RESUME

Name: Xinyu Li
Day of Birth: 1989.08
Education: PhD
Address: Rm 207, Chow Yei Ching Building, The University of Hong Kong, Pokfulam, Hong Kong.
Phone: +85297023548
E-mail: xinyuli1920@gmail.com

Working Experience:

2020.12 – : Department of Computer Science, The University of Hong Kong. (**Postdoctoral Fellow**)

Education:

2016.09 – 2020.09: University of Chinese Academy of Sciences, Computer Science and Technology (**Doctor**)
2013.09 – 2016.06: University of Science and Technology of China, Electronic and Communication Engineering. (**Master**)
2009.09 – 2013.06: University of Science and Technology of China, Information Security. (**Bachelor**)

Honors and Scholarly Recognition:

1. Received the Second-class academic scholarship, University of Chinese Academy of Sciences, 2016-2018
2. Received the Merit Student award, University of Chinese Academy of Sciences, 2017
3. Received the Excellent League Member award, University of Science and Technology of China, 2012
4. Received the Third-class outstanding Freshman Scholarship, University of Science and Technology of China, 2009

Research Interests:

Applied Cryptography, Provable Security, Authenticated Key Establishment Protocols, Blockchain Security

Publications:

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. **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.

4. **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%)

5. **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.

6. **Xinyu Li,** Jing Xu, Lingyuan Yin, Yuan Lu, Qiang Tang, Zhenfeng Zhang: Escaping from Consensus: Instantly Redactable Blockchain Protocols in Permissionless Setting. (Under revision for TDSC)

7. Chengru Zhang, **Xinyu Li***, Man Ho Au: ePoSt: Practical and Client-friendly Proof of Storage-Time. (Manuscript)

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

Patents:

1. Jing Xu, Xinyu Li, Zhenfeng Zhang. A puncturable signature scheme. 2019102798818.
2. Jing Xu, Xinyu Li, Zhenfeng Zhang, Xinlei Zhai. Tag based puncturable signature and its application in PoS blockchain protocols. 2019109177796.