Rex Fernando

Department of Computer Science
UCLA
rex@cs.ucla.edu
515-231-9568
Website: `https://web.cs.ucla.edu/~rex`

EDUCATION

UCLA, 2016-Present.
PhD Student: Cryptography
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

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

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*.

MANUSCRIPTS

S. Badrinarayanan, R. Fernando, A. Jain, D. Khurana, and A. Sahai. "Statistical ZAP Arguments". In: *IACR Cryptology ePrint Archive*. 2019, p. 780. URL: `https://eprint.iacr.org/2019/780`.

S. Badrinarayanan, R. Fernando, and A. Sahai. "Secure Two Party Computation in Two Rounds". In: *Manuscript*. 2019.

RESEARCH EXPERIENCE

Summer Internship with Alon Rosen, Summer 2019

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

Research Assistant under Amit Sahai, 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. [2]
- Multiparty computation. Studying MPC protocols under super-polynomial simulation with round-optimal communication.
- 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. [3]
- Multilinear maps. Gave a defense against attacks on obfuscation which target a vulnerability in the CLT13 multilinear map construction. [6]

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 yields infinitely many "Carmichael-like" numbers. [1]

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 EUROCRYPT 2019.

September 11, 2019