

陆正昊 Emison Lu

+86 15715880829 | lzh1633856298@sjtu.edu.cn | EmisonLu(微信) | 性别: 男 | 现居地: 上海

Github: <https://github.com/EmisonLu>

教育背景

上海交通大学 电子信息与电气工程学院 信息安全专业 2018.09-2022.06

- GPA: 3.93/4.3 专业排名: 2/127
- 研究方向: 隐私保护、可信执行环境、SGX、安全多方计算 实验室: 信息安全与密码研究所(IISec)
- A+ 课程: 数据结构、编译原理、计算机组成与体系结构、现代密码学、信息安全数学基础、离散数学 等 19 门

实习经历

阿里巴巴集团-阿里云-操作系统团队 2021.07-2021.08

- 参与业界机密容器的预研以及开源社区 `inclave-containers` 的建设, 推动机密容器未来标准的制定, 参与机密容器远程证明框架 EAA 的设计和开发工作, 负责并实现了用户侧策略引擎子模块。
- 深入调研供应链安全, 负责并实现了 EAA POC 阶段可重复构建基础设施的替代品 `verdict`。
- 累计向开源社区以及公司内部贡献代码 3000 余行, 组织 2 次团队内部技术分享、1 次事业部技术分享。

项目经历

基于 TEE 的密文空间全文搜索 (队长, 大学生创新实践计划) 2020.11-2021.08

- 从云计算、云存储的安全性问题出发, 探索隐私计算解决方案。抛开全同态加密等低效密码学手段, 创新性提出利用可信执行环境解决隐私计算问题, 并实现用户视角的密文空间全文搜索, 最终获评全国大学生信息安全竞赛三等奖。
- 设计并实现系统整体架构, 设计并实现基于 SGX 的全文搜索引擎 `TeeSearch`, 设计并实现拟同态加密通信协议 `ETIs`, 参与项目全栈开发。最终系统表现出极其优秀的性能, 全文搜索的时间开销仅为明文搜索的 2 倍。
- 作为第一发明人, 相关成果获得专利: 一种基于可信执行环境的密文搜索方法与系统。

基于 TEE 的区块链零知识证明 (队长, 上海交通大学本科生研究计划 PRP) 2019.12-2020.09

- 承担 SGX 理论学习与研究, 探索零知识证明与可信执行环境的结合方式, 个人获评本科生研究计划 A 级(前 15%)。

可信执行环境中的隐私计算 (企业合作项目) 2021.10-至今

- 利用可信执行环境解决公司业务中的用户隐私问题, 目前正在对 SGX 中的数据处理与持久化存储方案进行研究和设计。

基于可信执行环境中的安全多方计算协议研究 (毕业设计) 2021.11-至今

- 针对基于可信执行环境的安全多方协议, 设计基于可信执行环境的通用安全多方计算框架, 并根据应用的典型场景完成原型系统的开发。

个人技能

- 程序语言: Rust / C / C++ / Python / Golang / JavaScript / HTML5 / Verilog
- 语言: 中文(母语) / 英文(CET6)
- 熟悉 Linux 平台开发、Git 代码管理、密码学基础理论

自我评价

- 热爱技术, 热爱开源。