Rex Fernando

Department of Computer Science
UCLA
rex@cs.ucla.edu
Website: https://web.cs.ucla.edu/~rex

EDUCATION

UCLA, 2016-Present.
Ph.D.: Computer Science
Advisor: Amit Sahai

University of Wisconsin-Madison, 2013-2016.
M.S.: Computer Science
GPA: 3.76/4.0
Major GPA: 4.0/4.0

Iowa State University, 2009-2013.
B.S.: Computer Science and Applied Mathematics
GPA: 3.86/4.0

PUBLICATIONS

(Note: Publications in theoretical computer science venues list authors in alphabetical order, not in order of contribution.)

[1]: S. Badrinarayanan, **R. Fernando**, and A. Sahai. "Concurrent-Secure Two-Party Computation in Two Rounds from Subexponential LWE". *In submission*.

[2]: **R. Fernando**, A. Jain, and I. Komargodski. "Maliciously-Secure MrNISC in the Plain Model". *In submission*.

[3]: **R. Fernando**, I. Komargodski, Y. Liu, and E. Shi. "Secure Massively Parallel Computation for Dishonest Majority". In: *TCC 2020*.

[4]: S. Badrinarayanan, **R. Fernando**, A. Jain, D. Khurana, and A. Sahai. "Statistical ZAP Arguments". In: *EUROCRYPT 2020*.

[5]: S. Badrinarayanan, **R. Fernando**, V. Koppula, A. Sahai, and B. Waters. "Output Compression, MPC, and iO for Turing Machines". In: *ASIACRYPT 2019*.

[6]: **R. Fernando**, P. Rasmussen, and A. Sahai. "Preventing CLT Attacks on Obfuscation with Linear Overhead". In: *ASIACRYPT 2017*.

[7]: E. Bach and **R. Fernando**. "Infinitely Many Carmichael Numbers for a Modified Miller-Rabin Prime Test". In: *ISSAC 2016*.

MANUSCRIPTS

[8]: **R. Fernando**, I. Komargodski, Y. Liu, and E. Shi. "Secure Massively Parallel Computation for All-but-One Corruptions: Weaker Assumptions and Stronger Security". In: *Manuscript*. 2021.

[9]: **R. Fernando**, A. Jain, and I. Komargodski. "On Pseudorandom Functions in NC^1 from LWE". in: *Manuscript*. 2021.

RESEARCH EXPERIENCE

Intern *hosted by Prof. Elaine Shi*, Carnegie Mellon University School of Computer Science, Jun-Dec 2021

- Secure multiparty computation (MPC). Constructed the first concurrent-secure MPC protocol in two rounds in the plain model, with security based on the existence of subexponential indistinguishability obfuscation along with other standard assumptions. [2]
- Constructed a concurrent-secure two-party computation protocol, with security based on subexponential hardness of the learning with errors problem. [1]

Intern *hosted by Dr. Ilan Komargodski*, NTT Research, Jan-Sept 2020

- Large-Scale Secure Multi-Party Computation (MPC), where the total input size is much larger than the local storage of each party. Constructed several protocols which advance the state-of-the-art in this area. [8, 3].
- Studied new constructions of Pseudorandom Function Families (PRFs) from lattices. [9]
- Byzantine Agreement (BA). Studied BA protocols with sublinear communication complexity per party.

Summer Intern *hosted by Prof. Alon Rosen*, IDC Herzliya, Summer 2019

- Studied the average-case complexity of PPAD and other related subclasses of TFNP.

Research Assistant *with Prof. Amit Sahai*, UCLA, 2016-Present

- ZAP Arguments. Constructed the first public coin two message witness indistinguishable (WI) arguments for NP with statistical privacy, assuming quasi-polynomial hardness of the learning with errors (LWE) assumption. [4]
- Applications of randomized encodings in iO and MPC. Constructed output-compressing randomized encodings (OCREs) for Turing Machines in the shared randomness model from standard assumptions. Applied this to get succinct obfuscation as well as MPC for Turing machines where the transcript size is independent of the output size and running time. [5]
- Multilinear maps. Gave a defense against attacks on obfuscation which target a vulnerability in the CLT13 multilinear map construction. [6]

Research Assistant *with Prof. Eric Bach*, 2014-2016

- Algorithmic number theory. Studied randomized primality tests. Showed that weakening the Miller-Rabin test by artificially limiting the number of iterations yields infinitely many "Carmichael-like" numbers. [7]

CODING EXPERIENCE

Databases Course, Winter 2017

- Several projects using Apache Spark, including modifying Spark internally to cache user-defined function computation.

Distributed Systems Course, Fall 2015

- For the final project, wrote an event-based simulation of the Raft consensus protocol, with the goal of demonstrating how Raft handles various edge cases.

  `https://github.com/rex1fernando/raft-simulation`

Undergraduate Research Assistant, ISU Laboratory for Software Design, 2011-2013

- With two other students, built a totally new language feature on top of the OpenJDK compiler. 15,000 lines of code. https://ptolemy.cs.iastate.edu

Intern, Sukra Helitek, Summer 2010

- Implemented the visualization UI for a fluid dynamics simulation tool used by US Helicopter manufacturers to simulate helicopter rotor airflows.

Intern, Applied Genetics Network, Summer 2009

- Built a web version of the interactive tool I designed the previous summer, in order to allow multiple researchers to run resource-intensive analyses on a server. Allowed cross-referencing of results with a popular genome database.

Intern, Pioneer, Summer 2008

- Designed and built an interactive tool around a genomic selection analysis, for plant breeding researchers to use to visualize and make inferences about the effect of certain genotypes on desirable phenotypes.

TEACHING

Teaching Assistant *at UW Madison and UCLA*, 2013-2014 and 2018

- Formal languages and automata theory: Collaborated on the design of the midterm and final. Led a weekly discussion session in order to reinforce the concepts introduced in lecture.
- Algorithms: Held office hours, wrote model solutions for homework assignments, and led a biweekly discussion session in order to reinforce the concepts introduced in lecture.
- Data structures: Held office hours, designed and wrote model solutions and automated tests for homework assignments.
- Intro to programming: led a weekly interactive lab session to provide hands-on experience for students in the basics of programming.

SOFTWARE SKILLS

C, C++, Python, Haskell, Javascript, HTML/CSS.

COMMUNITY SERVICE

I have been an external reviewer for TCC 2017, PKC 2018 and 2020, EUROCRYPT 2019 and 2020 and CRYPTO 2020.

November 15, 2021