Ling Ren

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

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

Department, University
Teaching Assistant, 6.046 – Design and Analysis of Algorithms, Fall 2015
Grader, 6.875 – Cryptography, Spring 2013

Publications

1. **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 (to appear)

2. Ittai Abraham, Christopher Fletcher, Kartik Nayak, Benny Pinkas, and **Ling Ren**. Asymptotically tight bounds for composing ORAM with PIR. In *International Workshop on Public Key Cryptography (PKC)*. Mar. 2017 (to appear). **(alphabetical order)**

3. Kartik Nayak, Christopher Fletcher, **Ling Ren**, Nishanth Chandran, Satya Lokam, Elaine Shi, and Vipul Goyal. HOP: Hardware makes obfuscation practical. In *Network and Distributed System Security Symposium (NDSS)*, Feb. 2017 (to appear)

4. **Ling Ren** and Srinivas Devadas. Proof of space from stacked expanders. In *14th International Conference on Theory of Cryptography (TCC)*. Nov. 2016

5. 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)*, Mar. 2016

6. 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)*. Jan. 2016. **(alphabetical order)**

7. **Ling Ren**, Christopher Fletcher, Albert Kwon, Emil Stefanov, Elaine Shi, Marten Van Dijk, and Srinivas Devadas. Constants count: practical improvements to oblivious RAM. In *Proceedings of the 24th USENIX Conference on Security Symposium (Usenix Security)*. Aug. 2015

8. 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)*. June 2015

9. 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 International Symposium on Field-Programmable Custom Computing Machines (FCCM)*. May 2015

10. 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)*. Mar. 2015

11. 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)*, Mar. 2014

12. 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)*. Feb. 2014

13. 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 *Proceedings of the 2013 ACM workshop on Cloud computing security workshop (CCSW)*. Nov. 2013

14. 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 *Proceedings of the 2013 ACM conference on Computer & communications security (CCS)*. Nov. 2013

15. **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)*. Sept. 2013

16. **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 *40nd International Symposium on Computer Architecture (ISCA)*. June 2013

17. 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*, May 2013

18. **Ling Ren**, Xiaoming Chen, Yu Wang, Chenxi Zhang, and Huazhong Yang. Sparse LU factorization for parallel circuit simulation on GPU. In *Proceedings of the 49th Annual Design Automation Conference (DAC)*. June 2012

19. 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)*. May 2012

20. 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)*. Nov. 2011

Talks

1. Solidus: An Incentive-compatible Cryptocurrency Based on Permissionless Byzantine Consensus
   Tsinghua/Cornell Workshop on Security and Cryptography, Beijing, Dec. 2016
   Cornell Crypto Seminar, Ithaca, Dec. 2016
   Berkeley Security Seminar, Berkeley, Nov. 2016
   VMWare Research Group, Palo Alto, Aug. 2016

2. Proof of Space from Stacked Expanders
   Conference talk at TCC, Beijing, Nov. 2016
   Tsinghua University EE Department, Beijing, Nov. 2016
   MIT Cryptography and Information Security Seminar, Cambridge, Oct. 2016

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

4. Practical ORAM in Hardware
   Conference talk at ASPLOS, Istanbul, Mar. 2015
   NSF MACS ORAM Day, Boston, January 2015
   Qatar Computing Research Institute (QCRI), Doha, June 2014

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

Service

Reviewer

CCS'2014, CHES'2015, NDSS'2015, CCS'2016, ICCD'2016, Eurocrypt'2017, IEEE Transactions on Dependable and Secure Computing (TDSC), IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD) Information Processing Letters (IPL)