

LI, XIANG (李想)

Homepage: <https://ambitionxiang.github.io> ◇ **Telephone/Wechat:** +86-19800359715

Email: lixiang20@tsinghua.org.cn ◇ **LinkedIn:** [xiang-li-a5a962198](#)

EDUCATION

Tsinghua University

Sep. 2020 - Jun. 2025

Institute for Interdisciplinary Information Sciences (IIIS)

Ph.D. in Computer Science, advised by Prof. Mingyu Gao (高鸣宇).

Southeast University

Sep. 2016 - Jun. 2020

School of Information Science and Engineering, Sep. 2017 - Jun. 2020

B.Eng. in Information Engineering. Rank: 1/240.

School of Transportation, Aug. 2016 - Sep. 2017

Undergraduate student in Transportation Engineering. Rank: 2/270.

EMPLOYMENT

China Telecom eSurfing Cloud (State Cloud)

Jul. 2025 - Present

R&D Expert

- I am combining confidential computing with cloud products.

Database and Storage Lab, Alibaba Cloud

Jul. 2024 - Present

Research Intern, mentored by Dr. Sheng Wang

- I investigated the products of the data clean room and found a lack of clear boundaries about legal leakage. So I am exploring a formal security goal and the corresponding solution.

System Security Technology Lab, Huawei

Oct. 2023 - Apr. 2024

Research Intern, mentored by Dr. Peng Xu

- I found and investigated some interesting problems. Besides, I learned data parallelism and model parallelism in Pytorch. And I also investigated the pKVM on ARM.

Security and Trust Division (S&T), Ant Group

Sep. 2022 - Oct. 2023

Research Intern, mentored by Dr. Hongliang Tian

- I explored the integration of Kubernetes into virtual-machine-based TEEs and designed a hierarchical system, striking a balance between security and resource utilization (*in submission*).

RESEARCH INTERESTS

My research interests mainly lie in confidential computing and system security, especially, the trusted execution environment (TEE), including its applications, constructions, side channels, formal models, and combination with cryptography. I also pay attention to data element infra.

PUBLICATIONS

Xiang Li, Weijie Liu, Fabing Li, Hongliang Tian, Zheli Liu, Shoumeng Yan, and Mingyu Gao. Pyramid: A Secure, Resource-Efficient, and Pluggable Kubernetes for Multi-Tenancy. In *EuroSys 2026* . (CCF-A, TH-CPL-A).

Xiang Li, Huanchen Zhang, and Mingyu Gao. TwinStore: Secure Key-Value Stores Made Faster with Hybrid Trusted/Untrusted Storage. In *the 16th International Symposium on Advanced Parallel Processing Technology (APPT 2025)*.

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

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).

Ruixuan Wang, Siyi Lv, **Xiang Li**, Haoshuai Gong, Zheli Liu, Tong Li, and Liang Guo. BOMAP: A Round-Efficient Construction of Oblivious Maps. In *IEEE Transactions on Dependable and Secure Computing (TDSC)*. (CCF-A, TH-CPL-A).

Jiaoyi Zhang, Liqiang Peng, Mo Sha, Weiran Liu, **Xiang Li**, Sheng Wang, Feifei Li, Mingyu Gao, and Huanchen Zhang. Femur: A Flexible Framework for Fast and Secure Querying from Public Key-Value Store. In *SIGMOD 2025*. (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).

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).

LEADING PROJECTS

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

- Research Problem: How to efficiently isolate corevisor from host OS when enabling ARM VHE?
- Tradeoff: Isolation vs. Context Switch Cost.
- Intra-level isolation between host OS and corevisor in EL2 with a more practical threat model.

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

- Research Problem: How trustworthy are the TEEs and how to combine the semi-trust TEEs with cryptographic schemes like MPC?
- Filmy enclave model to describe the semi-trustworthiness of TEEs.
- Using the filmy enclave model to upgrade semi-honest MPC protocols to malicious protocols, during which some vulnerabilities are explored.
- Using the model to accelerate semi-honest MPC protocols.

[EuroSys 2026] Pyramid: A Secure, Resource-Efficient, and Pluggable Kubernetes with Multi-Tenancy Compatibility.

- Research Problem: Is there an intermediate position between only putting containers into TEEs and putting the whole k8s cluster into TEEs?
- Tradeoff: Resource utilization vs. Multi-Tenant Isolation.
- 1: A study analyzing the pros & cons for both extreme options.
- 2: An overlay system architecture to centralize the resource management while providing strong isolation among tenant clusters.

[APPT 2025] TwinStore: Secure Key-Value Stores Made Faster with Hybrid Trusted/Untrusted Storage.

- Research Problem: Is it optimal to put the whole KV store into VM TEEs with TEE-IO and trusted storage?
- Tradeoff: Difficulty guaranteeing freshness using SW vs Repetitive encryption cost using HW.
- 1: A comprehensive analysis of the pros and cons of the pure SW and HW methods.
- 2: A hybrid system combining both untrusted/trusted storage to achieve optimal performance with full security.

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

- Research Problem: How to design efficient bulk loading for Path ORAM while the resulting structure has the same distribution as Path ORAM?
- Tradeoff: Startup Latency vs. Information Leakage.
- 1: Potential use cases for ORAM bulk loading.
- 2: Discussion on a simple but insecure bulk loading scheme.
- 3: A new algorithm with corresponding theoretical proofs.

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

- Research Problem: How to minimize data padding and simplify the computation when requiring oblivious distributed DB operators.
- Tradeoff: Data Padding & Redundant Computation vs. Information Leakage.
- 1: Observation: balanced communication is the core to guarantee oblivious network traffic.
- 2: Turning specific communication patterns into secure (pseudo-)random communication, avoiding expensive global sort and significant padding, and giving theoretical bounds.

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

- Research Problem: How to run Spark framework with Intel SGX efficiently and securely?
- Tradeoff: TCB vs. Domain Switch Cost vs. Execution Integrity.
- 1: Minimalist Philosophy for separating the framework.
- 2: Fused operator execution to reduce domain switch cost.
- 3: Memory-efficient processing for different execution patterns in Spark.
- 4: Dependency graph checking mechanism for execution integrity.

HONORS AND AWARDS

Qi Hang Award in Tsinghua University	2025
Outstanding Graduate of IIIS	2025
Jiang Nanxiang Scholarship	2024
Comprehensive Excellence Scholarship of Tsinghua University	2023
Comprehensive Excellence Scholarship of IIIS	2022 - 2023
Excellent Social Practice Award of Tsinghua University	2022
Cyrus Tang Scholarship	2016 - 2020
The Most Influential Undergraduate Students of Southeast University	2020
Outstanding Undergraduate Graduate of Southeast University	2020
Sun Qingyun Innovation Scholarship	2019
National Encouragement scholarship	2019
Merit Student	2019
National Scholarship	2018
Pacemaker to Merit Student	2018
The First Prize Scholarship of CDEL (正保教育)	2018