

Name: **Rafael Pass**

Title: Prof Asst

Office: Upson Hall, Room 5139

Phone: (607)255-5578

Email: rafael@cs.cornell.edu

University Activities

- Cornell Boom Faculty contact
- Cornell Ph.D Admission committee

Professional Activities

- 29th Annual International Cryptology Conference (CRYPTO 2009) in Santa Barbara, CA, USA, August 2009.
- 6th Theory of Cryptography Conference (TCC'09), 2009

Publications

- *Non-malleability Amplification*. (STOC'09) H. Lin and R. Pass.
- *A Unified Framework for Concurrent Security: Universal Composability from Stand-alone Non-malleability*. (STOC'09) H. Lin, R. Pass and M. Venkatasubramanian.
- *Black-box Constructions of Two-party Protocols from One-way Functions*. (TCC'09) R. Pass and H. Wee.
- *Adaptive One-way Functions and Applications*. (Crypto'08) O. Pandey, R. Pass and V. Vaikuntanathan.

Lectures

- AFOSR presentation, Concurrent Security, 2009
- MIT, Non-malleability Amplification, 2009
- Cornell, Game Theory with Costly Computation, 2009
- Weizmann, Game Theory with Costly Computation, 2009
- KTH, Game Theory with Costly Computation, 2009
- I3P presentation (at Cornell), Towards new definitions of concurrent security, 2008
- World Congress of Game Theory, Iterated Regret Minimization: A New Solution Concept, 2008
- Dagstuhl, Algorithmic Rationality: Game Theory with Costly Computation, 2008
- CRYPTO 2008, Adaptive One-way Functions and Applications, 2008