

# 刘逸

(+86) 130-1667-4179 · mail@imliuyi.com

<https://imliuyi.com>

## 研究兴趣

---

密码学与网络安全，特别是安全两方/多方计算 (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)。

## 教育背景

---

香港大学

2018.9 至今

- 计算机科学在读博士研究生
- 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)

南方科技大学

2014.9 - 2018.7

- 工学学士 (计算机科学与技术)
- GPA: 3.84/4.00 (专业核心课程); 3.70/4.00 (所有课程)
- 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

---

1. Making Private Function Evaluation Safer, Faster, and Simpler.  
Yi Liu, Qi Wang, Siu-Ming Yiu.  
To appear in The 25th IACR International Conference on Practice and Theory of Public Key Cryptography (**PKC 2022**).  
在线版本: <https://eprint.iacr.org/2021/1682>
2. Improved Zero-Knowledge Argument of Encrypted Extended Permutation.  
Yi Liu, Qi Wang, Siu-Ming Yiu.  
The 17th International Conference on Information Security and Cryptology (**Inscrypt 2021**).  
在线版本: <https://eprint.iacr.org/2021/1430>
3. Blind Polynomial Evaluation and Data Trading.  
Yi Liu, Qi Wang, Siu-Ming Yiu.  
The 19th International Conference on Applied Cryptography and Network Security (**ACNS 2021**).  
在线版本: <https://eprint.iacr.org/2021/413>
4. An Improvement of Multi-Exponentiation with Encrypted Bases Argument: Smaller and Faster.  
Yi Liu, Qi Wang, Siu-Ming Yiu.  
The 16th International Conference on Information Security and Cryptology (**Inscrypt 2020**).  
在线版本: <https://eprint.iacr.org/2020/567>

## 预发表论文

---

1. Towards Practical Homomorphic Time-Lock Puzzles: Usability and Verifiability.  
Yi Liu, Qi Wang, Siu-Ming Yiu.  
Manuscript, 2022.

2. 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

---

- 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. June 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. 2021.

## 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 (毕业论文)

## 学术活动

---

成员 IACR 学生会会员

审稿 IEEE BSC@QRS (2021, 2020)

## 技能

---

语言 中文 (母语), 英文 (流畅)

编程 C/C++, Python