Min Xu

Contact Information	5730 S. Ellis Avenue, John Crerar Library, Chicago, IL, 60637,	312-874-2708 xum@cs.uchicago.edu Personal website

Research Interests: My current research interest is applied crypto for cloud integrity & privacy.

Education

University of Chicago — Chicago, IL

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

- Advisor: David Cash

Master, Computer Science — 2015-2017

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

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 Assistant — 2018 - present
Department of Computer Science, University of Chicago — *Chicago, IL*
Supervisor: David Cash

Research Assistant — 2015 - 2017
Department of Computer Science, University of Chicago — *Chicago, IL*
Supervisor: Ariel Feldman

Summer Research Intern — Jun - Sep, 2017
Microsoft Research — *Redmond, WA*
Mentor: Arvind Arasu

Research Assistant — Jul, 2013 - Jul, 2015
CSE Depart., The Chinese University of Hong Kong — *Hong Kong*
Supervisor: Patrick, P.C. Lee

Past Research

Secure computation outsourcing to the untrusted cloud This project focuses on the security of the data-intensive computations that are outsourced to the cloud. Our major objective is to make them privacy-preserving, even under the threat model that the cloud infrastructures are malicious or semi-malicious. We realize that side channel vulnerabilities in both hardwares and softwares render the existing encryption based approach ineffective, and leverage cryptographic techniques and hardware support to efficiently mitigate the issues.

Memory integrity verification This work aims at achieving efficient memory integrity verification on applications with large-scale memory states and concurrent memory accesses. Existing solutions, i.e., Merkle hash tree and Blum's memory checking, fail on concurrency and scale, respectively. We build a new hybrid verification scheme that achieves the baseline, i.e., without integrity verification, concurrency, $O(1)$ verification cost and $O(mlog(N))$ scanning cost, where m is the number of unique memory accesses within a verification window and N is the size of the memory state.

Cloud privacy and integrity against untrusted app and OS This project aims to protect cloud users' private data from the potentially untrusted cloud applications and

OS. In our threat model, the untrusted OS could eavesdrop or tamper users' private data at rest, and the untrusted applications can collude with unstrusted OS to leak sensitive information via possible covert channels. We combine trusted hardware, i.e., Intel SGX and application sandbox, i.e., Google Native Client, to tackle attacks from both OS and the untrusted applications.

Distributed Storage Systems with Deduplication We designed and implemented a distributed deduplication system to tackle the read imbalance problem induced by deduplication in a distribution storage system.

Efficient Hybrid Inline and Out-of-line Deduplication for Backup Storage We designed and implemented RevDedup, an efficient hybrid inline and out-of-line deduplication system for backup storage, which can can bring high performance to the backup, restore, and deletion operations, while maintaining high storage efficiency comparable to conventional inline deduplication.

Referred Publications

1. **M. Xu***, A. Papadimitriou*, A. Feldman, A. Haeberlen. "Using Differential Privacy to Efficiently Mitigate Side Channels in Distributed Analytics." In EuroSec'18: 11th European Workshop on Systems Security, Porto, Portugal, April 23, 2018 (*: joint first authors with equal contributions)
2. **M. Xu**, Y.F. Zhu, P.P.C. Lee, Y.L. Xu, "Even Data Placement for Load Balance in Reliable Distributed Deduplication Storage Systems." Proceedings of the IEEE/ACM International Symposium on Quality of Service (IWQoS'15) (Full paper), Portland, Oregon, USA, Jun 2015.
3. Y.K. Li, **M. Xu**, C.H. Ng, P.P.C. Lee, "Efficient Hybrid Inline and Outofline Deduplication for Backup Storage." *ACM Transactions on Storage (TOS)*, 2014.

Talks

Using Differential Privacy to Efficiently Mitigate Side Channels in Distributed Analytics
11th European Workshop on Systems Security (EuroSec'18), Porto, Portugal, April 23, 2018

Hermetic: Privacy-preserving distributed analytics without (most) side channels
Center for Unstoppable Computing (CERES) Summit, Chicago, IL, Mar, Sep, 2017 (Poster)
6th Greater Chicago Area Systems Research Workshop (GCASR), Chicago, IL, Apr, 2017 (Poster)

Isolation and Transparency for Outsourced Applications
Center for Unstoppable Computing (CERES) Summit 2016 Poster Session, Chicago, IL, Jan, 2016 (Poster)

Even Data Placement for Load Balance in Reliable Distributed Deduplication Storage Systems
IEEE/ACM International Symposium on Quality of Service (IWQoS'15), Portland, OR, Jun, 2015

Awards & Grants

- 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 — E-mail: davidcash@cs.uchicago.edu
Department of Computer Science
University of Chicago

Ariel Feldman (Ph.D. advisor)
Assistant Professor — E-mail: arielfeldman@cs.uchicago.edu
Department of Computer Science
University of Chicago

Arvind Arasu (Internship Mentor)
Researcher — E-mail: arvinda@microsoft.com
Microsoft Research

Patrick P.C. Lee (M.Phil. advisor)
Associate Professor — E-mail: pclee@cse.cuhk.edu.hk
Department of Computer Science and Engineering
The Chinse University of Hong Kong