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**, **automated reasoning** and **formal verification** 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 September–2023 March	🔖	**Research Engineer Intern.** Chainlink Labs.
2019 July – 2023 September	🔖	**Graduate Student Researcher.** UC Riverside.

Technical Skills

Object-Oriented Programming Languages	🔖	Go, Java, Python, C++.
SMT Solvers (SMT-LIB)	🔖	Z_3, CVC4.
Databases	🔖	SQL (PostgreSQL).
Others	🔖	Version Control (Git), LaTeX.

Research Projects

2023/09 – Present	🔖 **Censorship resistant reputation system for consensus protocols** Mentor: Dr. Chrysa Stathakopoulou

- Designed and implemented censorship resistant reputation-based leader election module to prevent slow leaders from stalling progress. It improves throughput and reduces latency for leader-based blockchains.

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

- Designed replication protocols that enable over two times throughput increase 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.
- Proposed a reconfiguration optimization technique based on the graph characterization of HQS.
- Implemented the reconfiguration protocols in Stellar-core framework with C++.

Research Projects (continued)

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.

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.
- Designed and experimented synthesised run-time system on top of BFT-SmaRt library and SMT solver.

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

2024   🔖 **SIGPLAN Mentorship**, Symposium on Principles of Programming Languages (POPL).

       🔖 **Dissertation Year Completion Fellowhip**, UC Riverside .

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

       🔖 **Dissertation Year Program Fellowhip 2023/2024**, UC Riverside .

2022   🔖 **Student Travel Grant**, 2022 ACM Conference on Computer and Communications Security (CCS).

       🔖 **GSA Travel Award**, UC, Riverside.

       🔖 **Student Travel Award**, 2022 IEEE Symposium on Security and Privacy (S&P).

2021   🔖 **Selected and Funded**, SPLASH Programming Languages Mentoring Workshop (PLMW) 2021.

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

Awards and Achievements (continued)

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.