Xiaoyuan Liu (刘啸远)

Ph.D. Candidate in Computer Science

Email: xiaoyuanliu@berkeley.edu
Tel: (+1) 510 328 0269
Home Page: https://xiaoyuanliu.cn/

EDUCATION

University of California, Berkeley — **Berkeley, USA**
EECS Ph.D. student advised by Professor Dawn Song — 2020 – 2026

- Member of Berkeley Center for Responsible, Decentralized Intelligence (RDI),
- Initiative for Cryptocurrencies & Contracts Lab (IC3), and
- Berkeley Artificial Intelligence Research (BAIR) Lab.

Shanghai Jiao Tong University — **Shanghai, China**
Honors Bachelor of Engineering (B.Eng. Hons) in Computer Science — 2016 – 2020

SELECTED PROJECTS & EXPERIENCE

AgentX – AgentBeats Competition (as Organizer & Paradigm Designer, at Berkeley RDI) — 2026
The largest open competition for agentic AI, with over $1M in prizes and resources

AgentCTF (as Initiator & Organizer, among 4 accepted competitions at IEEE SaTML 2026) — 2025
Designing AI agents that autonomously exploit real-world vulnerabilities

CoLearn/CoLink (talk at NeurIPS 2022 workshop) — 2022
A generic programming framework for federated and decentralized data science

MPC4F (with Meta AI, Oasis Labs, rolled out on Instagram to U.S. users) — 2021
Multi-party computation for AI fairness evaluation

- Architect a privacy-preserving fairness evaluation system that involves multi-party computation, differential privacy, homomorphic encryption, and zero-knowledge proof.
- Lead a team to fulfill its development, industry-level code auditing, deployment, and delivery to Meta.

PUBLICATIONS

Security/ML/Agent/System - Top-tier publications in VLDB, ACL, ICLR [Google Scholar]

The Attack and Defense Landscape of Agentic AI: A Comprehensive Survey [pdf] — In Submission
Juhee Kim, **Xiaoyuan Liu**, Zhun Wang, Shi Qiu, Bo Li, Wenbo Guo, Dawn Song

Measuring Agents in Production [pdf] — In Submission
Melissa Z. Pan, Negar Arabzadeh, Riccardo Cogo, … , **Xiaoyuan Liu**, … , Dawn Song, Ion Stoica, Matei Zaharia, Marquita Ellis

Can LLMs Ask Good Questions? [pdf] — ACL Rolling Review Findings
Yueheng Zhang*, **Xiaoyuan Liu*** (equal contribution), Yiyou Sun, Atheer Alharbi, Hend Alzahrani, Basel Alomair, Dawn Song

HADES: Range-Filtered Private Aggregation on Public Data [pdf] *(Invited to the "Best of VLDB 2025")* — VLDB'25
Xiaoyuan Liu, Ni Trieu, Trinabh Gupta, Ishtiyaque Ahmad, Dawn Song

ThreatKG: An AI-Powered System for Automated Open-Source CTI Gathering and Management [pdf] — LAMPS'24
Peng Gao*, **Xiaoyuan Liu*** (equal contribution), Edward Choi, Sibo Ma, Xinyu Yang, Dawn Song

Ratel: MPC-extensions for Smart Contracts [pdf] — AsiaCCS'24
Yunqi Li, Kyle Soska, Zhen Huang, Sylvain Bellemare, Mikerah Quintyne-Collins, Lun Wang, **Xiaoyuan Liu**, Dawn Song, Andrew Miller

Evaluating Large Language Models in an Emerging Domain: A Pilot Study in Decentralized Finance [pdf] — ICLR Workshop'24
Joshua Carter Pearlson, **Xiaoyuan Liu**, Chengsong Huang, Kripa Ann George, Dawn Song, Chenguang Wang

Effective and Efficient Federated Tree Learning on Hybrid Data [pdf] — ICLR'24
Qinbin Li, Chulin Xie, Xiaojun Xu, **Xiaoyuan Liu**, Ce Zhang, Bo Li, Bingsheng He, Dawn Song

Lessons Learned: Surveying the Practicality of Differential Privacy in the Industry [pdf] — PETS'23
Gonzalo Munilla Garrido, **Xiaoyuan Liu**, Florian Matthes, Dawn Song

A System for Automated Open-Source Threat Intelligence Gathering and Management [pdf] — SIGMOD'21 Demo
Peng Gao*, **Xiaoyuan Liu*** (equal contribution), Edward Choi, Bhavna Soman, Chinmaya Mishra, Kate Farris, Dawn Song

Enabling Efficient Cyber Threat Hunting With Cyber Threat Intelligence [pdf] — ICDE'21
Peng Gao, Fei Shao, **Xiaoyuan Liu**, Xusheng Xiao, Zheng Qin, Fengyuan Xu, Prateek Mittal, Sanjeev R Kulkarni, Dawn Song

A System for Efficiently Hunting for Cyber Threats in Computer Systems Using Threat Intelligence [pdf] — ICDE'21 Demo
Peng Gao, Fei Shao, **Xiaoyuan Liu**, Xusheng Xiao, Haoyuan Liu, Zheng Qin, Fengyuan Xu, Prateek Mittal, Sanjeev R Kulkarni, Dawn Song

BeeTrace: A Unified Platform for Secure Contact Tracing that Breaks Data Silos [pdf] — IEEE Data Eng. Bulletin'20
Xiaoyuan Liu, Ni Trieu, Evgenios M Kornaropoulos, Dawn Song

Pretrained Transformers Improve Out-of-Distribution Robustness [pdf] — ACL'20
Dan Hendrycks*, **Xiaoyuan Liu*** (equal contribution), Eric Wallace, Adam Dziedzic, Rishabh Krishnan, Dawn Song

Distributed Structured Actor-Critic Reinforcement Learning for Universal Dialogue Management [pdf] — IEEE-ACM T AUDIO SPE
Zhi Chen, Lu Chen, **Xiaoyuan Liu**, Kai Yu

TEACHING

Lead Teaching Assistant (Fall 2022)
Entrepreneurship in Web3
Teaching Assistant (Fall 2021)
Decentralized Finance
Student Instructor (Summer 2018)
Principle and Practice of Computer Algorithms
Lead Teaching Assistant (Spring 2018)
Data Structures
Lead Teaching Assistant (Fall 2017)
C++ Programming (A)

HONORS AND AWARDS

RDI Frontier Fellowship – 2024
JP Morgan Chase PhD Fellowship (**13 awardees globally**) – 2023
Berkeley EECS Department Fellowship – 2020
Outstanding Student Cadre (**Top 0.8%**, SJTU) – 2018
KoGuan Encouragement Scholarship (**Top 0.3%**, SJTU) – 2017
Academic Excellence Scholarship – 2017,2018,2019
Zhiyuan Honorary Scholarship – 2016,2017,2018
China's National Olympiad in Informatics (NOI) Silver Medal – 2015