REX FERNANDO

Department of Computer Science
UCLA
rex@cs.ucla.edu
515-231-9568

EDUCATION

UCLA, 2016-Present
PhD Student: Cryptography
Current GPA: 3.97/4.0

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 (Magna Cum Laude)

EXPERIENCE

Research Assistant under Amit Sahai, 2016-Present

- Multilinear maps. Collaborators: Peter Rasmussen and Amit Sahai. Multilinear maps are a key tool in constructions of indistinguishability obfuscation. We give a defense against attacks on obfuscation which target a vulnerability in the CLT13 multilinear map construction. Our key insight is that the function being obfuscated needs to have a certain property to be attacked. We call these functions "input partitionable," and we describe a modification to a function which causes it to be unpartitionable and which only causes an additive linear blowup in the size of the branching program which computes the function. [4]
- Applications of randomized encodings in iO and MPC. Collaborators: Saikrishna Badrinarayanan, Venkata Koppula, and Amit Sahai. We construct output-compressing randomized encodings (OCREs) for Turing Machines in the shared randomness model, assuming iO for circuits and either LWE, DDH, or N^{th} residuosity. An OCRE is a randomized encoding where the encoding size is independent of the running time and output length of the Turing Machine on the given input. This notion was previously proved impossible in the plain model. We use this to construct, among other things, a malicious-secure MPC protocol for Turing Machines in the random oracle model whose communication complexity is independent of the running time and output length.[2]
- Multiparty computation. Collaborators: Saikrishna Badrinarayanan and Amit Sahai. We are studying MPC protocols with round-optimal communication.

Research Assistant under 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 allows infinitely many composite numbers to pass by undetected. [1]

Teaching Assistant at UW Madison, 2013-2014

- Algorithms: wrote model solutions for homework assignments, and led a biweekly review session.
- Data structures: designed and wrote model solutions and automated tests for homework assignments.
- Intro to programming: led a weekly lab session.

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

- Programming language design. Developed a new language feature called "event inheritance" for the Ptolemy research language. [3] Worked to formalize Ptolemy's type soundness proof using an interactive theorem prover (Coq). Helped implement the compiler for Ptolemy. `http://web.cs.iastate.edu/~ptolemy/`

Intern, Sukra Helitek, Summer 2010

- Worked on a computational fluid dynamics simulation tool used by US Helicopter manufacturers to simulate helicopter rotor airflows.

Undergraduate Research Assistant, ISU Robotics Laboratory, 2009-2010

- 3D Modeling. Animated several rigid body collision models using OpenGL. `http://robotics.cs.iastate.edu/Research3DImpact`

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.

RECOGNITION

UW CS Summer Research Assistant Award

Winner, ISU Game Development Competition
My team developed a real-time strategy game, including the engine. Features included fully simulated projectiles and multiplayer over the local network. First place ($10000) in the PC/Console category.

Presenter, ISU Symposium on Undergraduate Research
Was selected to present my work on event inheritance in Ptolemy.

ISU Dean's List

PUBLICATIONS

S. Badrinarayanan, R. Fernando, V. Koppula, A. Sahai, and B. Waters. "Output Compression, MPC, and iO for Turing Machines". In: *IACR Cryptology ePrint Archive* 2018 (2018). URL: https://eprint.iacr.org/2018/866.

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

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

M. Bagherzadeh, R. Dyer, R. Fernando, J. Sánchez, and H. Rajan. "Modular reasoning in the presence of event subtyping". In: *Modularity 2015*.

December 4, 2018