李想 (LI, XIANG)

主页: https://ambitionxiang.github.io ◇ **电话/微信**: +86-19800359715
邮箱: lixiang20@mails.tsinghua.edu.cn ◇ **领英**: xiang-li-a5a962198

教育背景

清华大学 *2020.9 - 2025.6 (预计)*
交叉信息研究院
直博生，计算机科学与技术；导师：高鸣宇.

东南大学 *2016.9 - 2020.6*
信息科学与工程学院, 2017.9 - 2020.6
学士，信息工程；排名: 1/240.
交通学院, Aug. 2016 - Sep. 2017
转专业前，交通工程；排名: 2/270.

研究兴趣

机密计算，系统安全，可信执行环境（包括其应用，构建，侧信道，建模，与密码学方案的结合），数据要素基础设施。

论文发表

Xiang Li, Yunqian Luo, and Mingyu Gao. BULKOR: Enabling Bulk Loading for Path ORAM. In ***IEEE S&P 2024*** . (**CCF-A, TH-CPL-A**).

Fabing Li, **Xiang Li**, and Mingyu Gao. Secure MLaaS with Temper: Trusted and Efficient Model Partitioning and Enclave Reuse. In ***ACSAC 2023***. (**CCF-B, TH-CPL-B**).

Xiang Li, Nuozhou Sun, Yunqian Luo, and Mingyu Gao. SODA: A Set of Fast Oblivious Algorithms in Distributed Secure Data Analytics. In ***VLDB 2023***. (**CCF-A, TH-CPL-A**).

Xiang Li, Fabing Li, and Mingyu Gao. Flare: A Fast, Secure, and Memory-Efficient Distributed Analytics Framework. In ***VLDB 2023***. (**CCF-A, TH-CPL-A**).

Bohan Zhao, **Xiang Li**, Boyu Tian, Zhiyu Mei, Wenfei Wu. DHS: Adaptive Memory Layout Organization of Sketch Slots for Fast and Accurate Data Stream Processing. In ***KDD 2021***. (**CCF-A, TH-CPL-A**).

主导项目

[In progress] Optimizing Protected KVM with ARM Virtualization Host Extensions.

- 研究问题: 当使能 ARM VHE 时如何隔离 hypervisor 和 host OS?
- 权衡: 隔离性 vs. 上下文切换开销。
- 在一个更实际的威胁模型下做到同异常层级内 hypervisor 和 host OS 的隔离。

[审稿中] Loricae: Upgrading and Optimizing Multi-Party Computation Procotols with Filmy Hardware Enclaves.

- 研究问题：TEE 究竟有多可信，以及如何将它与 MPC 这样的密码学方案结合?
- 我们提出了 Filmy enclave model 来为 TEE 的半可信特性建模。
- 我们用 filmy enclave model 来把半诚实 MPC 协议升级成恶意协议，在升级过程中我们发现并解决了一些漏洞。
- 我们用同样的 model 来优化半诚实 MPC 协议的通信量并实现加速。

[审稿中] Pyramid: A Secure, Resource-Efficient, and Pluggable Kubernetes with Multi-Tenancy Compatibility.

· 研究问题：用 TEE 保护单个容器和保护整个 k8s 集群之间有没有中间地带?
· 权衡：资源利用率 vs. 多租户隔离性。
· 1: 针对两个极端选项，我们分析了其优劣.
· 2: 一个 overlay 的系统架构使得资源调度中心化管理的同时，保证多租户集群的强隔离性。

[IEEE S&P 2024] BULKOR: Enabling Bulk Loading for Path ORAM.

· 研究问题：如何快速初始化 Path ORAM 结构，使得其和正常初始化得到的结构有着一样的安全性?
· 权衡：启动延迟 vs. 信息泄露。
· 1: 我们探索了 ORAM 批量化加载的应用场景
· 2: 我们讨论了一个简单但是不安全的基本方案。
· 3: 我们设计了一个新算法并给出了安全证明。

[VLDB 2023] SODA: Distributed Oblivious Algorithms in TEEs.

· 研究问题：如何最小化数据填充并且简化计算的同时，使得计算过程不经意?
· 权衡：数据填充需求量 & 冗余的计算 vs. 信息泄露。
· 1: 观察：均衡的通信时保证不经意网络传输的关键。
· 2: 我们设计了一系列方案将特定的传输模式变成了安全的伪随机通信传输模式，避免了全局排序和过量的数据填充，并给出了理论上的填充量。

[VLDB 2023] Flare: Distributed Analytics Framework in TEEs.

· 研究问题：如何在 Intel SGX 上高效安全地运行 Spark 框架?
· 权衡：可信计算基 vs. 域切换开销 vs. 执行完整性.
· 1: 我们用最小化原则来划分 Spark 框架。
· 2: 我们融合算子执行来减少域切换次数和开销。
· 3: 我们针对 Spark 中不同的执行模式设计了内存高效处理方案。
· 4: 我们通过对有向无环图的检查来保证执行完整性。

实习经历

阿里云数据库与存储实验室 2024.7 - 至今
研究型实习生，导师：汪晟博士

· 我正在进行数据净室相关的调研。

华为系统安全技术实验室 2023.10 - 2024.4
研究型实习生，导师：徐鹏博士

· 我调研并找到了一些有趣的研究问题。此外，我阅读了 Pytorch 框架源码。后续我在探索 ARM pKVM 的性能优化，并设计了初步方案。

蚂蚁集团安全可信事业部 2022.9 - 2023.10
研究型实习生，导师：田洪亮博士

· 我探索了 k8s 和 VM TEE 的结合，设计并实现了一个层次化的系统，达到安全和资源利用率的折中。

获奖情况

清华大学综合优秀奖学金 *2023*
清华大学交叉信息院综合优秀奖学金 *2022 - 2023*
清华大学社会实践优秀奖学金 *2022*
唐仲英德育奖学金 *2016 - 2020*
东南大学最具影响力本科生（全校每年 10 人） *2020*
孙庆云创新奖学金 *2019*
国家励志奖学金 *2019*
三好学生 *2019*

国家奖学金 *2018*
三好学生标兵 *2018*
正保教育一等奖学金 *2018*