Ling Ren

Last updated: January 2018

Contact

MIT Stata Center 32-G890
32 Vassar Street,
Cambridge, MA, 02139

E-mail: renling@mit.edu
Website: http://people.csail.mit.edu/renling/
Phone: (857) 998-8088

Interests

computer security, applied cryptography, computer architecture, distributed computing

Education

Massachusetts Institute of Technology
Ph.D., Electrical Engineering and Computer Science, 2018 (expected).
M.S., Electrical Engineering and Computer Science, 2014.
Advisor: Srinivas Devadas

Tsinghua University
B.S., Electronic Engineering, 2012.

Research

MIT CSAIL
Research Assistant, 2012 – present

VMware Research Group
Research Intern, summer 2016

Tsinghua University
Undergraduate Research Assistant, 2010 – 2012

Teaching

MIT
Instructor, 6.046 – Design and Analysis of Algorithms, Fall 2017
Teaching Assistant, 6.046 – Design and Analysis of Algorithms, Spring 2015
Grader, 6.875 – Cryptography, Spring 2013

Publications

27. Emil Stefanov, Marten van Dijk, Elaine Shi, T-H. Hubert Chan, Christopher Fletcher, **Ling Ren**, Xiangyao Yu, and Srinivas Devadas. Path ORAM: an extremely simple oblivious RAM protocol. *Journal of the ACM (JACM)*, 2018 (accepted, to appear).

26. Chenglu Jin, Charles Herder, **Ling Ren**, Phuong Ha Nguyen, Benjamin Fuller, Srinivas Devadas, and Marten van Dijk. FPGA implementation of a cryptographically-secure PUF based on learning parity with noise. *Cryptography: Special Issue on PUF-Based Authentication*, 2017.

25. Ittai Abraham, Dahlia Malkhi, Kartik Nayak, **Ling Ren**, and Alexander Spiegelman. Solida: A blockchain protocol based on reconfigurable Byzantine consensus. In *International Conference on Principles of Distributed Systems (OPODIS)*, 2017. (alphabetical order)

24. **Ling Ren** and Srinivas Devadas. Bandwidth hard functions for ASIC resistance. In *15th International Conference on Theory of Cryptography (TCC)*, 2017.

23. Srinivas Devadas, **Ling Ren**, and Hanshen Xiao. On iterative collision search for LPN and subset sum. In *15th International Conference on Theory of Cryptography (TCC)*, 2017. (alphabetical order)

22. Leo Alcock and **Ling Ren**. A note on the security of Equihash. In *ACM Workshop on Cloud Computing Security (CCSW)*, 2017.

21. Ittai Abraham, Srinivas Devadas, Kartik Nayak, and **Ling Ren**. Brief announcement: Practical synchronous Byzantine consensus. In *International Symposium on Distributed Computing (DISC)*, 2017. Full version at https://arxiv.org/abs/1704.02397. (alphabetical order)

20. **LING REN**, Christopher Fletcher, Albert Kwon, Marten van Dijk, and Srinivas Devadas. Design and implementation of the Ascend secure processor. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2017 (accepted, to appear).

19. Ittai Abraham, Christopher Fletcher, Kartik Nayak, Benny Pinkas, and **LING REN**. Asymptotically tight bounds for composing ORAM with PIR. In *20th International Workshop on Public Key Cryptography (PKC)*, 2017. (alphabetical order)

18. Kartik Nayak, Christopher Fletcher, **LING REN**, Nishanth Chandran, Satya Lokam, Elaine Shi, and Vipul Goyal. HOP: Hardware makes obfuscation practical. In *24th Annual Network and Distributed System Security Symposium (NDSS)*, 2017.

17. Charles Herder, **LING REN**, Marten van Dijk, Meng-Day Yu, and Srinivas Devadas. Trapdoor computational fuzzy extractors and stateless cryptographically-secure physical unclonable functions. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2017.

16. **LING REN** and Srinivas Devadas. Proof of space from stacked expanders. In *14th International Conference on Theory of Cryptography (TCC)*, 2016.

15. Srinivas Devadas, Marten van Dijk, Christopher Fletcher, **LING REN**, Elaine Shi, and Daniel Wichs. Onion ORAM: A constant bandwidth blowup oblivious RAM. In *13th International Conference on Theory of Cryptography (TCC)*, 2016. (alphabetical order)

14. **LING REN**, Christopher Fletcher, Albert Kwon, Emil Stefanov, Elaine Shi, Marten van Dijk, and Srinivas Devadas. Constants count: practical improvements to oblivious RAM. In *24th USENIX Conference on Security Symposium (Usenix Security)*, 2015.

13. Xiangyao Yu, Syed Kamran Haider, **LING REN**, Christopher Fletcher, Albert Kwon, Marten van Dijk, and Srinivas Devadas. PrORAM: dynamic prefetcher for oblivious RAM. In *42nd International Symposium on Computer Architecture (ISCA)*, 2015.

12. Christopher Fletcher, **LING REN**, Albert Kwon, Marten van Dijk, Emil Stefanov, Dimitrios Serpanos, and Srinivas Devadas. A low-latency, low-area hardware oblivious RAM controller. In *IEEE 23rd Annual International Symposium on Field-Programmable Custom Computing Machines (FCCM)*, 2015.

11. Christopher Fletcher, **LING REN**, Albert Kwon, Marten van Dijk, and Srinivas Devadas. Freecursive ORAM: [nearly] free recursion and integrity verification for position-based oblivious RAM. In *20th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)*, 2015.

10. Xiaoming Chen, **LING REN**, Yu Wang, and Huazhong Yang. GPU-accelerated sparse LU factorization for circuit simulation with performance modeling. *IEEE Transactions on Parallel and Distributed Systems (TPDS)*, 2015.

9. Christopher Fletcher, **LING REN**, Xiangyao Yu, Marten van Dijk, Omer Khan, and Srinivas Devadas. Suppressing the oblivious RAM timing channel while making information leakage and program efficiency trade-offs. In *20th International Symposium on High Performance Computer Architecture (HPCA)*, 2014.

8. Xiangyao Yu, Christopher W Fletcher, **LING REN**, Marten van Dijk, and Srinivas Devadas. Generalized external interaction with tamper-resistant hardware with bounded information leakage. In *ACM Workshop on Cloud Computing Security (CCSW)*, 2013.

7. Emil Stefanov, Marten van Dijk, Elaine Shi, Christopher Fletcher, **LING REN**, Xiangyao Yu, and Srinivas Devadas. Path ORAM: an extremely simple oblivious RAM protocol. In *ACM Conference on Computer & Communications Security (CCS)*, 2013. **Best Student Paper**

6. **LING REN**, Christopher W Fletcher, Xiangyao Yu, Marten van Dijk, and Srinivas Devadas. Integrity verification for path oblivious RAM. In *IEEE High Performance Extreme Computing Conference (HPEC)*, 2013.

5. **LING REN**, Xiangyao Yu, Christopher W Fletcher, Marten van Dijk, and Srinivas Devadas. Design space exploration and optimization of path oblivious RAM in secure processors. In *40th International Symposium on Computer Architecture (ISCA)*, 2013.

4. Yu Wang, Haixiao Du, Mingrui Xia, **LING REN**, Mo Xu, Teng Xie, Gaolang Gong, Ningyi Xu, Huazhong Yang, and Yong He. A hybrid CPU-GPU accelerated framework for fast mapping of high-resolution human brain connectome. *PloS one*, 2013.

3. **LING REN**, Xiaoming Chen, Yu Wang, Chenxi Zhang, and Huazhong Yang. Sparse LU factorization for parallel circuit simulation on GPU. In *49th Annual Design Automation Conference (DAC)*, 2012.

2. Mo Xu, Xiaorui Zhang, Yu Wang, **LING REN**, Ziyu Wen, Yi Xu, Gaolang Gong, Ningyi Xu, and Huazhong Yang. Probabilistic brain fiber tractography on GPUs. In *26th International Parallel and Distributed Processing Symposium Workshops (IPDPSW)*, 2012.

1. Yu Wang, Mo Xu, **LING REN**, Xiaorui Zhang, Di Wu, Yong He, Ningyi Xu, and Huazhong Yang. A heterogeneous accelerator platform for multi-subject voxel-based brain network analysis. In *International Conference on Computer-Aided Design (ICCAD)*, 2011.

Talks

7. Bandwidth-hard Functions for ASIC Resistance
   Conference talk at TCC, Nov. 2017

6. Solida: A Blockchain Protocol Based on Reconfigurable Byzantine Consensus
   Conference talk at OPODIS, Dec. 2017
   MIT Bitcoin Expo, Mar. 2017
   Tsinghua/Cornell Workshop on Security and Cryptography, Dec. 2016
   Cornell Crypto Seminar, Dec. 2016
   Berkeley Security Seminar, Nov. 2016
   VMWare Research Group, Aug. 2016

5. Proof of Space from Stacked Expanders
   Conference talk at TCC, Nov. 2016
   Tsinghua University EE Department, Nov. 2016
   MIT Cryptography and Information Security (CIS) Seminar, Oct. 2016

4. Onion ORAM: A Constant Bandwidth Blowup Oblivious RAM
   Stanford Security Seminar, July 2016

3. Practical ORAM in Hardware
   Conference talk at ASPLOS, Mar. 2015
   NSF MACS ORAM Day, Jan. 2015
   Qatar Computing Research Institute (QCRI), June 2014

2. Integrity Verification for Path Oblivious RAM
   Conference talk at HPEC, Sept. 2013
   IBM Research China, Aug. 2013

1. Sparse LU Factorization for Parallel Circuit Simulation on GPU
   Conference talk at DAC, June. 2012
   Chinese National Symposium on High Performance Algorithm and Software, Dec. 2011
   Chinese Academy of Sciences, Nov. 2011

Service

Reviewer
CCS'14, CHES'15, NDSS'15, CCS'16, ICCD'16, Eurocrypt'17, NSDI'17, ASPLOS'17, ICALP'17, Crypto'17, Asiacrypt'17, TCC'17, Eurocrypt'18, FC'18, STACS'18, STOC'18
IEEE Trans. on Dependable and Secure Computing (TDSC),
Journal of Cryptology (JCrypto),
Data & Knowledge Engineering (DKE),
IEEE Trans. on Industrial Informatics (TII),
IEEE Trans. on Information Forensics & Security (TIFS),
IEEE Trans. on Computer-Aided Design of Integrated Circuits and Systems (TCAD)
Information Processing Letters (IPL)

References

Ittai Abraham
Senior researcher at VMware Research
iabraham@vmware.com

Srinivas Devadas (advisor)
Edwin Sibley Webster Professor of EECS at MIT
devadas@csail.mit.edu

Marten van Dijk
Charles H. Knapp Associate Professor of ECE at University of Connecticut
marten.van_dijk@uconn.edu

Dahlia Malkhi
Principal researcher at VMware Research
dmalkhi@vmware.com

Elaine Shi
Associate Professor of CS at Cornell University
elaine@cs.cornell.edu

Vinod Vaikuntanathan
Associate Professor of EECS at MIT
vinodv@csail.mit.edu