李新宇

出生年月： 1989 年 8 月
政治面貌：中共党员
联系电话：（+86） 131-2131-0816
邮箱： xinyu2016@iscas.ac.cn
研究方向：复杂网络环境下应用密码协议的设计与安全性分析

教育和工作经历

2020/11 – 至今 香港大学 计算机科学系 博士后研究员，**合作导师**：区文浩 教授
2016/09 – 2020/09 中国科学院软件研究所 可信计算与信息保障实验室 博士，**导师**：徐静 研究员
2014/09 – 2016/06 中国科学院软件研究所 可信计算与信息保障实验室 联合培养
2013/09 –2016/06 中国科学技术大学 中科院电磁空间信息重点实验室 硕士，
导师：冯登国 研究员、 胡红钢 教授
2009/09 – 2013/06 中国科学技术大学 信息安全专业 学士，**学位论文导师**： 张振峰 研究员

项目经历

(1) 高安全强度 SM2 公钥算法的实现与性能评估，实验室项目，2014.7 — 2014.10。
(2) 匿名认证协议的设计理论与分析方法研究，国家自然科学基金面上项目，2016-2019。
(3) 电子货币新算法与新原理研究，国家重点研发计划， 2017—2020。
(4) JDD-NJIT-ISCAS 区块链联合实验室研究，2019-2020。
(5) 共识协议的设计理论与分析方法研究，密码科学技术国家重点实验室重点课题，2019-2020。
(6) 抗量子隐私保护密码方案的关键技术研究，国家自然科学基金面上项目，2021—至今。

研究成果_论文

(1) **Xinyu Li,** Jing Xu, Zhenfeng Zhang, Dengguo Feng: On the security of TLS resumption and renegotiation, China Communications, 13(12):176—188, 2016. (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), 486–505, 2016.
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. 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”。
4. 作为 TLS 1.3 的重要安全性分析结果，文章被发表在顶级期刊 TDSC、顶级会议 IEEE S&P 和 CRYPTO 等中的文章引用，据不完全统计，文章被引 30 余次（Google 学术检索）。
5. 分析方法被 Chen 等学者在 ESORICS’19 (CCF 网络与信息安全 B 类会议) 的文章中使用。

(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，5(5):516-528，2018.（通讯作者）。

(4) **Xinyu Li,** Jing Xu, Zhenfeng Zhang: Revisiting the Security of Qian et al.'s Revised Tree- LSHB+ Protocol. Wireless Personal Communications, 106:321–343，2019. (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), 276-293, 2020.
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), 15:3872-3885, 2020.
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. 投稿中

研究成果_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：2019102798818. 已授权.
(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：2019109177796. 已授权.

已获得奖励

(1) “三好学生”荣誉称号，中国科学院大学，2017 年
(2) 二等国科大学业奖学金， 2016 年-2018 年
(3) 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
(4) “校优秀团员”荣誉称号，中国科学技术大学，2012 年
(5) “院优秀学生干部”荣誉称号， 中国科学技术大学， 2011 年