# 李新宇副研究员招收哈尔滨工业大学&&中关村实验室联合培养博士

## 导师简介

李新宇，现任北京中关村实验室副研究员，国家海外高层次青年人才计划入选者，哈尔滨工业大学兼职博士生导师。他于 2020 年于中国科学院大学获得博士学位，在加入实验室之前，曾在香港大学从事博士后研究。他对安全协议、区块链/车联网/物联网/5g 通信/外包存储等实际系统安全、应用密码学、可证明安全等方向的研究有广泛的兴趣。近年来以第一/通讯作者身份在网络安全领域国际顶级会议和期刊 IEEE S&P、IEEE TDSC、IEEE TIFS 和 IEEE EuroS&P 等发表多篇学术论文，获得多项国家发明专利。 成果得到了包括 IACR Fellow 在内的众多学者以及顶级会议/期刊文章的积极评价和引用，并在京东和华为等互联网企业得到应用。其关于 TLS 等国际标准的可证明安全工作已入选密码理论与技术丛书《安全认证协议——基础理论与方法》， 相关成果还获得了国际标准 TLS 1.3 的引用，成为 TLS 标准 20 多年历史上引用的唯一来自中国的研究成果(详见个人主页：https://dblp.org/pid/63/6849.html )。

## 团队简介

申请人所在的安全协议团队长期致力于密码学理论、密码应用、安全协议等领域的研究，团队在中关村实验室拥有成员十余名，含中科院院士 1 名，研究员 6 名，副研究员 1 名，团队成员在 CRYPTO、EUROCRYPT、IEEE S&P、ACM CCS、NDSS 等网络安全、密码学领域国际顶级会议和期刊上发表了一系列高质量论文，多次得到国际著名专家的正面引用和高度评价，主持研制国际和国家标准 20 多项，荣获国家科技进步奖一等奖、国家技术发明奖二等奖等多项奖励。
同时，项目团队与香港大学、香港理工大学、悉尼大学、康奈尔大学、中国科学院、中国科学技术大学、西安电子科技大学等国内外多个一流科研机构保持着良好学术交流和合作关系。

## 招生方向

围绕网络空间安全需求，开展以下（包含但不局限于）相关研究：

- 安全协议：研究密钥协商、安全多方计算、身份认证等安全协议的设计与分析
- 实际系统安全：研究区块链、车/物联网、5g 通信、外包存储等实际系统的安全保障机制
- 应用密码学：研究传统和后量子密码算法及分析技术在实际中的应用
- 可证明安全：研究主流网络安全国际/国内标准在复杂网络环境中的可证明安全性

## 招生要求

- 对学术研究具有兴趣；
- 工作认真负责，态度严谨；
- 具有较好的英文文献阅读、写作能力；
- 品格端正，情绪稳定，乐于沟通；
- 编程基础扎实，具备工程经验；
- 硕士生发表过高水平期刊、会议论文者优先考虑；

**申请方式**

有意向申请的同学，请把 CV 和研究兴趣简要发送至邮箱 lixy@mail.zgclab.edu.cn。邮件名格式为：“博士申请 |推免 or 非推免| 姓名 | 学校 | 专业”，其中，推免生申请截止时间为：2025 年 8 月 20 日。

**科研环境**

中关村实验室是中央管理的国家网络信息领域的新型科研事业单位。中关村实验室主体位于中关村科学城北区。中关村实验室聚焦国家网络信息领域的重大目标使命，开展战略性、前瞻性、基础性重大科学问题和关键核心技术研究；探索新型科研机构管理体制机制创新；聚焦培育高端创新人才，推动网络信息领域的产学研融通科技创新，开展与国内外相关机构和组织的交流合作，打造突破性、引领型、平台型一体化的世界一流实验室。

**资源和保障：**

学生同时享受哈尔滨工业大学与中关村实验室提供的服务保障，第一年在哈尔滨工业大学完成课程学习，之后在中关村实验室完成科研工作。其中，中关村实验室提供免费宿舍、免费三餐、免费健身房、免费班车等；联合培养博士研究生毕业后在应聘中关村实验室时具有明显的优势，此外，优秀者可推荐至境外高水平科研机构深造。