李新宇 Email: xinyuli1920@gmail.com Web: https://lixinyu2016.github.io/xinyuli/

姓名: 李新宇
学历: 博士
地址: 香港大学周亦卿楼 207 室
联系电话: +85297023548

研究兴趣：应用密码学

- 密码协议
- 可证明安全
- 区块链安全

工作经历

- 博士后研究员， 香港大学，计算机科学系，合作导师：区文浩教授 2020.12 —— 至今

教育背景

- 博士，中国科学院大学，计算机科学与技术 （导师：徐静） 2016.09 —— 2020.09
- 硕士联合培养，中国科学院软件研究所（导师：徐静、张振峰） 2014.09 —— 2016.06
- 硕士，中国科学技术大学，电子与通信工程（导师：冯登国、胡红钢） 2013.09 —— 2016.06
- 学士，中国科学技术大学，信息安全 （论文导师：张振峰） 2009.09 —— 2013.06

论文

(1) **Xinyu Li,** Jing Xu, Zhenfeng Zhang, Dengguo Feng: On the security of TLS resumption and renegotiation, ***China Communications***, 2016, 13(12): 176--188. (SCI)
中国通信学会推荐 A 类国内期刊

(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%)
网络安全四大国际顶级会议之一，CCF 推荐网络与信息安全 A 类会议，接受率 13.8%。大陆科研机构作为第一单位在该会议发表的第 7/8 篇论文，也是大陆学者独立完成的第 1 篇论文。
1. 同行审稿评论“迄今为止针对 TLS 1.3 最强的密码分析结果”；
2. 文章被 IETF 在 TLS 1.3 标准文档 RFC 8446 中引用以论证其安全性；
3. 被顶级期刊 TDSC、顶级会议 IEEE S&P 和 CRYPTO 等中的文章引用作为 TLS 1.3 的重要安全性分析结果，据不完全统计，文章他引 40 余次（Google 学术检索）；
4. 国际互联网研究任务组 CFRG 主席、IACR Fellow、《Journal of Cryptology》主编 Kenny Paterson 教授评价“帮助建立了 TLS 1.3 协议设计的信心”。

(3) 郭兵勇，**李新宇***: 一个高传输效率的多值拜占庭共识方案。密码学报，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. (SCI)

(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%)
网络安全国际重要会议（B 类水平），接受率 14.5%。是该会议录取的大陆学者独立完成的第 1 篇论文。

(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.
CCF 推荐网络与信息安全 A 类期刊，SCI 一区

(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.
CCF 推荐网络与信息安全 A 类期刊

(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%)
CCF 推荐 B 类会议

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

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

荣誉

网络安全研究国际学术论坛（InForSec）学术新星奖，清华大学等， 2016 年

专利

(1) 徐静，**李新宇**，张振峰。**一种可刺穿的数字签名方法。**专利号：ZL 201910279881.8，中国。

(2) 徐静，**李新宇**，张振峰，翟欣磊。**带标签的私钥可更新数字签名方法及其在PoS区块链协议中的应用。**专利号：ZL 201910917779.6，中国。

学术服务

- 会议审稿：FC (2017), ACM CCS (2019), ASIACRYPT (2020), ESORICS (2020), ACM ASIACCS (2020,2021,2022), ACNS(2021), CT-RSA(2022).
- 期刊审稿：TSC (2018), TMC (2019), TDSC(2021), JISAS(2021,2022)