (IELTS 7.0), Mandarin Chinese. |
| Research Field | Applied Cryptography, Secure Multiparty Computation, Private Set Intersection.               |

## Academic Service

- |                   |                                                                                                                                                                      |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Program committee | MetaCom 2025, 22nd Annual International Conference on Privacy, Security, and Trust (PST 2025), 11th ACM Cyber-Physical System Security Workshop (CPSS 2025).         |
| External reviewer | 31st Australasian Conference on Information Security and Privacy (ACISP 2026), 47th IEEE Symposium on Security and Privacy (EuroS&P 2026).                           |
| Journal reviewer  | IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Network Science and Engineering. |

## Miscellaneous Experience

### Awards and Achievements

- |      |                                                                                                       |
|------|-------------------------------------------------------------------------------------------------------|
| 2023 | First Prize. Guangdong Science and Technology Progress Award                                          |
| 2020 | National Bronze Award. China College Students "Internet+" Innovation and Entrepreneurship Competition |
| 2018 | 6th place in the group, iDash Competition                                                             |
| 2017 | Second-class scholarship for outstanding students. Awarded by Jinan University.                       |

### Projects

- |      |                                                                                                                       |
|------|-----------------------------------------------------------------------------------------------------------------------|
| 2019 | Public key cryptography. (61825203) National Science Fund for Distinguished Young Scholars                            |
| 2018 | Quantum-safe lightweight cryptography and security protocols. (61732021) National Natural Science Foundation of China |

## Patents

- 2020
- **Yaxi Yang**, Jian Weng, Jia-nan Liu, Ming Li, Caiqin Dong, Yuxian Li, Yijun Mao. A Verifiable Query Protocol over Outsourced Genomic Data (Chinese Patent) 202011473367.7
  - **Yaxi Yang**, Jian Weng, Zhenghao Wu, Jia-nan Liu. Secure Genomic Sequence Comparison Scheme with Anonymous Authentication (Chinese Patent) 202011590499.8
  - Jian Weng, Zhenghao Wu, **Yaxi Yang**, Zhufeng Ye, Yuxian Li. Privacy-preserving Financial Audit System based on Function Encryption (Chinese Patent) 202011184529.5
  - JianWeng, Hongwei Huang, **Yaxi Yang**, Weiqi Luo. SGX-based Efficient Deep Learning Method (Chinese Patent) 202010338636.2
- 2018
- Jian Weng, Bingwen Feng, **Yaxi Yang**, Kaimin Wei, Zhiquan Liu, Caiqin Dong. Privacy-Preserving Image Region Duplication Detection Scheme (PCT Patent) PCT/CN2018/121122