Xiao Li, Ph.D. Candidate

xli289@ucr.edu xiaoli0614.github.io +1 9514215297

Research Objective

- I'm a fifth-year Ph.D. candidate. My research interest spans over the theory and practice of **distributed systems**, **programming languages** and **computer security**. I'm particularly interested in **Byzantine fault-tolerant replication** and **program synthesis** in distributed systems..

Education

2019 – Present **Ph.D. Candidate, University of California, Riverside, USA** in Computer Science. GPA:3.88/4

2017 – 2019 **M.Sc., University of California, Riverside, USA** in Computer Science. GPA: 3.88/4 (Transfered to Ph.D. program)

2013 – 2017 **B.E., Huazhong University of Science and Technology, China** in Information Security. GPA: 3.65/4 (Outstanding Graduates)

2016 **Summer Intern, The University of Singapore, Singapore**

Employment

2023 Fall–Present **Research Engineer Intern.** Chainlink Labs.

2019 – 2023 Summer **Graduate Student Researcher.** UC Riverside.

Technical Skills

Object-Oriented Programming Languages: Java, Python, C++, Go.

SMT Solvers (SMT-LIB): Z3, CVC4.

Databases: SQL (PostgreSQL).

Others: Version Control (Git), LaTeX.

Research Projects

2023 – Present **Reconfiguratble clustered Byzantine replication**) (under review) Advisor: Prof. Mohsen Lesani

- Designed replication protocols that enable higher throughput with heterogeneous reconfigurable clusters.

2022 – Present **Reconfiguratble Heterogeneous Quorum Systems**) (under review) Advisor: Prof. Mohsen Lesani

- Designed reconfiguration protocols for heterogeneous quorum systems (HQS) to enable open membership for permissioned blockchains.
- Presented a reconfiguration optimization technique based on the graph characterization of HQS.
- Implemented the reconfiguration protocols in Stellar-core framework with C++.

2022 – 2023 **On the power of quorum subsumption for heterogeneous quorum systems** (published in DISC 2023) Advisor: Prof. Mohsen Lesani

- Proved an impossibility result that shows quorum intersection and quorum availability are not sufficient for Byzantine reliable broadcast (BRB) and consensus in HQS setting.
- Proposed a new property (quorum-subsumption) to help achieve BRB and consensus with detailed protocols and correctness proofs.

Research Projects (continued)

2020 – 2022 **Hamraz: Resilient Partitioning and Replication** (published in *S&P 2022*) Advisor: Prof. Mohsen Lesani

- Presented a security-typed object-based language and an information flow type inference system to automatically synthesis trustworthy-by-construction distributed system.
- Designed and implemented a CPS transformation and program partitioning system in Java.
- Designed and implemented a type inference system to generate verification conditions in Python and Z3 framework.

2019 – 2020 **Hampa: Solver-aided Recency-Aware Replicated Objects** (published and artifact evaluated in *CAV 2020*) Advisor: Prof. Mohsen Lesani

- Designed a relational object language, its denotational semantics and syntax-directed analysis to infer optimum staleness bounds.
- Designed and implemented a Java module to generate verification conditions in CVC4 framework.
- Designed and experimented synthesised run-time system on top of BFT-SmaRt library and SMT solver.

2016 – 2017 **Research and Implementation of Identification Authentication System Based on Face Recognition** (Bachelor Thesis) Advisor: Prof. Yongquan Cui

- Implemented a facial recognition system based on Principal Components Analysis and Linear Discriminating Analysis.

2014 – 2015 **Conditional Identity-based Broadcast Proxy Re-Encryption and Its Application to Cloud E-mail** Advisor: Prof. Peng Xu

- Lead a team to implement a prototype for a cloud email system based on CIBPRE and obtained *3rd Prize* in the 8th National College Student Information Security Contest.

Publications

1. Li, X., Chan, E., & Lesani, M. (2023). On the power of quorum subsumption for heterogeneous quorum systems, In *Disc'23 (international symposium on distributed computing)*.
2. Li, X., Houshmand, F., & Lesani, M. (2022). Hamraz: Resilient partitioning and replication, In *S&p'22 (ieee symposium on security and privacy)*.
3. Li, X., Houshmand, F., & Lesani, M. (2020). Hampa: Solver-aided recency-aware replication, In *International conference on computer aided verification*. Springer.

Awards and Achievements

2023 **Grace Hopper Conference Scholarship 2023**, UC Riverside .

Dissertation Year Program Fellowhip 2023/2024, UC Riverside .

2022 **Student Travel Grant**, 2022 ACM CCS.

GSA Travel Award, UC, Riverside.

Student Travel Award, 2022 IEEE Symposium on Security and Privacy.

2021 **Selected and Funded**, PLMW@SPLASH 2021.

2019 **Department Fellowship Award**, UC, Riverside.

2017 **Outstanding Graduates**, Huazhong University of Science and Technology.

2016 **Outstanding Academic Award**, Huazhong University of Science and Technology.

2015 **Third Prize**, in the 8th National College Student Information Security Contest.

2014 **Public Welfare Scholarship**, Huazhong University of Science and Technology.