

刘逸

(+86) 130-1667-4179 · 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

- 讲师 网络空间安全学院，暨南大学 2023.4 至今

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)
 - 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

已发表论文

- 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**).
<https://eprint.iacr.org/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**).
<https://eprint.iacr.org/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**).
<https://eprint.iacr.org/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**).
<https://eprint.iacr.org/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**).
<https://eprint.iacr.org/2020/567>

其他论文

- An E-voting Protocol Based on Blockchain.
Yi Liu and Qi Wang.
Manuscript, 2017.
在线版本: <https://eprint.iacr.org/2017/1043>

学术报告

- 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.

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
- 研究助理
 - 南方科技大学编码理论与密码学实验室 2016.9 – 2018.8
 - * 导师: 王琦
 - * 成果一: An E-voting Protocol Based on Blockchain. (Manuscript)
 - * 成果二: An Evaluation System Based on Blockchain and Linkable Ring Signature. (本科毕业论文)

学术活动

- 会员资格 IACR 学生会员 (2022, 2021, 2020, 2019)
- 期刊审稿 International Journal of Information Security
- 会议审稿 IEEE BSC@QRS (2022, 2021, 2020)