

Min Xu

CONTACT INFORMATION	1100 East 58th Street, University of Chicago, Chicago, IL, 60637,	312-874-2708 xum@cs.uchicago.edu Personal website
RESEARCH INTERESTS	My current research interest is cloud integrity & privacy.	
EDUCATION	University of Chicago Ph.D. Candidate, Computer Science • Advisor: Ariel Feldman The Chinese University of Hong Kong M.Phil., Computer Science and Engineering • Thesis: <i>Even Data Placement for Load Balance in Distributed Storage Systems with Deduplication and Erasure Coding</i> • Advisor: Patrick, P.C. Lee B.S., Mathematics and B.Eng., Information Engineering	Chicago, IL 2015-present Hong Kong 2013-2015 2008-2013
WORK EXPERIENCE	Research Assistant Department of Computer Science University of Chicago Supervisor: Ariel Feldman Summer Research Intern Microsoft Research Mentor: Arvind Arasu Research Assistant Department of Computer Science and Engineering The Chinese University of Hong Kong Supervisor: Patrick, P.C. Lee Summer Research Intern Department of Computer Science and Engineering, The Chinese University of Hong Kong Supervisor: Patrick, P.C. Lee Software Engineer WisdomOne Ltd. Summer Research Intern Oak Ridge National Laboratory Supervisor: Prof. Yvonne M.J. Ou Partner: Mr. T.K. Mak	2015 - present <i>Chicago, IL</i> Jun - Sep, 2017 <i>Redmond, WA</i> Jul, 2013 - Jul, 2015 <i>Hong Kong</i> Jun - Aug, 2012 <i>Hong Kong</i> Jul, 2011 - Jun, 2012 <i>Hong Kong</i> Jun - Aug, 2010 <i>Knoxville, TN</i>
CURRENT 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 $O(m \log(N))$ scanning cost, where m is the number of unique memory accesses within a verification window and N is the size of the memory state.

PAST
RESEARCHES

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 untrusted 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 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

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 (Oral)

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

TEACHING EXPERIENCE **Teaching Assistant**
University of Chicago
CMSC23200/33250 - Introduction to Computer Security Autumn, Winter 2015

The Chinese University of Hong Kong
CSCI4180 - Introduction to Cloud Computing and Storage Fall 2012, 2013
ENGG5015/CSCI5470 - Computer and Network Security Spring 2013, 2014

COURSES

University of Chicago
CMSC31230 - Fundamentals of Deep Learning Winter 2016
CMSC32200 - Computer Architecture Autumn 2016
CMSC37110 - Discrete Mathematics Autumn 2016
CMSC33251 - Topics in Computer Security Spring 2016
CMSC35400 - Machine Learning Spring 2016
CMSC33550 - Introduction to Databases Winter 2015
CMSC37000 - Algorithms Winter 2015
CMSC33250 - Introduction to Computer Security Autumn 2015
CMSC33100 - Advanced Operating Systems Autumn 2015

The Chinese University of Hong Kong
CSCI5010 - Practical Computational Geometry Algorithms Spring 2014
CSCI5060 - Semidefinite programming and approximation algorithms Spring 2014
CSCI5120 - Advanced Topics in Database Systems Fall 2013
CSCI5510 - Big Data Analytics Fall 2013

SKILLS C/C++; Java; Python; Visual Studio; shell scripting; Linux; SGX
 \LaTeX ; Gnuplot; Svn; Git
Native speaker of Mandarin; Fluent in English and Cantonese.

REFERENCES

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

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