Rafael Pass

Department of Computer Science
Cornell NYC Tech
2 W Loop Rd, NY, NY 100 44
http://www.cs.cornell.edu/~rafael

Office: (646) 971-3700
Cell: (607) 379-9993
Citizenship: Swedish
rafael@cs.cornell.edu

Research Interest

Cryptography and its interplay and Game Theory.

Current Academic Position

Full Professor in Computer Science.
5/1/2018–present *Cornell Tech & Cornell University*, NY, NY, USA.

Past Academic Positions

Affiliated Full Professor of Computer Science.
6/1/2013–6/1/2017 *Royal Institute of Technology (KTH)*, Stockholm, Sweden, USA.

Associate Professor (with tenure) in Computer Science.
7/1/2013–6/1/2018 *Cornell Tech & Cornell University*, NY, NY, USA.

Associate Professor (with tenure) in Computer Science.
7/1/2012–7/1/2013 *Cornell University*, NY, NY, USA.

Assistant Professor in Computer Science.
7/15/2006–7/1/2012 *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.

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

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. Studies at the Maitrise level (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 Full Professor at the *Ecole Normale Superieur*, Paris, 2016.
- Invited plenary talk at *Conference on Security and Cryptography for Networks*, 2016.
- Google Faculty Award, 2015.
- Wallenberg Academy Fellow (awarded by the Royal Academy of Science in Sweden), 2013.
- Fiona Ip Li and Donald Li Excellence in Teaching Award, 2012.
- Invited plenary 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. Huijia Lin, Rafael Pass, Pratik Soni. *Two-Round and Non-interactive Concurrent Non-Malleable Commitment from Time-Lock Puzzles*. Invited to SIAM Journal of Computing special issue on selected papers of FOCS 2017.
  2. N. Bitansky, S. Garg, H Lin, R. Pass and S. Telang. *Succint Randomized Encoding*. Invited to SIAM Journal of Computing special issue on selected papers of STOC 2015.
  3. P. Austrin, K. Chung, M. Mahmoody, R. Pass, K. Seth. *On the impossibility of Cryptography with Tamperable Randomness*. Invited to Algorithmica special issue on best papers from CRYPTO'14.
  4. S. Hohenberger, S. Myers, R. Pass, and A. Shelat: ANONIZE: A Large-Scale Anonymous Survey System. Invited to the IEEE Security & Privacy Magazine issue on best papers from Oakland 2014.
  5. A. Bjorndahl, J.. Halpern, and R Pass. Language-Based Games (best-papers track). Invited to the best-paper track at *IJCAI 2013* (as the best paper from *TARK 2013*).
  6. Rafael Pass, Huijia Lin, Muthuramakrishnan Venkitasubramaniam: *A Unified Framework for UC from Only OT*. Invited to Journal of Cryptology special issue on best papers from ASIACRYPT 2012.
  7. K. Chung, R. Pass, K. Seth. *Non-black-box simulation from one-way functions and applications to resettable security.* Invited to SIAM Journal of Computing special issue on selected papers of STOC 2012.
  8. R. Pass. *Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments*. Invited to Computational Complexity special issue for the ten year anniversary of TCC.
  9. R. Pass. *Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments*. Invited to Journal of Cryptology special issue on best papers from TCC'13.
  10. 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.
  11. R. Pass and M. Venkitasubramaniam. *On Constant-Round Concurrent Zero Knowledge*. Invited to Journal of Cryptology.
  12. H. Lin, R. Pass and M. Venkitasubramaniam. *Concurrent Non-malleable Commitments from One-way Functions*. Invited to Journal of Cryptology.
  13. R. Canetti, Y. Dodis, R. Pass and S. Walfish. *Universally Composable Security with Global Set-up*. Invited to Journal of Cryptology.

14. 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.
15. 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.
16. 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 5854 Networks and Markets.* Fall 2016, Fall 2017.
- *NBA 5400 Tech for Business.* Fall 2015, Fall 2016.
- *CS 5830 Cryptography.* Cornell NYC Tech, Fall 2013.
- *CS 5831 Security Protocols and Privacy.* Cornell NYC Tech, Spring 2014.
- *CS 2800 Discrete Structures.* Cornell University, Spring 2011, Spring 2012, Fall 2013.
- *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, Spring 2015, Spring 2016, Spring 2017.
- *CS 6810 Theory of Computing.* Cornell University, Spring 2009.
- *CS 7893 Cryptography Seminar.* Cornell University, every semester since Fall 2008.
- *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.

Course Books/Lecture Notes

- R. Pass and A. Shelat. *A Course in Cryptography.* Book/lecture notes for an upper-level undergraduate or graduate course in Cryptography. Available online. In revision at MIT Press; accepted for publication.
  - Used as course material at e.g. CMU, Berkeley, Georgia Tech, JHU, U Michigan, NYU, Columbia, U. Rochester, USB, Purdue, Northeastern, UVA, Oregon State, IIT.

- R. Pass. *A Course in Networks and Markets.* Book/lecture notes for a Masters-level course in Networks and Markets. Available online. Accepted for publication 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; tenured at U. Rochester)
- Huijia (Rachel) Lin (July 2011; postdoc at MIT & BU; now tenure-track faculty at University of California, Santa Barbara).
- Wei-Lung Dustin Tseng (July 2011; now at Google)
- Adam Bjorndahl (July 2014; (informally) co-advised with Joe Halpern; now tenure-track faculty at CMU)
- Edward Lui (July 2015; founder at start-up)
- Lior Seeman (July 2015, co-advised with Joseph Halpern; now at Uber Research)
- Karn Seth (June 2016, now at Google)
- Sidharth Telang (June 2016, now at Google)

Current Ph.D. Students

- Antonio Marcedone (expected graduation May 2019)
- Andrew Morgan (expected graduation May 2021)
- Naomi Ephraim (expected graduation May 2021)

Current Postdocs

- Ilan Komargodksi (Ph.D Weizmann, current, co-advised with Elaine Shi)
- Gilad Asharov (Ph.D Bar-Ilan University, Simon's Fellow, current)
- Antigoni Polychroniadou (Ph.D Aarhus University, current, co-advised with Elaine Shi)

Past Postdocs

- Mohammad Mahmoody (Ph.D Princeton, now tenure-track at University of Virginia)
- Kai-min Chung (Ph.D Harvard, Simon's Fellow, now tenure-track at Academia Sinica, Taiwan)
- Elette Boyle (previously at MIT, now tenure track at IDC Israel)

Non-Academic Work Experience

2013– *Anonize*, NY.
Co-founder. Anonize develops cryptographic systems for achieving anonymity.
Our system is the cornerstone of the anonymity solution used in the new *Brave* browser (founded by Brendan Eich, previously co-founder of Mozilla)

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

Journal papers

1. K. Chung, R. Pass, K. Seth: Non-black-box Simulation from One-way Functions and Applications to Resettable security. *SIAM Journal of Computing*, Vol 45(2), pages 415-458, 2016.

2. Ran Canetti, Huijia Lin, Rafael Pass: Adaptive Hardness and Composable Security in the Plain Model from Standard Assumptions. *SIAM Journal of Computing*, Vol 45(5), pages 1793-1834, 2016.

3. R. Pass. Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments. *Computational Complexity*, Vol 25(3), pages 607–666, 2016.

4. H. Lin and R. Pass. Constant-round Non-malleable Commitments from Any One-way Function. *Journal of the ACM*, Vol 62(1), pages 5:1-5:30, 2015.

5. J. Chen, S. Micali, R. Pass. Tight Revenue Bounds With Possibilistic Beliefs and Level-k Rationality. *Econometrica*, Volume 83, Issue 4, pages 16191639, 2015.

6. S. Hohenberger, S. Myers, R. Pass and Abhi Shelat: An Overview of ANONIZE: A Large-Scale Anonymous Survey System. *IEEE Security & Privacy Magazine*, Vol 13(2), pages 22-29, 2015.

7. J. Y. Halpern and R. Pass: Algorithmic rationality: Game theory with costly computation. *J. Economic Theory*, Vol 156, pages 246-268, 2015.

8. R. Pass, W. Dustin Tseng and M. Venkitasubramaniam: Concurrent Zero Knowledge, Revisited. *Journal of Cryptology*, Vol 27(1), pages 45-66, 2014.

9. J. Halpern and R. Pass. *Conservative Belief and Rationality. Games and Economic Behavior*, Vol 80, pages 186-192, 2013.

10. K. Chung and R. Pass. Parallel Repetition Theorems for Interactive Arguments. *SIGACT News*. Vol 44(1), pages 50–69, 2013.

11. R. Pass, A. Rosen and W. Tseng. Public-coin Parallel Zero Knowledge. *Journal of Cryptology*, Vol 26(1), pages 1–10, 2013.

12. R. Pass, M. Venkitasubramaniam. A Parallel Repetition Theorem for Constant-Round Arthur-Merlin Proofs. *ACM Transactions on Computation Theory*. Vol 4(4) 10, 2012.

13. T. Roeder, R. Pass and F. Schneider. Multi-Verifier Signatures. *Journal of Cryptology*, Vol. 25(2), pages 310–348, 2012.

14. R. Pass, W. Tseng and D. Wikstrom. On the Composition of Public-coin Zero Knowledge. *SIAM Journal of Computing*, Vol 40(6), pages 15290-1553, 2011.

15. J. Halpern and R. Pass. Iterated Regret Minimization: A New Solution Concept. *Games and Economic Behavior*, Vol 74(1), pages 184–207, 2012.

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

17. B. Barak, R. Canetti, Y. Lindell, R. Pass and T. Rabin. Secure Computation without Authentication. *Journal of Cryptology*, Vol 24(4): 720–760, 2011.

18. R. Pass and A. Rosen. Concurrent Non-malleable Commitments. *SIAM Journal of Computing* 37(6), pages 1891–1925, 2008.

19. R. Pass and A. Rosen. New and Improved Constructions of Non-malleable Cryptographic Protocols. *SIAM Journal of Computing* 38(2), pages 702-752, 2008.

Conference papers

1. Huijia Lin, Rafael Pass, Pratik Soni. Two-Round and Non-interactive Concurrent Non-Malleable Commitment from Time-Lock Puzzles. To appear in *FOCS 2017*.

2. Rafael Pass and Elaine Shi. Hybrid Consensus: Efficient Consensus in the Permissionless Model. To appear in *DISC 2017*.

3. Rafael Pass and Elaine Shi. Sleepy Consensus. To appear in *AsiaCrypt 2017*.

4. Joseph Halpern and Rafael Pass. A knowledge-based analysis of the blockchain. In *TARK 2017*, 2017.

5. Rafael Pass and Elaine Shi. FruitChains: A Fair Blockchain. In *PODC 2017*, pages 315-324, 2017

6. Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the Blockchain Protocol in Asynchronous Networks. In *EuroCrypt17*, pages 260–289, 2017.

7. Rafael Pass, Elaine Shi and Florian Tramer. Formal Abstractions for Attested Execution Secure Processors. In *EuroCrypt17*, pages 643–673, 2017.

8. Antonio Marcedone, Rafael Pass and Abhi Shelat. Bounded KDM Security from iO and OWF. In *Security and Cryptography for Networks (SCN)*, pages 571-586, 2016.

9. Joseph Y. Halpern, Rafael Pass and Lior Seeman. Computational Extensive-Form Games. In *Conference on Economics and Computation (EC)*, pages 681-698, 2016.

10. J. Halpern and R. Pass. Sequential Equilibrium in Games of Imperfect Recall. In *Knowledge Representation (KR)*, pages 278-287, 2016.

11. H. Lin, R. Pass, K. Seth and S. Telang. Indistinguishability Obfuscation with Non-trivial Efficiency. In *Public Key Cryptography (PKC)*, pages 447-462, 2016.

12. R. Pass and A. Shelat. Impossibility of VBB Obfuscation with Ideal Constant-Degree Graded Encodings. In *Theory of Cryptography Conference (TCC 2016-A)*, pages 3-17, 2016.

13. M. Mahmoody, A. Mohammed, S. Nematihaji, R. Pass and A. Shelat. Lower Bounds on Assumptions Behind Indistinguishability Obfuscation. In *Theory of Cryptography Conference (TCC 2016-A)*, pages 49-66, 2016.

14. H. Lin, R. Pass, K. Seth and S. Telang. Output-Compressing Randomized Encodings and Applications. In *Theory of Cryptography Conference (TCC 2016-A)*, pages 96-124, 2016.

15. E. Boyle, K, Chung and R. Pass Oblivious Parallel RAM and Applications. In *Theory of Cryptography Conference (TCC 2016-A)*, pages 175-204, 2016.

16. S. Leung, E. Lui and R. Pass: Voting with Coarse Beliefs. In *Innovations in Theoretical Computer Science (ITCS 2015)*, page 61, 2015.

17. J. Chen, S. Micali, R. Pass: Better Outcomes from More Rationality. In *Innovations in Theoretical Computer Science (ITCS 2015)*, page 325, 2015

18. N. Bitansky, S. Garg, H. Lin, R. Pass and S. Telang: Succinct Randomized Encodings and their Applications. In *STOC 2015*, pages 439-448, 2015.

19. K. Chung, E. Lui and R. Pass. From Weak to Strong Zero-Knowledge and Applications. In *Theory of Cryptography Conference (TCC 2015)*, pages 66-92, 2015.

20. K. Chung and R. Pass. Tight Parallel Repetition Theorems for Public-Coin Arguments Using KL-Divergence. In *Theory of Cryptography Conference (TCC 2015)*, pages 229-246, 2015.

21. V. Goyal, H. Lin, O. Pandey, R. Pass and A. Sahai. Round-Efficient Concurrently Composable Secure Computation via a Robust Extraction Lemma. In *Theory of Cryptography Conference (TCC 2015)*, pages 260-289, 2015.

22. E. Lui, R Pass. Outlier Privacy. In *Theory of Cryptography Conference (TCC 2015)*, pages 277-305, 2015.

23. Kai-Min Chung, Z. Liu, and R. Pass. Statistically-secure ORAM with $\tilde{O}(\log^2 n)$ Overhead. In *ASIACRYPT 2014*, pages 62-81, 2014.

24. P. Austrin, K. Chung, M. Mahmoody, R. Pass, and K. Seth. On the Impossibility of Cryptography with Tamperable Randomness. In *CRYPTO 2014*, pages 462-479, 2014.

25. R. Pass, K. Seth and S. Telang. Indistinguishability Obfuscation from Semantically-Secure Multilinear Encodings. In *CRYPTO 2014*, pages 500-517, 2014.

26. I. Komargodski, T. Moran, M. Naor, R. Pass, A. Rosen, E. Yogev. One-Way Functions and (Im)Perfect Obfuscation. In *FOCS 2014*, pages 374-383, 2014.

27. A. Bjorndahl, J. Halpern and R. Pass: Axiomatizing Rationality. In *KR 2014*.

28. R. Pass and K. Seth. On the Impossibility of Black-Box Transformations in Mechanism Design. In *SAGT 2014*, pages 279-290, 2014.

29. S. Hohenberger, S. Myers, R. Pass, and A. Shelat: ANONIZE: A Large-Scale Anonymous Survey System. In *IEEE Symposium on Security and Privacy (Oakland 2014)*, pages 375-389, 2014.

30. J. Halpern, R. Pass and L. Seeman. The truth behind the myth of the folk theorem. In *Innovations in Theoretical Computer Science (ITCS 2014)*, pages 543-554, 2014

31. E. Boyle, K. Chung and R. Pass. On Extractability Obfuscation. In *Proceedings of the 11th Theory of Cryptography Conference (TCC 2014)*, pages 52-73, 2013.

32. K. Chung, R. Ostrovsky, R. Pass, Muthuramakrishnan Venkitasubramaniam and Ivan Visconti. 4-Round Resettably-Sound Zero Knowledge. In *Proceedings of the 11th Theory of Cryptography Conference (TCC 2014)*, pages 192-216, 2014.

33. K. Chung, H. Lin and R. Pass. Constant-Round Concurrent Zero Knowledge From P-Certificates. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2013)*, pages 50-59, 2013.

34. K. Chung, R. Pass and S. Telang. Knowledge-Preserving Interactive Coding. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2013)*, pages 449-458, 2013.

35. R. Canetti, H. Lin and R. Pass. From Unprovable Security to Enviromental Friendliness. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2013)*, pages, 70-79, 2013.

36. K. Chung, R. Ostrovsky, R. Pass and I. Visconti. Simultaneous Resettability from One-way Functions. In *Proceedings of the 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2013)*, pages 60-69, 2013.

37. A. Bjorndahl, J.. Halpern, and R Pass. Language-Based Games (best-papers track). In *Proceeding of the 24st International Joint Conference on Artificial Intelligence (IJCAI 2013)*, 2013.

38. J. Halpern and R. Pass. Sequential Equilibrium in Computational Games. In *Proceeding of the 24st International Joint Conference on Artificial Intelligence (IJCAI 2013)*, 2013.

39. K. Chung, E. Lui and R. Pass. Can theories be tested?: a cryptographic treatment of forecast testing. In *Innovations in Theoretical Computer Science (ITCS 2013)*, pages 47–56, 2013

40. P. Austrin, J. Håstad and R. Pass. On the power of many one-bit provers. In *Innovations in Theoretical Computer Science (ITCS 2013)*, pages 215–220, 2013

41. K. Chung, H. Lin, M. Mahmoody, R. Pass. On the power of nonuniformity in proofs of security. In *Innovations in Theoretical Computer Science (ITCS 2013)*, pages 389–400, 2013

42. J. Halpern and R. Pass. Game-Theory with Translucent Players. In *Proceedings of the 13th Conference on Theoretical Aspects of Rationality and Knowledge (TARK 20113*, 2013.

43. A. Bjorndahl, J. Halpern and R. Pass. Language-Based Games. In *Proceedings of the 13th Conference on Theoretical Aspects of Rationality and Knowledge (TARK 20113*, 2013.

44. K. Chung, R. Pass, K. Seth: Non-black-box Simulation from One-way Functions and Applications to Resettable security. In *Proceedings of the 41th Annual Symposium on Theory of Computing (STOC 2013)*, pages 231–240, 2013. Invited to *SIAM Journal of Computing* special-issue on selected papers from STOC 2013.

45. R. Pass. Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments. In *Proceedings of the 10th Theory of Cryptography Conference (TCC 2013)*, pages 334–354, 2013. Invited to *Computational Complexity* special issue celebrating the 10 year anniversary of TCC.

46. E. Birrell, K. Chung, R. Pass, S. Telang. Randomness-Dependent Message Security. In *Proceedings of the 10th Theory of Cryptography Conference (TCC 2013)*, pages 700–720, 2013.

47. J. Halpern, R. Pass, L. Seeman. I'm Doing as Well as I Can: Modeling People as Rational Finite Automata. In *Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence (AAAI 2013)*, 2012.

48. H. Lin, R. Pass and M. Venkitasubramaniam. A Unified Framework for UC from Only OT. *Advances in Cryptology (ASIACRYPT 2012)*, Springer LNCS, pages 699–717, 2012. Invited to *Journal of Cryptology* special issue on selected papers from ASIACRYPT 2012.

49. Huijia Lin, Rafael Pass: Black-Box Constructions of Composable Protocols without Set-Up. *Advances in Cryptology (CRYPTO 2012)*, Springer LNCS, pages 461–478, 2012.

50. J. Gehrke, M. Hay, E. Lui and R. Pass. Crowd-Blending Privacy. *Advances in Cryptology (CRYPTO 2012)*, Springer LNCS, pages 479–496, 2012.

51. M. Mahmoody and R. Pass. The Curious Case of Non-Interactive Commitments - On the Power of Black-Box vs. Non-Black-Box Use of Primitives. *Advances in Cryptology (CRYPTO 2012)*, Springer LNCS, pages 701–718, 2012.

52. K. Chung, R. Pass and W. Tseng. The Knowledge Tightness of Parallel Zero-Knowledge. In *Proceedings of the 8th Theory of Cryptography Conference (TCC 2012)*, pages 512–529, 2012.

53. K. Chung and R. Pass. The Randomness Complexity of Parallel Repetition. In *Proceedings of the 52th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2011)*, pageas 658–667, 2011.

54. 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.

55. 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.

56. 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.

57. 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.

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

59. 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.

60. 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.

61. 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.

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

63. 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.

64. 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.

65. 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.

66. 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.

67. 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.

68. 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.

69. 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.

70. 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.

71. 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.

72. 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.

73. 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.

74. 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.

75. 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.

76. 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.

77. 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.

78. 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.

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

80. 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.

81. 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.

82. 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.

83. 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.

84. 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.

85. 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.

86. 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.

87. 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.

88. 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.

89. 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. of Computational Complexity 2006.

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

91. 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.

92. 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.

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

94. 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.

95. 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.

96. 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.

97. 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.

98. 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.

99. 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.

100. 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.

Selected Talks

- DISC Blockchain Workshop, "Sleepy Consensus", 2017.
- DISC Blockchain Workshop, "Thunderella: Blockchains with Optimistic Instant Confirmation", 2017.
- DISC, "Hybrid Consensus", 2017.
- Stanford, "Rethinking Large Scale Consensus", 2017.
- Berkeley Blockchain Workshop, "Thunderella: Blockchains with Optimistic Instant Confirmation", 2017.
- PODC, "FruitChains: A Fair Blockchain", 2017.
- Technion Summer School, "Zero-Knowledge and Anonize", 2017.
- Technion Summer School, "Nakamoto Consensus", 2017.
- Technion Summer School, "Thunderella: Blockchains with Optimistic Instant Confirmation", 2017.
- KTH, "Rethinking Large Scale Consensus", 2017.
- EuroCrypt, "Analysis of the Blockchain Protocol in Asynchronous Networks", 2017.
- IC3 workshop, "Rethinking Large Scale Consensus", 2017.

- IC3 workshop, "Incentive-Compatible Blockchains", 2017.
- MIT Seminar, "Rethinking Large Scale Consensus", 2016.
- Invited talk at Conference on Security and Cryptography for Networks (SCN), "Cryptographic Rationality", 2016.
- Oberwolfach MFO, "Rethinking Large Scale Consensus", 2016.
- Oberwolfach MFO, "Foundations of Blockchains", 2016.
- NYC Crypto day, Columbia, "Rethinking Large Scale Consensus", 2016.
- Paris Crypto Day "Design and Analysis of Blockchains", Ecole Normale Superieure, Paris, 2016.
- Ecole Normale Superieure, Paris, "Foundations of Program Obfuscation", 2016.
- MIT Seminar, "Design and Analysis of Blockchains", 2016.
- Simon's workshop, "Analysis of the Blockchain Protocol in Asynchronous Networks", 2016.
- IC3 workshop, "Design and Analysis of Blockchains", 2016.
- Theory and Practice of Secure Computation Workshop, Aarhus, "Design and Analysis of Blockchains", 2016.
- AFOSR briefing, "Recent progress on the Foundation of Program Obfuscation", 2016.
- PKC 2016, Taiwan. "Obfuscation with Non-trivial Efficiency", 2016.
- TCC 2016, Tel-Aviv, "On the Impossibility of VBB Obfuscation with Ideal Constant-Degree Graded Encodings.", 2016.
- Cryptography in the desert workshop, Negev, Israel, "Indistinguishability Obfuscation v.s. Randomzed Encodings", 2016.
- 22nd International Symposium on Mathematical Programming, "Reasoning Cryptographically About Knowledge", 2015.
- TCC 2015, Warsaw, "From Weak to Strong Zero-Knowledge", 2015
- Greater Tel-Aviv Area Crypto Day (Bar-Ilan Uni), "Constant-round Concurrent Zero-knowledge from Indistinguishability Obfuscation", 2015
- DARPA Briefing, Washington DC, 2015, "Large-Scale Multi-party Computation"
- U. of Indiana CS Colloquium, 2015. "Reasoning Cryptographically about Knowledge".
- Cornell (CCTEC event): "Anonize: A Large-Scale Anonymous Survey System", 2014.

- Cornell Tech (Future of Money Workshop), "Anonize: A Large-Scale Anonymous Survey System",2014.
- KTH, 2014, "Obfuscation From Semantically Secure Encryption".
- Workshop on Secure Multiparty Computation, Aarhus, "Obfuscation From Semantically Secure Encryption".
- NYU Security Seminar, 2014, "Obfuscation From Semantically Secure Encryption"
- BU Security Colloquium, 2014, "On the Impossibility of Cryptography With Tamperable Randomness"
- MIT TOC Colloquium, Washington DC, 2014, "Obfuscation From Semantically Secure Encryption"
- Visions in Cryptography, Weizmann, 2014, "On Cryptographic Assumptions"
- DARPA Briefing, Washington DC, 2013, "Obfuscation From Semantically Secure Encryption"
- Faces of Modern Cryptography, 2013, "On the impossibility of Tamper-Resilient Cryptography".
- Rutgers CS Colloquium (inaugural talk), 2013. "Reasoning Cryptographically about Knowledge".
- Invited speaker at the 2013 Turing Award Fest for Goldwasser-Micali, "Reasoning Cryptographically about Knowledge".
- Trends i Cryptography Workshop, NYC, 2013, "Interactive Coding, Revisited".
- AFOSR presentation, "Security-preserving Interactive Coding".
- FOCS 2013, "Simultanous Resettability from One-way Functions".
- Viruses, Tampering and Leakage Workshop, Warshaw, Poland, 2013, "On the impossibility of Tamper-Resilient Cryptography".
- TCC 2013, "Unprovable Security of Perfect NIZK and Non-interactive Non-malleable Commitments".
- TARK 2013, "Game Theory with Translucent Players".
- DARPA Briefing, Charlottesville, 2013, "On the impossibility of Tamper-Resilient Cryptography".
- TRUST meeting, 2013, "On the impossibility of Tamper-Resilient Cryptography".

- World Congress of Game Theory, Northwestern University, Istanbul, 2012, "Game-Theory with Costly Computation".
- World Congress of Game Theory, Northwestern University, Istanbul, 2012, "An Epistemic Approach to Mechanism Design".
- World Congress of Game Theory, Northwestern University, Istanbul, 2012, "That's All I know: A Logical Characterization of Iterated Admissability and Extensive-Form Rationalizability".
- AFOSR presentation, 2012, "On the impossibility of Tamper-Resilient Cryptography".
- Theory and Implementation of Multiparty Computation Workshop, Aarhus, 2012, "Constant-round Non-malleability and its Application to Secure Computation".
- Northwestern University, 2012, "An Epistemic Approach to Mechanism Design".
- DARPA Briefing, Ft Lauderdale, 2012, "On the (Im)possibility of Tamper-resilient Cryptography".
- DARPA Briefing, UVA, 2012, "Constant-round Non-malleability and its Application to Secure Computation".
- KTH, 2012, "An Epistemic Approach to Mechanism Design".
- Charles River Cryptography Day, 2012, "An Epistemic Approach to Mechanism Design".
- AFOSR presentation 2011, "Constant-round Non-malleability from Any One-way Function".
- IBM Hawthorne, 2011, "Non-malleability and Concurrency".
- U Rochester, "Constant-round Non-malleable Commitments from Any One-way Function", 2011.
- MIT, 2011, "Limits of Provable Security from Standard Assumptions".
- 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:

- 15th Theory of Cryptography Conference (TCC'17).
- 37th Annual International Cryptology Conference (CRYPTO'17).
- 14th Theory of Cryptography Conference (TCC'16).
- 10th Annual Conference on Security and Cryptography for Networks (SCN'16).
- 6th Innovations in Theoretical Computer Science Conference (ITCS'16).
- 57th Annual IEEE Symposium on Foundations of Computer Science (FOCS'15).
- 5th Innovations in Theoretical Computer Science Conference (ITCS'15).
- 34th Annual International Cryptology Conference (CRYPTO'14).
- 33th Annual International Cryptology Conference (EUROCRYPT'14).
- 26th IEEE Computer Security Foundations Symposium (CSF'13)
- 54th Annual IEEE Symposium on Foundations of Computer Science (FOCS'12).

- 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).

Journals:

- ACM Transactions of Comptuation Theory (TOCT), Associate Editor since 2013.
- Journal of Computer and System Sciences, Associate Editor since 2014.
- Journal Refereeing: Journal of the ACM, SIAM Journal of Computing, Information and Computation, Journal of Cryptology, Games and Economic Behavior, International Journal of Game Theory

Grants

- "SATC: CORE: LARGE: VIADUCT: A Framework for Automatically Synthesizing Cryptographic Protocols", $2,499,998, co-PI (joint with Andrew Myers (PI), Elaine Shi and Greg Morrisset), 6/1/2017—5/31/2021
- "RI: Medium: Computation, Language, and Games", $1,176,680, co-PI (joint with Joseph Halpern), 6/15/2017–5/31/2017.
- "AFOSR: Foundations of Program Obfuscation; add-on", $150,000, PI, 1/1/17—1/1/19.
- "TWC: LARGE: COLLABORATIVE: The Science and Applications of Crypto-Currency", $1,268,740, co-PI (joint with Elaine Shi), 12/6/2015—1/6/2018.
- "Google Faculty Award", Google Inc, $58,000, PI, 2015.

- "AFOSR: Foundations of Program Obfuscation", $390,000, PI, 1/1/16—
- "ICES: Large: Computation, Language, and Awareness in Games", $978,771.00, co-PI (joint with Joseph Halpern), 7/18/12—5/1/17.
- "AF: Small: New Barriers in Cryptography", $500,000, PI, 8/16/12—8/16/15.
- "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, $744,071. PI, 2/15/2008-1/31/2015.
- "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.