WEI-KAI LIN

+1 (607) 342-8261 \diamond we.lin@northeastern.edu \diamond https://weikailin.github.io

RESEARCH INTERESTS

My research lies in cryptography and algorithms, and I am interested in theoretical computer science in general. My results are published mainly in SODA, Crypto, Eurocrypt, Asiacrypt.

EDUCATION

Cornell University, Ithaca, NY, USA Ph.D. in Computer Science	August 2016 - August 2021
Thesis: Optimal Oblivious RAM and Its Extensions. Advisor: Prof. Elaine Shi.	
National Taiwan University, Taipei, Taiwan M.S. in Electrical Engineering (Computer Science Group)	June 2009
Thesis: Co-evolvability of games in coevolutionary genetic algo Advisor: Prof. Tian-Li Yu.	prithms.
National Taiwan University, Taipei, Taiwan B.S. in Chemistry	June 2007
EXPERIENCE	
Northeastern University, Boston, MA, USA Postdoctral Research Associate in Khoury College of Compute Supervisor: Prof. Daniel Wichs.	June 2022 - Present r Sciences
Carnegie Mellon University, Pittsburgh, PA, USA <i>Post Doctoral Fellow</i> in Computer Science Department Supervisor: Prof. Elaine Shi.	December 2021 - May 2022
NTT Research, East Palo Alto, CA, USA Research Intern in Cryptography & Information Security Lab Supervisor: Prof. Ilan Komargodski.	June 2020 - August 2020
Academia Sinica, Taipei, Taiwan Research Assistant in Institute of Information Science Supervisor: Dr. Kai-Min Chung.	November 2014 - July 2016
PUBLICATIONS	★ Selected

- ★ OptORAMa: Optimal Oblivious RAM Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, Kartik Nayak, Enoch Peserico, and Elaine Shi. In the 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques (Eurocrypt), 2020. In the Journal of the ACM (JACM), October, 2022.
- ★ Optimal Sorting Circuits for Short Keys Wei-Kai Lin, and Elaine Shi.*
 In ACM-SIAM Symposium on Discrete Algorithms (SODA), 2022.

- ★ A Logarithmic Lower Bound for Oblivious RAM (for all parameters) Ilan Komargodski, and Wei-Kai Lin. In Advances in Cryptology (CRYPTO), 2021.
- Optimal Oblivious Parallel RAM Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, Enoch Peserico, and Elaine Shi. In ACM-SIAM Symposium on Discrete Algorithms (SODA), 2022.
- Oblivious RAM with Worst-Case Logarithmic Overhead Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, and Elaine Shi. In Advances in Cryptology (**CRYPTO**), 2021.
- Perfectly Oblivious (Parallel) RAM Revisited, and Improved Constructions T-H. Hubert Chan, Elaine Shi, Wei-Kai Lin, and Kartik Nayak.* In Information-Theoretic Cryptography (**ITC**), 2021.
- Sorting Short Keys in Circuits of Size o(n log n) Gilad Asharov, Wei-Kai Lin, and Elaine Shi.
 In ACM-SIAM Symposium on Discrete Algorithms (SODA), 2021. In SIAM Journal on Computing (SICOMP), 51:3, 2022.
- Oblivious Parallel Tight Compaction Gilad Asharov, Ilan Komargodski, Wei-Kai Lin, Enoch Peserico, and Elaine Shi. In Information-Theoretic Cryptography (**ITC**), 2020.
- MPC for MPC: Secure Computation on a Massively Parallel Computing Architecture T-H. Hubert Chan, Kai-Min Chung, Wei-Kai Lin, and Elaine Shi. In Innovations in Theoretical Computer Science (**ITCS**), 2020.
- Can We Overcome the n log n Barrier for Oblivious Sorting? Wei-Kai Lin, Elaine Shi, and Tiancheng Xie. In ACM-SIAM Symposium on Discrete Algorithms (SODA), 2019.
- Game Theoretic Notions of Fairness in Multi-Party Coin Toss Kai-Min Chung, Yue Guo, Wei-Kai Lin, Rafael Pass, and Elaine Shi. In Theory of Cryptography Conference (**TCC**), 2018.
- Cache-Oblivious and Data-Oblivious Sorting and Applications T-H. Hubert Chan, Yue Guo, Wei-Kai Lin, and Elaine Shi. In ACM-SIAM Symposium on Discrete Algorithms (**SODA**), 2018.
- Oblivious Hashing Revisited, and Applications to Asymptotically Efficient ORAM and OPRAM T-H. Hubert Chan, Yue Guo, Wei-Kai Lin, and Elaine Shi. In proceedings of the 23rd Annual International Conference on the Theory and Applications of Cryptology and Information Security (Asiacrypt), 2017.
- Delegating RAM Computations with Adaptive Soundness and Privacy Prabhanjan Ananth, Yu-Chi Chen, Kai-Min Chung, Huijia Lin and Wei-Kai Lin. In Theory of Cryptography – 13th International Conference, **TCC** 2016-B, 2016.

 $^{^{*}}$ The author ordering is random. Unmarked publications are alphabetical ordering.

 $^{^{\}dagger} \mathrm{The}$ author ordering is contribution-based.

Fall 2016

Summer 2016

Summer 2015

- Cryptography for Parallel RAM from Indistinguishability Obfuscation Yu-Chi Chen, Sherman S. M. Chow, Kai-Min Chung, Russell W. F. Lai, Wei-Kai Lin and Hong-Sheng Zhou.
 In proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science (ITCS), 2016.
- Co-evolvability of Games in Coevolutionary Genetic Algorithms
 Wei-Kai Lin and Tian-Li Yu.[†]
 In Conference on Genetic and Evolutionary Computation (GECCO), 2009.
- Optimal Sampling of Genetic Algorithms on Polynomial Regression Tian-Li Yu and Wei-Kai Lin.[†]
 In Conference on Genetic and Evolutionary Computation (GECCO), 2008.

MANUSCRIPTS

- Optimal Single-Server Private Information Retrieval Mingxun Zhou, Wei-Kai Lin, Yiannis Tselekounis, Elaine Shi.* https://eprint.iacr.org/2022/609, 2022.
- NanoGRAM: Garbled RAM with $\widetilde{O}(\log N)$ Overhead Andrew Park, Wei-Kai Lin, Elaine Shi.* https://eprint.iacr.org/2022/191, 2022.
- Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE Wei-Kai Lin, Ethan Mook, Daniel Wichs. https://eprint.iacr.org/2022/1703, 2022.

TEACHING

- Teaching assistant Spring 2017
 Course: Introduction to Cryptography, Cornell University
 with Prof. Elaine Shi.
 https://cs4830-sp17.jimdofree.com
 Also polished "Oblivious RAM Course Materials": https://pathoram.jimdofree.com
- Teaching assistant Course: Signal Processing, Cornell University with Prof. Charles Johnson.
- Co-instructor

Course: 2016 Summer School of Cryptography, Institute of Mathematics, Academia Sinica with Dr. Yu-Chi Chen, Dr. Kai-Min Chung, Prof. Chia-Liang Sun, and Dr. Julie Tzu-Yueh Wang.

Co-instructor

Course: 2015 Summer School of Cryptography, Institute of Mathematics, Academia Sinica with Prof. Jiun-Ming Chen, Dr. Yu-Chi Chen, Dr. Kai-Min Chung, Prof. Anly Li, Prof. Chia-Liang Sun, and Dr. Julie Tzu-Yueh Wang.

2019 and 2020

SERVICES

- Program committee member of Conference on Information-Theoretic Cryptography (ITC), 2023
- External reviewer Asiacrypt 2017, 2019; Eurocrypt 2016, 2017, 2020, 2022; ITCS 2020; PKC 2018; S&P 2018; SICOMP 2021; SODA 2020; TCC 2016, 2017, 2019, 2020.
- Volunteer of PhD Admissions Review PhD applications to Computer Science at Cornell University.

EARLIER EDUCATION AND EXPERIENCE

Mstar Semiconductor, Inc., Hsinchu, Taiwan October 2010 - February 2014 Senior Software Engineer in Digital TV Software R&D Division Earned 11 Short-Term Rewards.

Military Service, Taiwan

August 2009 - July 2010

Company Chief Counselor in Army

REFERENCES

- Prof. Elaine Shi runting@gmail.com Carnegie Mellon University
- Prof. Daniel Wichs danwichs@gmail.com Northeastern University
- Prof. Ilan Komargodski ilank@cs.huji.ac.il Hebrew University of Jerusalem
- Dr. Kai-Min Chung kmchung@iis.sinica.edu.tw Academia Sinica