

# Yi LIU

i@liuyi.pro  
<https://liuyi.pro>

## Research Interests

---

Cryptography and network security, in particular: secure two-party/multi-party computation, zero-knowledge proofs, timed cryptography, blockchain-related applications.

## Employment

---

- **Jinan University (JNU)** April 2023 – Present
  - *Lecturer*, College of Cyber Security

## Education

---

- **The University of Hong Kong (HKU)** Sept. 2018 – Feb. 2023
  - *Ph.D.* in Computer Science
  - Joint Ph.D. Programme with SUSTech
  - Supervisors: Siu-Ming Yiu (HKU) and Qi Wang (SUSTech)
  - Thesis: Private Function Evaluation: Improvements and Applications
- **Southern University of Science and Technology (SUSTech)** Sept. 2014 – July 2018
  - *B.Eng.* in Computer Science and Technology
  - Thesis: An Evaluation System Based on Blockchain and Linkable Ring Signature.
    - \* Best Thesis Award in the CSE Department, SUSTech.

## Research Projects

---

- Research on the Design of New Secure Multi-Party Computation Protocols 2025 – 2026
  - Principal Investigator
  - Supported by the Guangzhou Municipal Fundamental and Applied Basic Research Special Topic Young Doctoral “Sail” Project (Grant No. 2025A04J2146).
- Design of Secure Multi-Party Computation Protocols in New Security Models 2024 – 2026
  - Principal Investigator
  - Supported by the Young Scientists Fund of the National Natural Science Foundation of China (Grant No. 62302194).

## Refereed Publications

---

- Zero-Knowledge Protocols with PVC Security: Striking the Balance between Security and Efficiency  
Yi Liu, Yipeng Song, Anjia Yang, Junzuo Lai  
The 27th International Conference on Information and Communications Security (**ICICS 2025**)  
[ePrint 2025/2146](#)

- Publicly Auditable Federated Learning with Privacy and Byzantine Robustness  
Huang Zeng, Anjia Yang, Jian Weng, Min-Rong CHen, Fengjun Xiao, Zilin Liu, [Yi Liu](#)  
IEEE Transactions on Dependable and Secure Computing (**TDSC**), 2025
- Highly Efficient Actively Secure Two-Party Computation with One-Bit Advantage Bound  
[Yi Liu](#), Junzuo Lai, Peng Yang, Anjia Yang, Qi Wang, Siu-Ming Yiu, Jian Weng  
The 46th IEEE Symposium on Security and Privacy (**S&P 2025**)  
[ePrint 2025/614](#)
- Towards Efficient and Practical Multi-party Computation under Inconsistent Trust in TEEs  
Xuanwei Hu, Rujia Li, [Yi Liu](#), Qi Wang  
The 46th IEEE Symposium on Security and Privacy (**S&P 2025**)
- Efficient and Privacy-Preserving Ride Matching over Road Networks against Malicious ORH server  
Mingtian Zhang, Anjia Yang, Jian Weng, Minrong Chen, Huang Zeng, [Yi Liu](#), Xiaoli Liu, Zhihua Xia  
IEEE Transactions on Information Forensics and Security (**TIFS**), 2025
- Enabling Privacy-Preserving and Publicly Auditable Federated Learning  
Huang Zeng, Anjia Yang, Jian Weng, Minrong Chen, Fengjun Xiao, [Yi Liu](#), Ye Yao  
IEEE International Conference on Communications (**ICC 2024**)
- MTDCAP: Moving Target Defense-Based CAN Authentication Protocol  
Heng Sun, Huibiao Su, Jian Weng, Zhiquan Liu, Ming Li, [Yi Liu](#), Yucheng Zhong, Wenzhen Sun  
IEEE Transactions on Intelligent Transportation Systems (**TITS**), 2024
- Robust Publicly Verifiable Covert Security: Limited Information Leakage and Guaranteed Correctness with Low Overhead  
[Yi Liu](#), Junzuo Lai, Qi Wang, Xianrui Qin, Anjia Yang, Jian Weng  
The 29th International Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT 2023**)  
[ePrint 2023/1392](#)
- Towards Practical Homomorphic Time-Lock Puzzles: Applicability and Verifiability  
[Yi Liu](#), Qi Wang, and Siu-Ming Yiu  
The 27th European Symposium on Research in Computer Security (**ESORICS 2022**)  
[ePrint 2022/585](#)
- Making Private Function Evaluation Safer, Faster, and Simpler  
[Yi Liu](#), Qi Wang, and Siu-Ming Yiu  
The 25th IACR International Conference on Practice and Theory of Public Key Cryptography (**PKC 2022**)  
[ePrint 2021/1682](#)
- Improved Zero-Knowledge Argument of Encrypted Extended Permutation  
[Yi Liu](#), Qi Wang, and Siu-Ming Yiu  
The 17th International Conference on Information Security and Cryptology (**Inscrypt 2021**)  
[ePrint 2021/1430](#)
- Blind Polynomial Evaluation and Data Trading  
[Yi Liu](#), Qi Wang, and Siu-Ming Yiu  
The 19th International Conference on Applied Cryptography and Network Security (**ACNS**

2021)

[ePrint 2021/413](#)

- An Improvement of Multi-Exponentiation with Encrypted Bases Argument: Smaller and Faster

[Yi Liu](#), [Qi Wang](#), and [Siu-Ming Yiu](#)

The 16th International Conference on Information Security and Cryptology (**Inscrypt 2020**)

[ePrint 2020/567](#)

## Manuscripts

---

- An E-voting Protocol Based on Blockchain

[Yi Liu](#) and [Qi Wang](#)

[ePrint 2017/1043](#)

## Talks

---

- Robust Publicly Verifiable Covert Security: Limited Information Leakage and Guaranteed Correctness with Low Overhead.  
The 29th International Conference on the Theory and Application of Cryptology and Information Security (**ASIACRYPT 2023**).  
Guangzhou, China. Dec. 2023.
- Towards Practical Homomorphic Time-Lock Puzzles: Applicability and Verifiability.  
The 27th European Symposium on Research in Computer Security (**ESORICS 2022**).  
Copenhagen, Denmark. Sept. 2022.
- Making Private Function Evaluation Safer, Faster, and Simpler.  
The 25th IACR International Conference on Practice and Theory of Public Key Cryptography (**PKC 2022**).  
Virtual. Mar. 2022.
- Improved Zero-Knowledge Argument of Encrypted Extended Permutation.  
The 17th International Conference on Information Security and Cryptology (**Inscrypt 2021**).  
Virtual. Aug. 2021.
- Blind Polynomial Evaluation and Data Trading.  
The 19th International Conference on Applied Cryptography and Network Security (**ACNS 2021**).  
Virtual. Jun. 2021.
- An Improvement of Multi-Exponentiation with Encrypted Bases Argument: Smaller and Faster.  
The 16th International Conference on Information Security and Cryptology (**Inscrypt 2020**).  
Guangzhou, China. Dec. 2020.

## Teaching

---

- **Undergraduate Courses**

- |   |     |
|---|-----|
| – C++ Programming (Fall 2025, Fall 2024, Fall 2023) | JNU |
| – Public Key Cryptography (Spring 2025)             | JNU |
| – Advanced Cryptography Practice (Fall 2025)        | JNU |

- **Graduate Courses**

## Professional Activities

---

- **Journal Reviewer**

IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Industrial Informatics, International Journal of Information Security, Web Intelligence

- **Conference Reviewer**

IEEE BSC@QRS (2022, 2021, 2020)

- **Membership**

IEEE Membership (2025), IACR Regular Membership (2023), CACR Regular Membership (2024), IACR Student Membership (2022, 2021, 2020, 2019)

## Other Experience

---

- Teaching Assistant

- |  |         |
|--|---------|
| – COMP2119: Introduction to Data Structures and Algorithms (Fall 2021) | HKU     |
| – CS403: Cryptography and Network Security (Fall 2019, Fall 2020)      | SUSTech |
| – COMP7904: Information Security: Attacks and Defense (Spring 2019)    | HKU     |
| – CS304: Software Engineering (Spring 2017)                            | SUSTech |
| – CS201: Discrete Mathematics (Fall 2016)                              | SUSTech |
| – CS302: Operating System (Spring 2016)                                | SUSTech |