Yi Liu

(+86) 130-1667-4179 · i@liuyi.pro · Guangzhou, China
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

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

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.

Refreed Publications

- 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

Manuscripts

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

Talks

- 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.

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
- Research Assistant at CoCrypto Lab, SUSTech Sept. 2016 – Aug. 2018
  - Adviser: Qi Wang
  - Result I: An E-voting Protocol Based on Blockchain. (Manuscript)
  - Result II: An Evaluation System Based on Blockchain and Linkable Ring Signature. (Undergraduate Thesis)

Professional Activities

- **Membership** IACR Student (2022, 2021, 2020, 2019)
- **Journal Reviewer** International Journal of Information Security
- **Conference Reviewer** IEEE BSC@QRS (2022, 2021, 2020)