Min Xu

Contact Information

1288 123rd Ave NE,
Bellevue, WA 98005,
312-874-2708
xum90@fb.com

Research Interests

My current research interest lies on improving the security & privacy of users' data in the cloud using applied cryptography and system design.

Education

University of Chicago — Chicago, IL

Ph.D. Candidate, Computer Science — 2018-2020

- Advisor: David Cash
- Theis: *Towards Better Data Privacy and Utility in the Untrusted Cloud*

Master, Computer Science — 2015-2017

- Advisor: Ariel Feldman
- Theis: *HERMETIC: Privacy-Preserving Distributed Analytics without (most) Side Channels*

The Chinese University of Hong Kong — Hong Kong

M.Phil., Computer Science and Engineering — 2013-2015

- Thesis: *Even Data Placement for Load Balance in Distributed Storage Systems with Deduplication and Erasure Coding*
- Advisor: Patrick, P.C. Lee

B.S., Mathematics and B.Eng., Information Engineering — 2008-2013

Work Experience

Research Scientist - AI Privacy & Transparency — Jan. 2021 - Present
Meta — *Bellevue, WA*

SWE Intern — Jun - Sep, 2019
Facebook, w/ Srikanth Sastry, Lucas Waye — *Boston, MA*

Research Intern — Mar - Jun, 2019
Alibaba DAMO, w/ Bolin Ding — *Bellevue, WA*

Summer Research Intern — Jun - Sep, 2017
Microsoft Research, w/ Arvind Arasu — *Redmond, WA*

Selected Research

Private and practical encrypted document keyword search over cloud We propose new constructions for keyword search on encrypted documents over cloud with better privacy guarantees than existing solutions. In particular, our solutions are secure against devastating file-injection attacks, and achieve good performance in real-world settings.

Joint data analytics over independent data collections under local differential privacy (LDP) We propose new LDP mechanims to enable multiple services to independently collect their users' data under LDP, and then to conduct joint analysis over arbitrary subset of the data collections without extra processing or privacy loss. Our mechanims can handle scenarios and queries that existing solutions either fail to handle or suffer from low utility

Secure cloud SQL processing without software side-channels We address the devastating side-channel leakages, including execution time, memory access pattern, and execution output size, all of which break the security guarantees for existing solutions for secure cloud computations using trusted-hardware, such as Intel SGX, for SQL processings in the cloud. We design an expressive set of optimized oblivious SQL algorithms, and differentially private data padding planner to efficiently address these side-channels.

Referred Publications

1. **M. Xu**, A. Namavari, D. Cash, T. Ristenpart. “Searching Encrypted Data with Size-Locked Indexes”. In USENIX Security’21.
2. A. Arasu, B. Chandramouli, J. Gehrke, E. Ghosh, D. Kossmann, J. Protzenko, R. Ramamurthy, T. Ramananandro, A. Rastogi, S. Setty, N. Swamy, A.v. Renen, **M. Xu**.“FastVer: Making Data Integrity a Commodity”. In SIGMOD’21.
3. T.H. Wang, B.L. Ding, **M. Xu**, Z.C. Huang, C. Hong, J.R. Zhou, N.H. Li, S. Jha. “Improving Utility and Security of the Shuffler based Differential Privacy”. In VLDB’20.
4. **M. Xu**, B.L. Ding, T.H. Wang, J.R. Zhou. “Collecting and Analyzing Data Jointly from Multiple Services under Local Differential Privacy”. In VLDB’20.
5. **M. Xu**, T.H. Wang, B.L. Ding, J.R. Zhou, C. Hong, Z.C. Huang. “DPSAaS: Multi-Dimensional Data Sharing and Analytics as Services under Local Differential Privacy.” In VLDB’19 *Demo*
6. **M. Xu**, A. Papadimitriou, A. Feldman, A. Haeberlen. “Hermetic: Privacy-preserving distributed analytics without (most) side channels.”, Technical Report
7. **M. Xu***, A. Papadimitriou*, A. Feldman, A. Haeberlen. “Using Differential Privacy to Efficiently Mitigate Side Channels in Distributed Analytics.” In EuroSec’18 (*: joint first authors with equal contributions)
8. **M. Xu**, Y.F. Zhu, P.P.C. Lee, Y.L. Xu, “Even Data Placement for Load Balance in Reliable Distributed Deduplication Storage Systems.” In IWQoS’15.
9. Y.K. Li, **M. Xu**, C.H. Ng, P.P.C. Lee, “Efficient Hybrid Inline and Outofline Deduplication for Backup Storage.” In ACM Transactions on Storage (TOS), 2014.

Awards & Grants

• VLDB 2019 Travel Grant	2019, 2020
• EuroSys 2018 Travel Grant, Porto, Portugal,	Apr, 2018
• University of Chicago University Unrestricted (UU) fellowship,	Spring, 2018
• CUHK CSE Department RPg Travel Grant, Portland, OR, USA	Jun, 2015
• HKSAR Government Admission Scholarship	2008-2011,2013
• Summer Research on Applied Mathematics, Knoxville, TN, USA	Aug, 2010
• Yasumoto Exchange Scholarship	Aug, 2010

References

David Cash	Ph.D. advisor
Associate Professor	CS@University of Chicago
Bolin Ding	Internship Mentor
Research Director	Alibaba DAMO
Ariel Feldman	Ph.D. advisor
Assistant Professor	CS@University of Chicago
Patrick P.C. Lee	M.Phil. advisor
Associate Professor	CSE@Chinse University of Hong Kong