

Rafael Pass

Department of Computer Science
Cornell University
Ithaca, NY 14853
<http://www.cs.cornell.edu/~rafael>

Office: (607) 255-5578
Cell: (617) 832 52 04
Citizenship: Swedish
rafael@cs.cornell.edu

Research Interest

Cryptography and its interplay with Computational Complexity (and Game Theory).

Current Position

Assistant Professor in Computer Science.
2006–present *Cornell University*, Ithaca, NY, USA

Education

Ph.D. in Computer Science, 2006.
2004–2006 *Massachusetts Institute of Technology*, Cambridge, MA, USA
Thesis Advisor: Prof. Silvio Micali.
Thesis: *A Precise Computational Approach to Knowledge.*

Licentiat (M.S.) in Computer Science, 2004.
2001–2004 *Royal Institute of Technology*, Stockholm, Sweden.
Thesis Advisor: Prof. Johan Håstad.
Thesis: *Alternative Variants of Zero Knowledge Proofs.*

Civilingenjör (Combined B.S. and M.S.) in Engineering Physics, 2000.
1995–2000 *Royal Institute of Technology*, Stockholm, Sweden.

Additional Educational Experience

1999–2000 *La Sorbonne, Paris I*, Paris, France.
Maitrise (fourth year studies) in Philosophical Logic.

1998–1999 *Ecole Polytechnique*, Paris, France.
Diploma in Mathematics and Computer Science.

Languages

- **Swedish:** native,
- **English, French, Polish:** fluent,
- **Spanish, German, Hebrew:** average.

Honors

- IBM Josef Raviv Fellow (declined), 2006.
- MIT Big George Ventures Fellow, 2006.
- MIT Akamai Presidential Fellow, 2004.
- Sweden-America Foundation Fellow, 2004.

Scientific Services

Program Commitees:

- 29th Annual International Cryptology Conference (CRYPTO'09) in Santa Barbara, CA, USA, August, 2009.
- 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, 2008.
- 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, 2007.
- 4th Theory of Cryptography Conference (TCC'07) in Amsterdam, Feb. 21-24, 2007.

Journal Refereeing: Journal of the ACM (JACM), Information and Computation, Journal of Cryptology.

Conference Refereeing: CRYPTO 2002, ICALP 2002, STOC 2003, CRYPTO 2004, STOC 2004, FOCS 2004, TCC 2004, CRYPTO 2005, ASIACRYPT 2005, ICALP 2005, STOC 2005, FOCS 2005, TCC 2005, STOC 2006, CCC 2006, FOCS 2006, STACS 2007, EUROCRYPT 2007, STOC 2007, CRYPTO 2007, FOCS 2007, TCC 2008, EUROCRYPT 2008.

Teaching Experience

Teaching

- *CS 487 Introduction to Cryptography*. Cornell University, Fall 2007.
- *CS 787 Topics in Cryptography*. Cornell University, Spring 2007.
- *CS 687 Introduction to Cryptography*. First graduate course in Cryptography at Cornell, Fall 2006.

Teaching Assistantships

- *Cryptographic Game Theory*. Massachusetts Institute of Technology, 2005.
Helped design a new course bridging cryptographic protocols and game theory.
- *Foundations of Cryptography*. Royal Institute of Technology, 2003.
- *Algorithms, Complexity and Data Structures*. Royal Institute of Technology, 2002, 2003.
- *Programming Techniques*. Royal Institute of Technology, 1997.

Current Ph.D. Advisees

- Huijia (Rachel) Lin
- Wei-Lung Dustin Tseng
- Muthuramakrishnan Venkitasubramaniam

Theses Supervised

- Mattias Ekholm, *Anonymous Electronic Cash - A Case Study*, Master's thesis. Department of Computer Science, Royal Institute of Technology, 2002-2003.
- Jonas Melander, *Security in Wireless Local Area Networks*, Master's thesis. Department of Computer Science, Royal Institute of Technology, 2003.

Work Experience

- 2001–2003 *Dactylis Software Solutions*, Stockholm, Sweden.
Co-founder of software company specializing in security solutions.
- 2000–2001 *PriceWaterhouseCoopers*, Paris, London.
Senior Analyst in Mergers and Acquisitions/Venture Capital.
- 3-8/2000 *JP Morgan Securities*, Paris.
Business Analyst in Emerging Markets Trading.

Publications

1. R. Pass and M. Venkatasubramanian. On Constant-Round Concurrent Zero Knowledge. To appear in *Proceedings of 5th Theory of Cryptography Conference (TCC 2008)*, 2008.
2. H. Lin, R. Pass and M. Venkatasubramanian. Concurrent Non-malleable Commitments from One-way Functions. To appear in *Proceedings of 5th Theory of Cryptography Conference (TCC 2008)*, 2008.
3. R. Pass, A. Shelat and V. Vaikuntanathan. Relations Among Notions of Non-malleability for Encryption. *Advances in Cryptology (ASIACRYPT 2007)*, Springer LNCS, pages 519–525, 2008.
4. R. Cramer, G. Hanaoka, D. Hofheinz, H. Imai, E. Kiltz, R. Pass, A. Shelat and V. Vaikuntanathan. Bounded-CCA Secure Encryption. *Advances in Cryptology (ASIACRYPT 2007)*. Springer LNCS, pages 502–518, 2008.
5. R. Canetti, R. Pass and A. Shelat. Cryptography from Sunspots: How to Use an Imperfect Reference String. *Proceedings of the 48th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2007)*, pages 249–263, 2007.
6. R. Pass, M. Venkatasubramanian. An Efficient Parallel Repetition Theorem for Arthur-Merlin Games. To appear in the *Proceedings of the 39th Annual Symposium on Theory of Computing (STOC 2007)*, pages 420–429, 2007.
7. R. Canetti, Y. Dodis, R. Pass and S. Walfish. Universally Composable Security with Global Set-up. *Proceedings of 4th Theory of Cryptography Conference (TCC 2007)*, pages 61–85, 2007.
8. S. Micali, R. Pass and A. Rosen. Input-Indistinguishable Computation. *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006)*, pages 367–378, 2006.

9. R. Pass, A. Shelat and V. Vaikuntanathan. Construction of a Non-malleable Encryption Scheme From Any Semantically Secure One. *Advances in Cryptology (CRYPTO 2006)*, Springer LNCS, pages 271-289, 2006.
10. R. Pass. Parallel Repetition of Zero-Knowledge Proofs and the Possibility of Basing Cryptography on NP-Hardness. *Proceedings of Conference on Computational Complexity (CCC 2006)*, pages 96–110, 2006. Invited to Computational Complexity special issue on the Conference of Computational Complexity 2006.
11. S. Micali and R. Pass. Local Zero Knowledge. *Proceedings of the 38th Annual Symposium on Theory of Computing (STOC 2006)*, pages 306–315, 2006.
12. R. Pass and A. Rosen. Concurrent Non-malleable Commitments. *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005)*, pages 563–572. Invited to SIAM Journal of Computing special issue on selected papers of FOCS 2005.
13. B. Barak, R. Canetti, Y. Lindell, R. Pass and T. Rabin. Secure Computation without Authentication. *Advances in Cryptology (CRYPTO 2005)*, Springer LNCS 3621, pages 361–377, 2003.
14. R. Pass and A. Shelat. Unconditional Characterizations of Non-interactive Zero-Knowledge *Advances in Cryptology (CRYPTO 2005)*, Springer LNCS 3621, pages 118–134, 2005.
15. R. Pass and A. Rosen. New and Improved Constructions of Non-malleable Cryptographic Protocols. *Proceedings of the 37th Annual Symposium on Theory of Computing (STOC 2005)*, pages 533–542, 2005. Invited to SIAM Journal of Computing special issue on selected papers of STOC 2005.
16. B. Barak, R. Canetti, J. Nielsen and R. Pass. Universally Composable Protocols with Relaxed Set-Up Assumptions. *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2004)*, pages 186-195, 2004.
17. R. Pass. Bounded-Concurrent Secure Multi-Party Computation with a Dishonest Majority. *Proceedings of the 36th Annual Symposium on Theory of Computing (STOC 2004)*, pages 232-241, 2004.
18. B. Barak and R. Pass. On the Possibility of One-Message Weak Zero-Knowledge. *Proceedings of 1st Theory of Cryptography Conference (TCC 2004)*, pages 121-132, 2004.
19. R. Pass and A. Rosen. Bounded-Concurrent Secure Two-Party Computation in a Constant Number of Rounds. *Proceedings of the 44rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2003)*, pages 404–413, 2003.
20. R. Pass. On Deniability in the Common Reference String and Random Oracle Models. *Advances in Cryptology (CRYPTO 2003)*, Springer LNCS 2729, pages 316–337, 2003.

21. R. Pass. Simulation in Quasi-Polynomial Time and its Application to Protocol Composition. *Advances in Cryptology (EUROCRYPT 2003)*, Springer LNCS 2656, pages 160–176, 2003.

Technical Reports

22. R. Pass, *A Precise Computational Approach to Knowledge*. Ph.D. Thesis at MIT, 2006.
23. R. Pass, *Alternative Variants of Zero-Knowledge Proofs*. ISBN 91-7283-933-3, Licentiate Thesis at Royal Institute of Technology, 2004.
24. R. Pass, *Local Modeling in Text Categorization*. TRITA-NA-E0106, Final Thesis at Royal Institute of Technology, 2000.
25. R. Pass, *Pricing of Brady Bonds*. Final Thesis at Ecole Polytechnique, 1999.