刘 逸

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

研究兴趣

密码学与网络安全，特别是安全两方/多方计算（2PC/MPC）、零知识证明（Zero-Knowledge Proofs），定时密码学（Timed Cryptography），以及区块链相关应用（Blockchain-Related Applications）。

职业经历

- 暨南大学   2023.4 至今
  讲师，网络空间安全学院

教育背景

- 香港大学   2018.9 – 2023.2
  计算机科学博士（香港大学-南方科技大学联合培养博士项目）
  导师：姚兆明 *Siu-Ming Yiu*（香港大学），王琦（南方科技大学）
  毕业论文：Private Function Evaluation: Improvements and Applications

- 南方科技大学   2014.9 – 2018.7
  工学学士（计算机科学与技术）
  导师：王琦
  毕业论文：An Evaluation System Based on Blockchain and Linkable Ring Signature
  ⋆ 南方科技大学计算机科学与工程系最佳论文奖

研究项目

- 新型安全多方计算协议设计研究   2025 – 2026
  - 项目负责人
  - 广州市基础与应用基础研究专题（青年博士"启航"项目）（No. 2025A04J2146）

- 新型安全模型中的安全多方计算协议设计   2024 – 2026
  - 项目负责人
  - 国家自然科学基金青年科学基金项目（No. 62302194）

已发表论文

- 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, <u>Yi Liu</u>
  IEEE Transactions on Dependable and Secure Computing (**TDSC**), 2025

- Highly Efficient Actively Secure Two-Party Computation with One-Bit Advantage Bound
  <u>Yi Liu</u>, 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, <u>Yi Liu</u>, 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, <u>Yi Liu</u>, 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, <u>Yi Liu</u>, 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, <u>Yi Liu</u>, 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
  <u>Yi Liu</u>, 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
  <u>Yi Liu</u>, 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
  <u>Yi Liu</u>, 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
  <u>Yi Liu</u>, 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
  <u>Yi Liu</u>, 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

其他论文

- An E-voting Protocol Based on Blockchain
  Yi Liu and Qi Wang
  ePrint 2017/1043

学术报告

- 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.

教学

- 本科课程

  - C++ 程序设计（2025 年秋季，2024 年秋季，2023 年秋季）　　　　　　　暨南大学
  - 公钥密码（2025 年春季）　　　　　　　　　　　　　　　　　　　　　　暨南大学
  - 高级密码学实践（2025 年秋季）　　　　　　　　　　　　　　　　　　　暨南大学

- **研究生课程**
  - 高级密码学（2025 年秋季，2024 年秋季，2023 年秋季）   暨南大学

学术活动

- **期刊审稿**

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

- **会议审稿**

  IEEE BSC@QRS (2022, 2021, 2020)

- **会员资格**

  IEEE 会员（2025），IACR 会员（2023），中国密码学会会员（2024，2023），IACR 学生会员 (2022, 2021, 2020, 2019)

其他经历

- **助教**
  - COMP 2119：数据结构与算法（2021 年秋季）   香港大学
  - CS403：密码学与网络安全（2019 年秋季, 2020 年秋季）   南方科技大学
  - COMP7904：信息安全：攻击与防御（2019 年春季）   香港大学
  - CS304：软件工程（2017 年春季）   南方科技大学
  - CS201：离散数学（2016 年秋季）   南方科技大学
  - CS302：操作系统（2016 年春季）   南方科技大学