Rafael Pass

University Activities

- Faculty recruiting committee

Professional Actitivities

- 39th ACM Symposium on Theory of Computing (STOC'08) in Victoria, May 17-20.
- 35th International Colloquium on Automata, Languages and Programming (ICALP'08) in Reykjavik, July 7-11.
- RSA Conference 2008, Cryptographers' Track (CT-RSA'08) in San Francisco, April 8-11
- 34th International Colloquium on Automata, Languages and Programming (ICALP'07) in Wroclaw, July 9-13.

Publications

- *Precise Concurrent Zero Knowledge.* (EuroCrypt'08) O. Pandey, R. Pass, A. Sahai, W. Tseng and M. Venkitasubramaniam.
- *Concurrent Non-malleable Commitments from One-way Functions.* (TCC'08) H. Lin, R. Pass and M. Venkitasubramaniam.
- *On Constant-Round Concurrent Zero Knowledge.* (TCC'08) R. Pass and M. Venkitasubramaniam.
- *Relations Among Notions of Non-malleability for Encryption.* (AsiaCrypt'07) R. Pass, V. Vaikuntanathan and A. Shelat.
- *Bounded-CCA Secure Encryption.* (AsiaCrypt'07) R. Cramer, G. Hanaoka, D. Hofheinz, H. Imai, E. Kiltz, R. Pass, A. Shelat and V. Vaikuntanathan.
- *Cryptography from Sunspots: How to Use an Imperfect Reference String.* (FOCS'07) R. Canetti, R. Pass and A. Shelat.

Lectures

- MIT, TOC Colloquium, May 6th: Game Theory with Costly Computation
- AFOSR presentation, June 12: Defending against Man-in-the-middle Attacks.

Awards

- NSF Career Award, $500,000
- AFOSR grant