Xinyu Li   Email: xinyuli1920@gmail.com   Web: https://lixinyu2016.github.io/xinyuli/

Name: Xinyu Li
Day of Birth: 1989.08
Education: PhD
Address: Rm 207, Chow Yei Ching Building, The University of Hong Kong
Phone: +85297023548

Research Interest：Applied Cryptography

- Cryptographic protocols
- Provable security
- Blockchain Security

Working Experience

Post-doctoral Fellow, working with Prof. Man Ho Au   2020.12 — now
Department of Computer Science, The University of Hong Kong, Hong Kong

Education

- PhD of Computer Science and Technology   2016.09 — 2020.09
  University of Chinese Academy of Sciences, Beijing, China
  Advisor: Prof. Jing Xu

- Joint Master Program   2014.09 — 2016.06
  Institute of Software, Chinese Academy of Sciences, Beijing, China
  Advisor: Prof. Jing Xu and Prof. Zhenfeng Zhang

- Master of Electronic and Communication Engineering   2013.09 — 2016.06
  University of Science and Technology of China, Hefei, China
  Advisor: Prof. Dengguo Feng and Prof. Honggang Hu

- Bachelor of Information Security   2009.09 — 2013.06
  University of Science and Technology of China, Hefei, China
  Thesis advisor: Prof. Zhenfeng Zhang

Articles

1. **Xinyu Li,** Jing Xu, Zhenfeng Zhang, Dengguo Feng: On the security of TLS resumption and renegotiation, *China Communications*, 2016, 13(12): 176--188.

2. **Xinyu Li,** Jing Xu, Zhenfeng Zhang, Dengguo Feng, Honggang Hu: Multiple handshakes security of TLS 1.3 candidates, *IEEE Symposium on Security and Privacy (S&P)*, 2016, 486–505. (Acceptance Rate: 13.8%)

3. Bingyong Guo, **Xinyu Li***：Multi-valued Byzantine Consensus Scheme with High Transmission Efficiency, *Journal of Cryptologic Research*, 2018, 5(5)：516-528.

4. **Xinyu Li,** Jing Xu, Zhenfeng Zhang: Revisiting the Security of Qian et al.'s Revised Tree- LSHB+ Protocol. *Wireless Personal Communications*, 2019, 106(2):321–343.

5. **Xinyu Li**, Jing Xu, Zhenfeng Zhang, Xiao Lan, Yuchen Wang: Modular Security Analysis of OAuth 2.0 in the Three-Party Setting. *IEEE European Symposium on Security and Privacy (EuroS&P)*, 2020, 276--293. (Acceptance Rate: 14.5%)

6. **Xinyu Li,** Jing Xu, Xiong Fan, Yuchen Wang, Zhenfeng Zhang: Puncturable Signatures and Applications in Proof-of-Stake Blockchain Protocols. *IEEE Transactions on Information Forensics and Security (TIFS)*, 2020, 15:3872--3885.

7. **Xinyu Li,** Jing Xu, Lingyuan Yin, Yuan Lu, Qiang Tang, Zhenfeng Zhang: Escaping from Consensus: Instantly Redactable Blockchain Protocols in Permissionless Setting. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2022.

8. Lixin Liu, **Xinyu Li**, Man Ho Au, Zhuoya Fan, Xiaofeng Meng: Metadata Privacy Preservation for Blockchain-Based Healthcare Systems. *International Conference on Database Systems for Advanced Applications (DASFAA)*, 2022, 404–412. (Acceptance Rate: 27.3%)

9. Chengru Zhang, **Xinyu Li* (corresponding author)**, Man Ho Au: ePoSt: Practical and Client-friendly Proof of Storage-Time. *IEEE Transactions on Information Forensics and Security (TIFS)*, 2022.

10. **Xinyu Li,** Jing Xu, Man Ho Au, Chengru Zhang: General design of (tag-based) puncturable signature and its application. (Manuscript)

Honors and Awards

"New academic star", InForSec, Tsinghua University, 2016.

Patents

1. **A puncturable signature scheme**
   Jing Xu, **Xinyu Li** and Zhenfeng Zhang
   Patent number: ZL 201910279881.8, CN.
2. **Tag based puncturable signature and its application in PoS blockchain protocols**
   Jing Xu, **Xinyu Li**, Zhenfeng Zhang and Xinlei Zhai
   Patent number: ZL 201910917779.6, CN

Academic Service

- Conference Review：FC (2017), ACM CCS (2019), ASIACRYPT (2020), ESORICS (2020), ACM ASIACCS (2020,2021,2022), ACNS(2021), CT-RSA(2022).
- Journal Review：TSC (2018), TMC (2019), TDSC(2021), JISAS(2021,2022).