Xiling Li

Tel: 206-228-1052 *Email:* xiling.li@northwestern.edu *Location: Evanston, IL, USA*
Personal Website: https://xilinggrantli.github.io Google Scholar DBLP

Research Interests

Broadly speaking, my research focuses on security, privacy and trustworthiness of data management and applications including verifiable query evaluation (DB) and privacy-preserving machine learning (PPML), and works extensively with secure multiparty computation, zero-knowledge proof and differential privacy.

Education

Ph.D. Computer Science, Northwestern University — Jun 2021 - Present
- Advisor: Dr. Jennie Rogers

M.S. Computer Science, University of Washington — Dec 2020
- Advisor: Dr. Martine De Cock
- Thesis: *Privacy-Preserving Filter-based Feature Selection with Secure Multiparty Computation*

B.S. Computer Science, University of California, San Diego — Dec 2016

Research Experience

Research Assistant, Northwestern University — Jun 2021 - Present
- *ZKSQL* (VLDB 2023): Proposed the first work [2] on verifiable and efficient query evaluation with zero knowledge proofs for ad-hoc SQL queries in an operator-at-a-time fashion.
- *RESCU-SQL* (VLDB 2023 demo): Proposed the first pragmatic OLAP system [1] with all-but-one malicious security for ad-hoc SQL queries.

Research Assistant, University of Washington @PPML Group — Sep 2019 - May 2021
- UbiTtention 2020 Workshop (UbiComp-ISWC 2020): Proposed Mean-Split Gini Impurity algorithm (MS-GINI) [4] for Filter-based Feature Selection (FFS).
- ICML 2021: Proposed the first general FFS-based secure multiparty computation protocol [3] with active security and honest majority, and instantiated feature scoring protocol based on MS-GINI.

Teaching Experience

Guest Lecturer
- *Database Architecture and Query Evaluation*, COMP_SCI 339, Northwestern University — Fall 2023
- *Relational Algebra*, COMP_SCI 339, Northwestern University — Spring 2024

Teaching Assistant
- *COMP_SCI 339: Intro to Database Systems*, Northwestern University — Spring 2023
- *COMP_SCI 339: Intro to Database Systems*, Northwestern University — Spring 2024

Industrial Experience

Data Scientist, IBM @Watson IoT — Jan 2018 - Aug 2019
- Developed a case-based reasoning system for disaster prevention based on knowledge graph.
- Developed a defective product detection vision system based on object detection of different crucial parts of product and defective classification according to partial detection of the product.
- Developed a real-time multi-face recognition system for storage monitoring.

Android Developer, Shenzhen Das Intellitech Co.,Ltd @R&D Department — Jul 2017 - Dec 2017
- Developed Android app as the client side of intelligent building systems

Services

Reviewer: ICML 2021, 2022, 2023,2024; NeurIPS 2021, 2022, 2023, 2024; ICLR 2022, 2023, 2024

Invited Talks

Privacy + Machine Learning, *Northwestern AI Journal Club*, Nov 2021.

Technical Skills

C++, Python, Java, EMP-toolkit, Scikit-Learn, PyTorch, MP-SPDZ, AWS EC2, Ubuntu, Docker

Open Source Artifacts

Xiling Li, Chenkai Weng, Yongxin Xu, Xiao Wang, Jennie Rogers. *ZKSQL: Verifiable and Efficient Query Evaluation with Zero-Knowledge Proofs*. https://github.com/vaultdb/zksql, Feb 2023.

Selected Publications

[1] **Xiling Li***, Gefei Tan*, Xiao Wang, Jennie Rogers, Soamar Homsi. *RESCU-SQL: Oblivious Querying for the Zero Trust Cloud*. In Proceedings of the VLDB Endowment (PVLDB), Volume 16, No. 12, 4086-4089, 2023. DOI:https://doi.org/ 10.14778/3611540.3611627.

[2] **Xiling Li**, Chenkai Weng, Yongxin Xu, Xiao Wang, Jennie Rogers. *ZKSQL: Verifiable and Efficient Query Evaluation with Zero-Knowledge Proofs*. In Proceedings of the VLDB Endowment (PVLDB), Volume 16, No. 8, 1804-1816, 2023. DOI:https://doi.org/10.14778/3594512.3594513.

[3] **Xiling Li**, Rafael Dowsley, Martine De Cock. *Privacy-Preserving Feature Selection with Secure Multiparty Computation*, In Proceedings of the 38th International Conference on Machine Learning, PMLR 139:6326-6336, 2021.

[4] **Xiling Li**, Martine De Cock. *Cognitive load detection from wrist-band sensors.* In Adjunct Proceedings of the 2020 ACM International Joint Conference on Pervasive and Ubiquitous Computing and Proceedings of the 2020 ACM International Symposium on Wearable Computers (UbiComp-ISWC '20). ACM, New York, NY, USA, 456–461. DOI: https://doi.org/10.1145/3410530.3414428