YINGJIE XUE

4015721784 ⋄ yingjie_xue@brown.edu
115 Waterman Street, Providence, RI 02912,USA

EDUCATION

Brown University *2018-present*
PhD candidate, Department of Computer Science
Concentration: Distributed Computing, Blockchain and Cryptocurrency, Security and Privacy

Brown University *2018-2020*
Department of Computer Science
M.S. in Computer Science

University of Science and Technology of China (USTC) *2015-2018*
Department of Electronic Engineering and Information Science
M.E. in Electronics and Communication Engineering

University of Science and Technology of China (USTC) *2011-2015*
Department of Electronic Engineering and Information Science
B.E. in Information Security

RESEARCH EXPERIENCE

Fault-tolerant and Expressive Cross-chain Swaps 2021.9-2022.9
Primary Contributor *Advisor: Maurice Herlihy*

- Primary focus: design cross-chain swap protocols that tolerate deviating behaviors of courterparties.
- Responsibilities: main contributor, detailed surveys, protocols design, and security proof.
- Work products: a paper is published in ICDCN'23, as the first author.

Cross-chain State Machine Replication 2021.2-2022.2
Primary Contributor *Advisor: Maurice Herlihy*

- Primary focus: design state machine replication protocols for cross-chain transactions.
- Responsibilities: main contributor, detailed surveys, protocols design, and security proof.
- Work products: a paper is published in SSS'22, as the first author.

Transferable Cross-chain Options 2021.6-2022.2
Primary Collaborator *Advisor: Maurice Herlihy*

- Primary focus: enable option holders/providers to trade his/her option to another party.
- Responsibilities: one of main contributors, detailed surveys, protocols design, and security proof.
- Work products: a paper is published in SSS'21 and another paper is accepted in AFT' 22.

Distributed Runtime Verification for Cross-Chain Protocols 2021.8-2022.1
Primary Collaborator *Advisor: Maurice Herlihy*

- Primary focus: build monitors to monitor transactions on blockchains, and verify if expected properties of protocols hold.
- Responsibilities: one of main contributors, protocol implementation, and generate trace logs.
- Work products: a paper is published in ICDCS'22, as co-first author.

Hedging Against Sore Loser Attacks in Cross-Chain Transactions 2019.11-2021.2
Primary Contributor *Advisor: Maurice Herlihy*

- Primary focus: a sore loser attack in cross-blockchain commerce rises when one party decides to halt participation partway through. Protocols to hedge against sore loser attacks are proposed.
- Responsibilities: main contributor, detailed surveys, protocols design, and security proof.
- Work products: a paper is published in PODC'21 (the first author).

Cloud Security 2014.9-2018.6
Primary Contributor *Advisor: Kaiping Xue*

- Primary focus: addressing security issues in the emerging cloud computing, including data access control, integrity auditing and searchable encryption; designing mechanisms for practical scenarios that address tradeoffs between security and efficiency.
- Responsibilities: main contributor, detailed surveys, protocols design, thorough analysis and proof.
- Work products: *seven* publications in major conferences and journals, such as TIFS and TDSC.

TEACHING&MENTORING EXPERIENCE

Teaching Assistant, *Blockchains and Cryptocurrencies*, Brown University, USA *2022.1–2022.5*
Teaching Assistant, *Network Security Protocols*, USTC, Hefei, China *2016.3–2016.6*
Graduate Student Mentor, Brown University, USA *2021.9–2022.1*
Undergraduate Student Mentor, Brown University, USA *2021.9–2022.1*
Job description: Mentored three undergraduates in a research project.
International Student Mentor, Brown University, USA *2021.2–2021.8*

OTHER WORK EXPERIENCE

Smart Contract Research Intern, Algorand Inc, Boston, MA, USA *2020.5–2020.8*
Supervisor: Jing Chen
Job description: prototyping Algorand smart contract architecture and virtual machine. Added features to the prototype, ran tests, using Rust and Clarity programming language.

SELECTED HONORS & AWARDS

Paris Christos Kanellakis Fellowship *2022-23*
Paris Christos Kanellakis Fellowship *2020-21*
National Scholarship for Graduate Students *2017*
Sunguosheng Leadership Award *2014*

SELECTED PUBLICATIONS

- **Y.Xue**, D. Jin, M. Herlihy. *Fault-tolerant and Expressive Cross-Chain Swaps.* ICDCN'23: In 24th International Conference on Distributed Computing and Networking, pp. 28-37. 2023.
- **Y.Xue**, M. Herlihy. *Cross-chain State Machine Replication.* SSS'22: In International Symposium on Stabilizing, Safety, and Security of Distributed Systems, pp. 51-65. Springer, Cham, 2022.
- D. Engel, **Y.Xue**. *Transferable Cross-Chain Options.* accepted by ACM Advances in Financial Technologies (AFT'22).
- R. Ganguly, **Y. Xue**, A. Jonckheere, P. Ljung, B. Schornstein, B. Bonakdarpour, M. Herlihy. *Distributed Runtime Verification of Metric Temporal Properties for Cross-Chain Protocols.* ICDCS'22: 42nd IEEE International Conference on Distributed Computing Systems. (co-first author)
- **Y. Xue**, and M. Herlihy. *Hedging Against Sore Loser Attacks in Cross-Chain Transactions.* PODC'21: Proceedings of the 2021 ACM Symposium on Principles of Distributed Computing, pp. 155–164, July 2021.
- E. Daniel, M. Herlihy, and **Y. Xue**. *Failure is (literally) an Option: Atomic Commitment vs Optionality in Decentralized Finance.* SSS'21: International Symposium on Stabilization, Safety, and Security of Distributed Systems. Springer, Cham, 2021.
- **Y. Xue**, K. Xue, N. Gai, J. Hong, D. S. L. Wei, P. Hong, *An Attribute-based Controlled Collaborative Access Control Scheme for Public Cloud Storage*, IEEE Transactions on Information Forensics and Security, vol. 14, no. 11, pp. 2927 - 2942, April 2019. (JCR Q1)

- K. Xue, J. Hong, **Y. Xue**, D. S. L. Wei, N. Yu, P. Hong, *CABE: A New Comparable Attribute-Based Encryption Construction with 0-Encoding and 1-Encoding*, IEEE Transactions on Computers, vol. 66, no. 9, pp. 1491 - 1503, September 2017. (JCR Q1)
- K. Xue, S. Li, J. Hong, **Y. Xue**, N. Yu, P. Hong, *Two-Cloud Secure Database for Numeric-Related SQL Range Queries with Privacy Preserving*, IEEE Transactions on Information Forensics and Security, vol. 12, no. 17, pp. 1596-1608, July 2017. (JCR Q1)
- K. Xue, **Y. Xue**, J. Hong, W. Li, H. Yue, D. S. L. Wei, P. Hong, *RAAC: Robust and Auditable Access Control with Multiple Attribute Authorities for Public Cloud Storage*, IEEE Transactions on Information Forensics and Security, vol. 12, no. 4, pp. 953-967, April 2017. (JCR Q1)
- J. Hong, K. Xue, **Y. Xue**, W. Chen, D. S. L. Wei, N. Yu, P. Hong, *TAFC: Time and Attribute Factors Combined Access Control for Time-Sensitive Data in Public Cloud*, IEEE Transactions on Services Computing, vol. 13, no. 1, pp. 158-171, March 2017. (JCR Q1)
- **Y. Xue**, J. Hong, W. Li, K. Xue, P. Hong, *LABAC: A Location-aware Attribute-based Access Control Scheme for Cloud Storage*, Proceedings of the 59th IEEE Global Communications Conference (GLOBECOM), pp. 1-6, 2016.
- W. Li, K. Xue, **Y. Xue**, J. Hong, *TMACS: A Robust and Verifiable Threshold Multi-Authority Access Control System in Public Cloud Storage*, IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 5, pp. 1484-1496, May 2016. (JCR Q1)

SERVICE

- Program Committee Member, IJTCS-FAW, 2023
- Program Committee Member, IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2023
- IEEE Transactions on Dependable and Secure Computing (TDSC), 2021
- IEEE/ACM Transactions on Networking (ToN), 2021
- Peer-to-Peer Networking and Applications (PPNA), 2020
- IEEE Transactions on Cloud Computing (TCC), 2020

ORAL PRESENTATIONS

- *Fault-tolerant and Expressive Cross-Chain Swaps*, 24th International Conference on Distributed Computing and Networking (ICDCN 2023), IIT Kharagpur, India.
- *Cross-chain State Machine Replication*, International Symposium on Stabilizing, Safety, and Security of Distributed Systems (SSS 2022), Clermont-Ferrand, France.
- *Transferable Cross-Chain Options*, The Science of Blockchain (SBC 2022), Stanford University, California, USA.
- *Hedging Against Sore Loser Attacks in Cross-Chain Transactions*, ACM Symposium on Principles of Distributed Computing (PODC 2021), Virtual Event Italy.
- *LABAC: A Location-aware Attribute-based Access Control Scheme for Cloud Storage*, the 59th IEEE Global Communications Conference (GLOBECOM 2016), Washington, DC, USA.

TECHNICAL STRENGTHS

Programming Languages	C/C++, Python, Rust, Java, Go, Solidity, Assembly language, SQL
Statistics	Machine Learning, Deep Learning, Probabilistic Methods, Matlab
Security	Network Security, Software Security, Applied Cryptography