# Yi Liu

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

## Research Interests

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

## Education

**The University of Hong Kong (HKU)** Sept. 2018 – Present

- Ph.D. candidate in Computer Science
- Joint Ph.D. Programme with SUSTech
- Supervisors: Siu-Ming Yiu (HKU) and Qi Wang (SUSTech)

**Southern University of Science and Technology (SUSTech)** Sept. 2014 – July 2018

- B.Eng. in Computer Science and Technology
- GPA: 3.84/4.00 (Core); 3.70/4.00 (Overall)
- Thesis: An Evaluation System Based on Blockchain and Linkable Ring Signature.
  - Best Thesis Award in the CSE Department, SUSTech.

## Refreed Publications

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**).
   Online Version: 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**).
   Online Version: 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**).
   Online Version: 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**).
   Online Version: https://eprint.iacr.org/2020/567

## Manuscripts

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.
   Online Version: https://eprint.iacr.org/2017/1043

## Talks

- 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.

## 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 1: An E-voting Protocol Based on Blockchain (Manuscript)
  - Result 2: An Evaluation System Based on Blockchain and Linkable Ring Signature (Undergraduate Thesis)

## Professional Activities

**Membership** IACR student Member
**External Reviewer** IEEE BSC@QRS (2021, 2020)

## Skills

**Languages** Chinese (Native), English (Fluent)
**Programming Skills** C/C++, Python