WEI-KAI LIN

Computer Science, Cornell University
440 Gates Hall, Ithaca, NY 14853, USA
wklin@cs.cornell.edu ⋄ https://weikailin.github.io

RESEARCH INTERESTS

Cryptography and data privacy, especially focused on oblivious algorithms. Theoretical computer science in general.

EDUCATION

Cornell University, Ithaca, NY, USA *August 2016 - Present*
Fifth-year Ph.D. student in Computer Science.
Advisor: Prof. Elaine Shi.

National Taiwan University, Taipei, Taiwan *June 2009*
M.S. in Electrical Engineering (Computer Science Group)
Thesis: *Co-evolvability of games in coevolutionary genetic algorithms.*
Advisor: Prof. Tian-Li Yu.

National Taiwan University, Taipei, Taiwan *June 2007*
B.S. in Chemistry

PUBLICATIONS

- *A Logarithmic Lower Bound for Oblivious RAM (for all parameters)*
  Ilan Komargodski, and **Wei-Kai Lin**.
  In **Crypto**, 2021.
- *Oblivious RAM with Worst-Case Logarithmic Overhead*
  Gilad Asharov, Ilan Komargodski, **Wei-Kai Lin**, and Elaine Shi.
  In **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.
- *Oblivious Parallel Tight Compaction*
  Gilad Asharov, Ilan Komargodski, **Wei-Kai Lin**, Enoch Peserico, and Elaine Shi.
  In Information-Theoretic Cryptography (**ITC**), 2020.
- *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.

- *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.
- *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.

EXPERIENCE

NTT Research, East Palo Alto, CA, USA *Juen 2020 - August 2020*
Research Intern in Cryptography & Information Security Lab
Supervisor: Dr. Ilan Komargodski.

Academia Sinica, Taipei, Taiwan *November 2014 - July 2016*
Research Assistant in Institute of Information Science
Supervisor: Dr. Kai-Min Chung.

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

TEACHING

- *Teaching assistant* *Spring 2017*
  Course: Introduction to Cryptography, Cornell University
  with Prof. Elaine Shi.
  https://cs4830-sp17.jimdo.com/
- *Teaching assistant* *Fall 2016*
  Course: Signal Processing, Cornell University
  with Prof. Charles Johnson.
- *Co-instructor* *Summer 2016*
  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* *Summer 2015*
  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.