# Rafael Pass

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

Office: (607) 255-5578
Cell: (607) 379-9993
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.**
07/15/2006–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.

## Awards and Honors

- Invited Talk at Theory of Cryptography Conference, 2011.
- Alfred P. Sloan Fellow, 2011.
- AFOSR Young Investigator Award, 2010.
- Microsoft Research Faculty Fellow, 2009.
- NSF Career Award, 2008.
- IBM Josef Raviv Fellow (declined), 2006.
- MIT Big George Ventures Fellow, 2006.
- MIT Akamai Presidential Fellow, 2004.
- Sweden-America Foundation Fellow, 2004.
- Papers invited to Special Issues:
  1. R. Canetti, H. Lin and R. Pass. *Adaptive Hardness and Composable Security from Standard Assumptions.* Invited to SIAM Journal of Computing special issue on selected papers of FOCS 2010.
  2. R. Pass and M. Venkitasubramaniam. *On Constant-Round Concurrent Zero Knowledge.* Invited to Journal of Cryptology.
  3. H. Lin, R. Pass and M. Venkitasubramaniam. *Concurrent Non-malleable Commitments from One-way Functions.* Invited to Journal of Cryptology.
  4. R. Canetti, Y. Dodis, R. Pass and S. Walfish. *Universally Composable Security with Global Set-up.* Invited to Journal of Cryptology.
  5. R. Pass, *Parallel Repetition of Zero-Knowledge Proof and the Possibility of Basing Cryptography on NP-Hardness.* Invited to Computational Complexity special issue on the Conference of Computational Complexity 2006.
  6. R. Pass and A. Rosen, *New and Improved Constructions of Non-malleable Cryptographic Primitives.* Invited to SIAM Journal of Computing special issue on selected papers of FOCS 2005.
  7. R. Pass and A. Rosen, *Concurrent Non-Malleable Commitments.* Invited to SIAM Journal of Computing special issue on selected papers of STOC 2005.

## Teaching Experience

### Teaching

- *CS 2800 Discrete Structures.* Cornell University, Spring 2011.
- *CS 4830 Introduction to Cryptography.* Cornell University, Fall 2007, Fall 2008, Fall 2010.
- *CS 6830 Cryptography.* First graduate course in Cryptography at Cornell, Fall 2006, Spring 2008, Fall 2009, Fall 2011.
- *CS 6810 Theory of Computing.* Cornell University, Spring 2009.
- *CS 7893 Cryptography Seminar.* Cornell University, Fall 2008, Spring 2009, Fall 2009, Spring 2010, Fall 2011.
- *CS 787 Topics in Cryptography.* Cornell University, Spring 2007.
- *Cryptographic Game Theory.* Massachusetts Institute of Technology, 2005.
  Helped design a new course bridging cryptographic protocols and game theory.

### Lecture Notes

- R. Pass and A. Shelat. *A Course in Cryptography.* Lecture notes for an upper-level undergraduate course in Cryptography. Available online. (In revision at MIT Press).
- R. Pass and W. Tseng. *A Course in Discrete Structures.* Lecture notes for a basic undergraduate course in Discrete Mathematics, with applications to Cryptography and Game Theory. Available online.

### Graduated Ph.D. Students

- Muthu Venkitasubramaniam (June 2010; CI Fellow; now tenure-track faculty at U. Rochester)
- Huijia (Rachel) Lin (July 2011; now postdoc at MIT; tenure-track faculty at Chinese University of Hong-Kong, on leave)
- Wei-Lung Dustin Tseng (July 2011; now at Google)

### Current Ph.D. Students

- Eleanor Birrell (expected graduation May 2013)
- Edward Lui (expected graduation May 2013)

### Current Postdocs

- Mohammad Mahmoody (previously at Princeton)
- Kai-min Chung (previously at Harvard)

## Work Experience

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

## Publications

1. K. Chung and R. Pass. *The Randomness Complexity of Parallel Repetition.* To appear in *Proceedings of the 52th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2011)*, 2011.

2. E. Birrell and R. Pass. *Approximately Strategy-proof Voting.* In *Proceeding of the 22st International Joint Conference on Artificial Intelligence (IJCAI 2011)*, pages 67–72, 2011.

3. R. Pass. *Limits of Provable Security from Standard Assumptions.* In *Proceedings of the 41th Annual Symposium on Theory of Computing (STOC 2011)*, pages 109–118, 2011.

4. H. Lin and R. Pass. *Constant-round Non-malleable Commitments from Any One-way Function.* In *Proceedings of the 41th Annual Symposium on Theory of Computing (STOC 2011)*, pages 705–714, 2011.

5. A. Bjorndahl, J. Halpern and R. Pass. *Reasoning about Justified Belief.* In *Proceedings of the 12th Conference on Theoretical Aspects of Rationality and Knowledge (TARK 2011)*, pages 221-227, 2011.

6. R. Pass. *Concurrent Security and Non-malleability*, In *Proceedings of the 8th Theory of Cryptography Conference (TCC 2011)*, page 540, 2011. Invited Talk.

7. J. Gehrke, E. Lui and R. Pass. *Towards Privacy in Social Networks: A Zero-knowledge Based Definition of Privacy.* In *Proceedings of the 8th Theory of Cryptography Conference (TCC 2011)*, pages 432–449, 2011.

8. J. Halpern and R. Pass. *Algorithmic rationality: adding cost of computation to game theory. SIGecom Exchanges*, Vol 10(2), pages 9–15, 2011.

9. R. Pass, W. Tseng and M. Venkitasubramaniam. *Towards Non-black-box Separations in Cryptography.* In *Proceedings of the 8th Theory of Cryptography Conference (TCC 2011)*, pages 579–596, 2011.

10. H. Lin and R. Pass. *Concurrent Non-malleable Zero-knowledge with Adaptive Inputs.* In *Proceedings of the 8th Theory of Cryptography Conference (TCC 2011)*, pages 274–292, 2011.

11. R. Pass and A. Shelat. *Renegotiation-safe Protocols.* In *Proceedings of the 2nd Innovations in Computer Science (ICS 2011)*, 2011.

12. T. Roeder, R. Pass and F. Schneider. *Multi-Verifier Signatures.* To appear in *Journal of Cryptology*, 2010.

13. R. Canetti, H. Lin and R. Pass. Adaptive Hardness and Composable Security from Standard Assumptions. In *Proceedings of the 51th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2010)*, pages 541-550, 2010. Invited to *SIAM Journal of Computing*, special issue on selected papers of FOCS 2010.

14. H. Lin, R. Pass, W. Tseng and M. Venkitasubramaniam. Concurrent Non-Malleable Zero Knowledge Proofs. *Advances in Cryptology (CRYPTO 2010)*, Springer LNCS 6223, pages 429–446, 2010.

15. R. Pass and H. Wee. Constant-round Non-malleable Commiments from Subexponential One-way Functions. *Advances in Cryptology (EUROCRYPT 2010)*, Springer LNCS 6110, pages 638–655, 2010.

16. J. Halpern and R. Pass. I Don't Want to Think about it Now: Decision Theory with Costly Computation. *Proceeding of the 12th International Conference on the Principles of Knowledge Representation and Reasoning (KR 2010)*, 2010.

17. R. Pass, M. Venkitasubramaniam and W. Tseng. Eye for an Eye: Efficient Concurrent Zero Knowledge in the Timing Model. In *Proceedings of the 7th Theory of Cryptography Conference (TCC 2010)*, pages 518–534, 2010.

18. R. Pass and M. Venkitasubramaniam. On Public versus Private Coins in Zero-Knowledge Proofs. In *Proceedings of the 7th Theory of Cryptography Conference (TCC 2010)*, pages 588–605, 2010.

19. R. Pass, J. Hastad, D. Wikstrom and K. Pietrzak. An Efficient Parallel Repetition Theorem. In *Proceedings of the 7th Theory of Cryptography Conference (TCC 2010)*, pages 1–18, 2010.

20. J. Halpern and R. Pass. Game Theory with Costly Computation: Formulation and Application to Protocol Security. In *Proceeding of the 1st Innovations in Computer Science Conference (ICS 2010)*, 2010.

21. R. Pass, W. Tseng and D. Wikstrom. On the Composition of Public-coin Zero Knowledge. In *Advances in Cryptology (CRYPTO 2009)*, Springer LNCS 5677, pages 160-176, 2009. Full version to appear in *SIAM Journal of Computing*, 2011.

22. J. Halpern and R. Pass. Iterated Regret Minimization: A New Solution Concept. In *Proceeding of the 21st International Joint Conference on Artificial Intelligence (IJCAI 2009)*, pages 153-158, 2009. Full version to appear in *Games and Economic Behavior*, 2011.

23. J. Halpern and R. Pass. A Logical Characterization of Iterated Admissability. In *Proceedings of the 12th Conference on Theoretical Aspects of Rationality and Knowledge (TARK 2009)*, pages 146-155, 2009.

24. J. Halpern, R. Pass and V. Raman. An Epistemic Characterization of Zero Knowledge. In *Proceedings of the 12th Conference on Theoretical Aspects of Rationality and Knowledge (TARK 2009)*, pages 156–165, 2009.

25. H. Lin and R. Pass. Non-malleability Amplification. In *Proceedings of the 41th Annual Symposium on Theory of Computing (STOC 2009)*, pages 189–198, 2009.

26. H. Lin, R. Pass and M. Venkitasubramaniam. A Unified Framwork for Concurrent Security: Universal Composability from Stand-alone Non malleability. In *Proceedings of the 41th Annual Symposium on Theory of Computing (STOC 2009)*, pages 179–188, 2009.

27. R. Pass and H. Wee. Black-box Constructions of Two-Party Protocols from One-way Functions. In *Proceedings of the 6th Theory of Cryptography Conference (TCC 2009)*, pages 403–418, 2009.

28. O. Pandey, R. Pass and V. Vaikuntanathan. Adaptive One-Way Functions and Applications. *Advances in Cryptology (CRYPTO 2008)*, Springer LNCS 5157, pages 57-074, 2003.

29. R. Pass and M. Venkitasubramaniam. On Constant-Round Concurrent Zero Knowledge. *Proceedings of 5th Theory of Cryptography Conference (TCC 2008)*, pages 553–570, 2008. Invited to Journal of Cryptology.

30. H. Lin, R. Pass and M. Venkitasubramaniam. Concurrent Non-malleable Commitments from One-way Functions. *Proceedings of 5th Theory of Cryptography Conference (TCC 2008)*, pages 571–588, 2008. Invited to Journal of Cryptology.

31. O. Pandey, R. Pass, A. Sahai, W. Tseng and M. Venkitasubramaniam. Precise Concurrent Zero Knowledge. *Advances in Cryptology (EUROCRYPT 2008)*, Springer LNCS 4965, pages 397–414, 2008.

32. 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.

33. 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.

34. 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.

35. R. Pass and M. Venkitasubramaniam. An Efficient Parallel Repetition Theorem for Arthur-Merlin Games. *Proceedings of the 39th Annual Symposium on Theory of Computing (STOC 2007)*, pages 420–429, 2007.

36. 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. Invited to Journal of Cryptology.

37. 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.

38. 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.

39. 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.

40. S. Micali and R. Pass. Local Zero Knowledge. *Proceedings of the 38th Annual Symposium on Theory of Computing (STOC 2006)*, pages 306–315, 2006.

41. 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. Full version in *SIAM Journal of Computing* 37(6), pages 1891–1925, 2008, special issue on selected papers from FOCS 2005.

42. 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. Full version to appear in *Journal of Cryptology*, 2011.

43. R. Pass and A. Shelat. Unconditional Characterizations of Non-interactive Zero-Knowledge *Advances in Cryptology (CRYPTO 2005)*, Springer LNCS 3621, pages 118–134, 2005.

44. 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. Full version in *SIAM Journal of Computing* 38(2), pages 702-752, 2008, special issue on selected papers of STOC 2005.

45. 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.

46. 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.

47. 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.

48. 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.

49. 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.

50. 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

51. M. Mahmoody and R. Pass. *The Curious Case of Non-interactive Commitments: Separating Black-box and Non-black-box Contructions.* Manuscript, 2011.

52. K. Chung, R. Pass and W. Tseng. *The Knowledge-tightness of Parallel Composition and Applications to Concurrent Zero Knowledge.* Manuscript, 2011.

53. J. Halpern and R. Pass. *Justified Belief and Rationality.* Manuscript, 2011.

54. J. Halpern and R. Pass. *Sequential Equilibrium in Games of Imperfect Recall.* Manuscript, 2011.

55. R. Pass, W. Tseng and M. Venkitasubramaniam. *Concurrent Zero Knowledge, Revisited.* Manuscript, 2011

56. R. Pass, A. Rosen and W. Tseng. *Public-coin Parallel Zero Knowledge.* Manuscript, 2011

57. S. Micali and R. Pass. *Precise Cryptography.* Manuscript, 2006.

58. R. Pass, *A Precise Computational Approach to Knowledge.* Ph.D. Thesis at MIT, 2006.

59. R. Pass, *Alternative Variants of Zero-Knowledge Proofs.* ISBN 91-7283-933-3, Licentiate Thesis at Royal Institute of Technology, 2004.

60. R. Pass, *Local Modeling in Text Categorization.* TRITA-NA-E0106, Final Thesis at Royal Institute of Technology, 2000.

61. R. Pass, *Pricing of Brady Bonds.* Final Thesis at Ecole Polytechnique, 1999.

## Selected Talks

- STOC, 2011, "Limits of Provable Security from Standard Assumptions".
- Theory of Cryptography Conference, 2011, "Concurrency and Non-malleability", invited talk.
- NSF Workshop on Economic Incentives and Security, 2011, "Game Theory and Security".
- ICS, Beijing, 2011, "Renegotiation-Safe Protocols".
- ITCS, Beijing, 2011, "Constant-round non-malleable commitments from One-way Functions".
- Eagle Workshop, Buffalo University, 2010,"Constant-round non-malleable commitments from One-way Functions".
- Princeton Workshop on Barriers in Complexity Theory, 2010, "Concurrency and Parallel repetition".
- Santa Fee Institute, 2010, "Algorithmic Rationality: Game Theory with Costly Computation".
- AFOSR, Washington D.C., 2010, "Concurrent Zero-Knowledge in the Timing Model".
- SIAM Conference on Discrete Math, 2010, "Game Theory with Costly Computation".
- Aarhus Workshop on Solution concepts for extensive form games, 2010, "Game Theory with Costly Computation".
- Princeton Workshop on Distributed Game Theory, 2010, "Game Theory with Costly Computation".
- Behavioral and Quantitative Game Theory, Newport Beach, 2010, "Game Theory with Costly Computation".
- ICS, Beijing, 2010, "Game Theory with Costly Computation: Formulation and Application to Protocol Security".
- AFOSR, Washington D.C., 2009, "Non-malleability Amplification".
- IJCAI, 2009, "Iterated Regret Minimization: A New Solution Concept in Games".

- Microsoft, Sillicon Valley, 2009, "Game Theory with Costly Computation".
- TARK, Stanford, 2009, "A Logical Characterization of Iterated Admissibility".
- MIT, 2009, "Non-malleability Amplification".
- Cornell Univesity, 2009, "Game Theory with Costly Computation".
- Weizmann Institute of Science, 2009, "Algorithmic Rationality: Game Theory with Costly Computation".
- Dagstuhl, Germany, 2008, "Algorithmic Rationality: Game Theory with Costly Computation".
- CRYPTO, Santa Barbara, 2008, "Adaptive One-way Functions and Applications".
- AFOSR, Washington D.C., 2008, "Concurrent Non-malleable Commitments from One-way Functions".
- World Congress of Game Theory, Northwestern University, Chicago, 2008, "Iterated Regret Minimization: A More Realistic Solution Concept".
- Massachusetts Institute of Technology, 2008, "Game Theory with Costly Computation".
- Massachusetts Institute of Technology, 2007, "Precise Cryptography".
- Dagstuhl, Germany, 2007, "Precise Cryptography".
- Insititute for Pure and Applied Mathematics (IPAM), UCLA, Los Angeleges, 2006, "Precise Zero Knowledge".
- FOCS, Berkeley, 2006, "Input-Indistinguishable Computation".
- Massachusetts Institute of Technology, 2006, "A Precise Computational Approach to Knowledge".
- STOC, Seattle, 2006, "Local Zero Knowledge".
- Cornell University, 2006, "Concurrency and the Security of Protocols".
- Georgia Tech, 2006, "Concurrency and the Security of Protocols".
- University of Chicago, 2006, "Concurrency and the Security of Protocols".
- IBM Almaden Research Center, 2006, "Concurrency and the Security of Protocols".
- Microsoft Research, Silicon Valley Campus, 2006, "Concurrency and the Security of Protocols".
- Royal Institute of Technology, 2005, "Alternative Variants of Zero-Knowledge Proofs".

- STOC, Baltimore, 2005, "New and Improved Constructions of Non-Malleable Commitments".
- IBM T.J. Hawthorne Research Center, 2005, "Secure Computation Without Authentication".
- CRYPTO, Santa Barbara, 2005, "Secure Computation Without Authentication".
- STOC, Chicago, 2004, "Bounded-Concurrent Secure Multi-Party Computation with a Dishonest Majority".
- Royal Institute of Technology, 2004, "Bounded-Concurrent Secure Multi-Party Computation with a Dishonest Majority".
- IBM T.J. Hawthone Research Center, 2004, "Bounded-Concurrent Secure Multi-Party Computation with a Dishonest Majority".
- New York University, 2004, "Bounded-Concurrent Secure Multi-Party Computation with a Dishonest Majority".
- Technion, 2004, "Bounded-Concurrent Secure Multi-Party Computation with a Dishonest Majority".
- TCC, Cambridge, 2004, "On the Possibility of One-message Weak Zero-Knowledge".
- FOCS, Cambridge, 2003, "Bounded-Concurrent Secure Two-Party Computation in a Constant Number of Rounds".
- Massachusetts Institute of Technology, 2003, "Bounded-Concurrent Secure Two-Party Computation in a Constant Number of Rounds".
- New York University, 2003, "Bounded-Concurrent Secure Two-Party Computation in a Constant Number of Rounds".
- Royal Institute of Technology, 2003, "Bounded-Concurrent Secure Two-Party Computation in a Constant Number of Rounds".
- CRYPTO, Santa Barbara, 2003, "On Deniability in the Common Reference String and Random Oracle Models".
- EUROCRYPT, Warsaw, Poland, 2003, "Simulation in Quasi-Polynomial Time and its Application to Protocol Composition".

## Scientific Services

**Program Commitees:**

- 31th Annual International Cryptology Conference (CRYPTO'11).
- 1st Innovations in Computer Science Conference (ICS'10).
- 30th Annual International Cryptology Conference (CRYPTO'10).
- 29th Annual International Cryptology Conference (CRYPTO'09).
- 6th Theory of Cryptography Conference (TCC'09).
- 39th ACM Symposium on Theory of Computing (STOC'08).
- 35th International Colloquium on Automata, Languages and Programming (ICALP'08).
- RSA Conference 2008, Cryptographers' Track (CT-RSA'08).
- 34th International Colloquium on Automata, Languages and Programming (ICALP'07).
- 4th Theory of Cryptography Conference (TCC'07).

**Journal Refereeing:** Journal of the ACM, SIAM Journal of Computing, Information and Computation, Journal of Cryptology, Games and Economic Behavior

## Grants

- "Alfred P. Sloan Foundation Fellowship", Sloan Fundation, $50,000. PI 9/15/2011-9/15/2013.
- "Minimizing Overhead for Secure Computation", DARPA, $441,230, PI, 10/1/2010–9/30/2014.
- "AFOSR YIP: New Models for Protocol Security", AFOSR Young Investigator Award, $596,905. PI, 4/1/2010–3/31/2015.
- "Microsoft Research Faculty Fellowship", Microsoft, $200,000. PI, 5/1/2009-4/30/2010.
- "CAREER: Computation and Collaboration in the Era of the Internet", NSF CAREER award, $500,000. PI, 2/15/2008-1/31/2013.
- "Concurrent Security of Cryptographic Protocols: From Foundations to Practice", AFOSR, $396,000. PI, 4/1/2008-11/30/2010.
- "Composition of Cryptographic Protocols", BSF, $49,630. PI, 10/1/2007-9/30/2011.
- "Secure Identity Management Infrastructure", I3P/Dartmouth, $200,000. PI, 4/1/2007-7/31/2009.