Rafael Pass

Department of Computer Science
Cornell NYC Tech
2 W Loop Rd, NY, NY 100 44

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

Research Interest

Cryptography and its interplay with Computational Complexity and Game Theory.

Current Academic Position

Full Professor in Computer Science.

5/1/2018–present	*Cornell Tech & Cornell University*, NY, NY, USA.
	One of the founding faculty members (3rd hire, 2013) at Cornell Tech.
1/1/2025–present	Full Professor, *Jacobs Technion-Cornell Institute*
9/1/2024–present	Visiting Full Professor, *Technion*, Israel.

Full Professor in Computer Science (Endowed Chair), *On leave.*

2023–present	*Tel-Aviv University*, Tel-Aviv, Israel.
Director,	Checkpoint Institute for Information Security.
Incumbment,	Chair of Cryptography and Information Security.

Past Academic Position

Affiliated Full Professor in Computer Science.

6/1/2013–6/1/2017	*Royal Institute of Technology (KTH)*, Stockholm, Sweden, USA.

Associate Professor (with tenure) in Computer Science.

7/1/2012–6/1/2018	*Cornell Tech & 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, Hebrew:** advanced,
- **Spanish, German:** intermediate.

Awards and Honors

- ERC Advanced Grant, 2024
- CACM Research Highlights, 2023.
- Fellow of the IACR, 2023.
- Fellow of the ACM, 2022.
- Winner of the 9th NSA Best Scientific Cybersecurity Paper Competition, 2022.
- Distinguished Scholar, Institute for Advanced Study (IAS), Tel-Aviv University, 2021
- The Best Paper Award at the 41st Annual International Cryptology Conference (CRYPTO), 2021.
- Invited Keynote at ITC 2022.
- The Cornell Tech Faculty Teaching Award, 2021.
- Richard Karp Distinguished Lectureship at Berkeley (Simons Institute), 2020.
- JP Morgan Faculty Award, 2020.
- 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. Noam Mazor, Rafael Pass: *Counting Unpredictable Bits: A Simple PRG from One-Way Functions*. Invited to Journal of Cryptology special issue on best papers from TCC'23.
  2. Yanyi Liu, Rafael Pass: *On the Possibility of Basing Cryptography on $EXP \neq BPP$.* Invited to Journal of Cryptography special issue on selected papers from CRYPTO'21. Invited to Communications of the ACM (CACM) as a featured research highlight.
  3. 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.
  4. 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.
  5. 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.
  6. 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.
  7. 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*).

8. 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.
9. 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.
10. 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.
11. 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.
12. 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.
13. R. Pass and M. Venkitasubramaniam. *On Constant-Round Concurrent Zero Knowledge*. Invited to Journal of Cryptology.
14. H. Lin, R. Pass and M. Venkitasubramaniam. *Concurrent Non-malleable Commitments from One-way Functions*. Invited to Journal of Cryptology.
15. R. Canetti, Y. Dodis, R. Pass and S. Walfish. *Universally Composable Security with Global Set-up*. Invited to Journal of Cryptology.
16. 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.
17. 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.
18. R. Pass and A. Rosen, *Concurrent Non-Malleable Commitments.* Invited to SIAM Journal of Computing special issue on selected papers of STOC 2005.

Course Books and Students

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. Published by MIT Press, 2019. Online version published in 2020.
- 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; now tenured at University of Washington).
- 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)
- Antonio Marcedone (May 2019, now at Cryptography Lead Zoom)
- Andrew Morgan (January 2022)
- Naomi Ephraim (May 2022, now tenure-track at Drexel University)
- Cody Frietag (May 2024, now postdoc at BU and NEU)

Current Ph.D. Students

- Yanyi Liu (expected graduation May 2024)
- Benjamin Chan (expected graduation May 2024)
- Eden Aldema-Tshuva (joint with Rotem Oshman)
- Tomer Solomon (joint with Zvika Brakerski)

Current Postdocs

- Noam Mazor
- Gilad Stern

Past Postdocs

- Roman Gay (now at IBM Research Zurich)
- Ilan Komargodski (Ph.D Weizmann, current, co-advised with Elaine Shi, now tenure-track at Hebrew University)
- Gilad Asharov (Ph.D Bar-Ilan University, Simon's Fellow, now tenure-track at Bar-Ilan University) current)
- Antigoni Polychroniadou (Ph.D Aarhus University, current, co-advised with Elaine Shi, now at Cryptography Lead at JP Morgan AI)
- Elette Boyle (previously at MIT, now tenured at Reichman University and Senior Scientiest at NTT Research)
- Daniel Reichman (Ph.D Weizmann, co-advised with Joe Halpern, now tenure-track at WPI)
- Kai-min Chung (Ph.D Harvard, Simon's Fellow, now tenured at Academia Sinica, Taiwan)
- Mohammad Mahmoody (Ph.D Princeton, now tenured at University of Virginia)

Publications

Journal papers

1. Yanyi Liu, Rafael Pass: Toward Basing Cryptography on the Hardness of EXP. *Communations of the ACM (CACM* 66(5): 91-99 (2023).

2. Ittai Abraham, T.-H. Hubert Chan, Danny Dolev, Kartik Nayak, Rafael Pass, Ling Ren, Elaine Shi: Communication complexity of byzantine agreement, revisited. *Distributed Computing* 36(1): 3-28 (2023)

3. Naomi Ephraim, Cody Freitag, Ilan Komargodski, Rafael Pass: SPARKs: Succinct Parallelizable Arguments of Knowledge. *Journal of the ACM (JACM)* 69(5): 31:1-31:88 (2022)

4. Gilad Asharov, T.-H. Hubert Chan, Kartik Nayak, Rafael Pass, Ling Ren, Elaine Shi: Locality-Preserving Oblivious RAM. *Journal of Cryptology* 35(2): 6 (2022)

5. Gilad Asharov, Ilan Komargodski, Rafael Pass, Naomi Sirkin: On the Complexity of Compressing Obfuscation. *Journal of Cryptology* 35(3): 21 (2022)

6. Ilan Komargodski, Tal Moran, Moni Naor, Rafael Pass, Alon Rosen, Eylon Yogev: One-Way Functions and (Im)perfect Obfuscation. *SIAM Journal of Computing* 51(6): 1769-1795 (2022)

7. Rafael Pass, Muthuramakrishnan Venkitasubramaniam: Average-case Complexity Through the Lens of Interactive Puzzles. *SIGACT News*, Vol 52(1), pages 47-69, 2021.

8. Huijia Lin, Rafael Pass and Pratik Soni: Two-Round and Non-Interactive Concurrent Non-Malleable Commitments from Time-Lock Puzzles. In *SIAM Journal of Computing*, 2020.

9. Adam Bjorndahl, Joseph Y. Halpern and Rafael Pass: Bayesian games with intentions. *Games and Economic Behavior*, Vol 123, pages 54-67, 2020.

10. Joseph Y. Halpern and Rafael Pass. Sequential Equilibrium in Computational Games. *ACM Trans. Economics and Comput*, Vol. 7(2), pages 9:1-9:19, 2019.

11. Joseph Y. Halpern, Rafael Pass and Lior Seeman. The truth behind the myth of the Folk theorem. *Games and Economic Behavaior.* Vol 117, pages 479-498, 2019.

12. Rafael Pass. A tutorial on concurrent zero-knowledge. *ACM Providing Sound Foundations for Cryptography.* Invited chapter in ACM Turing Award book for Shafi Goldwasser and Silvio Micali.

13. Joseph Y. Halpern and Rafael Pass. Game theory with translucent players. *Int. J. Game Theory.* Vol 47(3), pages 949-976, 2018.

14. Nir Bitansky, Ran Canetti, Sanjam Garg, Justin Holmgren, Abhishek Jain, Huijia Lin, Rafael Pass, Sidharth Telang and Vinod Vaikuntanathan: Indistinguishability Obfuscation for RAM Programs and Succinct Randomized Encodings. *SIAM J. Comput.* Vol 47(3), pages 1123-1210, 2018.

15. Per Austrin, Kai-Min Chung, Mohammad Mahmoody, Rafael Pass, Karn Seth: On the Impossibility of Cryptography with Tamperable Randomness. *Algorithmica.* Vol 79(4). 2017

16. Adam Bjorndahl, Joseph Y. Halpern, Rafael Pass: Reasoning about rationality. *Games and Economic Behavior.* 2017

17. 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.

18. 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.

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

20. 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.

21. J. Chen, S. Micali, R. Pass. Tight Revenue Bounds With Possibilistic Beliefs and Level-k Rationality. *Econometrica*, Volume 83, Issue 4, pages 1619–1639, 2015.

22. 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.

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

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

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

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

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

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

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

30. 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.

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

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

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

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

35. 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. Noam Mazor, Rafael Pass: The Non-Uniform Perebor Conjecture for Time-Bounded Kolmogorov Complexity Is False. In *ITCS 2024*: 80:1-80:20

2. Yanyi Liu, Rafael Pass: Leakage-Resilient Hardness vs Randomness. In *CCC 2023*: 32:1-32:20

3. Yanyi Liu, Rafael Pass: One-Way Functions and the Hardness of (Probabilistic) Time-Bounded Kolmogorov Complexity w.r.t. Samplable Distributions. In *CRYPTO* 2023: 645-673

4. Marshall Ball, Yanyi Liu, Noam Mazor, Rafael Pass: Kolmogorov Comes to Cryptomania: On Interactive Kolmogorov Complexity and Key-Agreement. In *FOCS 2023*: 458-483

5. Noam Mazor, Rafael Pass: Counting Unpredictable Bits: A Simple PRG from One-Way Functions. In *TCC 2023*: 191-218

6. Yanyi Liu, Rafael Pass: On One-Way Functions and Sparse Languages. In *TCC 2023*: 219-237

7. Benjamin Y. Chan, Rafael Pass: Simplex Consensus: A Simple and Fast Consensus Protocol. In *TCC 2023*: 452-479

8. Andrew Morgan, Rafael Pass: Concurrently Composable Non-interactive Secure Computation. In *ASIACRYPT 2022*: 526-555.

9. Yanyi Liu, Rafael Pass: Characterizing Derandomization Through Hardness of Levin-Kolmogorov Complexity. In *CCC 2022*: 35:1-35:17.

10. Yanyi Liu, Rafael Pass: On One-Way Functions from NP-Complete Problems. In *CCC 2022*: 36:1-36:24.

11. Omer Paneth, Rafael Pass: Incrementally Verifiable Computation via Rate-1 Batch Arguments. In *FOCS 2022*: 1045-1056.

12. Benjamin Y. Chan, Cody Freitag, Rafael Pass: Universal Reductions: Reductions Relative to Stateful Oracles. In *TCC 2022*: 151-180

13. Cody Freitag, Rafael Pass, Naomi Sirkin: Parallelizable Delegation from LWE. In *TCC 2022*: 623-652

14. Yanyi Liu, Rafael Pass On One-Way Functions from NP-Complete Problems. In *CCC 2022*, pages 36:1-36:24.

15. Yanyi Liu, Rafael Pass: On the Possibility of Basing Cryptography on $EXP \neq BPP$. In *CRYPTO 2021*. Winner of the best paper award.

16. Dana Dachman-Soled, Ilan Komargodski, Rafael Pass: Non-Malleable Codes for Bounded Polynomial Depth Tampering. In *CRYPTO 2021*.

17. Romain Gay, Rafael Pass: Indistinguishability Obfuscation from Circular Security. In *STOC 2021*.

18. Yanyi Liu, Rafael Pass: Cryptography from Sublinear-Time Average-Case Hardness of Time-Bounded Kolmogorov Complexity. In *STOC 2021*.

19. Yanyi Liu and Rafael Pass. On One-way Functions and Kolmogorov Complexity. In *FOCS 2020*.

20. Rafael Pass and Muthuramakrishnan Venkitasubramaniam. Is it Easier to Prove Theorems that are Guaranteed to be True? In *FOCS 2020*.

21. Andrew Morgan, Rafael Pass and Antigoni Polychroniadou. Succinct Non-interactive Secure Computation. In *EUROCRYPT 2020*, pages 216-245.

22. Naomi Ephraim, Cody Freitag. Ilan Komargodski and Rafael Pass. Continuous Verifiable Delay Functions. In *EUROCRYPT 2020*, pages 125-154.

23. Naomi Ephraim, Cody Freitag. Ilan Komargodski and Rafael Pass. SPARKs: Succinct Parallelizable Arguments of Knowledge. In *EUROCRYPT 2020*, pages 707-737.

24. Carmit Hazay, Rafael Pass and Muthu Venkitasubramaniam. Which Languages Have 4-Round Fully Black-Box Zero-Knowledge Arguments from One-Way Functions? In *EUROCRYPT 2020*, pages 599-619.

25. Andrew Morgan, Rafael Pass, Elaine Shi: On the Adaptive Security of MACs and PRFs. In *ASIACRYPT 2020*, pages 724-753.

26. T.-H. Hubert Chan, Rafael Pass and Elaine Shi. Sublinear-Round Byzantine Agreement Under Corrupt Majority. In *Public Key Cryptography (PKC) 2020*.

27. Cody Freitag, Ilan Komargodski, Rafael Pass: Impossibility of Strong KDM Security with Auxiliary Input. In *SCN 2020*, pages 512-524.

28. Rafael Pass: Unprovability of Leakage-Resilient Cryptography Beyond the Information-Theoretic Limit. In *SCN 2020*, pages 621-642.

29. Gilad Asharov, T.-H. Hubert Chan, Kartik Nayak, Rafael Pass, Ling Ren, Elaine Shi: Bucket Oblivious Sort: An Extremely Simple Oblivious Sort. In *SOSA@SODA 2020*, pages 8-14.

30. Hubert Chen, Rafael Pass and Elaine Shi. Sublinear-Round Byzantine Agreement under Corrupt Majority. In *PKC 2019*

31. Andrew Morgan and Rafael Pass. Paradoxes in Fair Computer-Aided Decision Making. In *AAAI AIES 2019*, pages 85-90

32. Cody Freitag, Ilan Komargodski and Rafael Pass. Non-Uniformly Sound Certificates with Applications to Concurrent Zero-Knowledge. In *CRYPTO 2019*, pages 98-127.

33. Yue Guo, Rafael Pass and Elaine Shi. Synchronous, with a Chance of Partition Tolerance. In *CRYPTO 2019*, pages 499-529.

34. Gilad Asharov, T.-H. Hubert Chan, Kartik Nayak, Rafael Pass, Ling Ren and Elaine Shi. Locality-Preserving Oblivious RAM. In *EUROCRYPT 2019*, pages 214-243.

35. T.-H. Hubert Chan, Rafael Pass and Elaine Shi. Consensus Through Herding. In *EUROCRYPT 2019*, pages 720-749.

36. Phil Daian, Rafael Pass and Elaine Shi: Snow White. Robustly Reconfigurable Consensus and Applications to Provably Secure Proof of Stake. In *Financial Cryptography 2019*, pages 23-41.

37. Antonio Marcedone, Rafael Pass and Abhi Shelat. Minimizing Trust in Hardware Wallets with Two Factor Signatures. In *Financial Cryptography 2019*, pages 407-425.

38. Ittai Abraham, T.-H. Hubert Chan, Danny Dolev, Kartik Nayak, Rafael Pass, Ling Ren and Elaine Shi: Communication Complexity of Byzantine Agreement, Revisited. In *PODC 2019*, pages 317-326.

39. Joseph Y. Halpern Rafael Pass and Daniel Reichman. On the Existence of Nash Equilibrium in Games with Resource-Bounded Players. In *SAGT 2019*, pages 139-152.

40. Liang Wang, Gilad Asharov, Rafael Pass, Thomas Ristenpart and Abhi Shelat. Blind Certificate Authorities. In *IEEE Symposium on Security and Privacy (Oakland) 2019*, pages 1015-1032.

41. Joseph Y. Halpern and Rafael Pass. A Conceptually Well-Founded Characterization of Iterated Admissibility Using an "All I Know" Operator. In *TARK 2019*, pages 221-232.

42. Gilad Asharov, Naomi Ephraim, Ilan Komargodski and Rafael Pass. On the Complexity of Compressing Obfuscation. In *CRYPTO 2018*, pages 753-783.

43. Rafael Pass and Elaine Shi: Thunderella: Blockchains with Optimistic Instant Confirmation. In *EUROCRYPT 2018*, pages 3-33.

44. Andrew Morgan, Rafael Pass: On the Security Loss of Unique Signatures. In *TCC 2018*, pages 507-536.

45. Kai-Min Chung, Yue Guo, Wei-Kai Lin, Rafael Pass and Elaine Shi. Game Theoretic Notions of Fairness in Multi-party Coin Toss. In *TCC 2018*, pages 563-596.

46. Elette Boyle, Yuval Ishai, Rafael Pass and Mary Wootters. Can We Access a Database Both Locally and Privately? In *TCC 2017*.

47. Ben Fisch, Rafael Pass, Abhi Shelat, Socially Optimal Mining Pools. In *WINE 2017*

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

49. Rafael Pass and Elaine Shi. Hybrid Consensus: Efficient Consensus in the Permissionless Model. In *DISC 2017*.

50. Rafael Pass and Elaine Shi. Sleepy Consensus. In *AsiaCrypt 2017*.

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

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

53. Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the Blockchain Protocol in Asynchronous Networks. In *EuroCrypt'17*, pages 260–289, 2017.

54. Rafael Pass, Elaine Shi and Florian Tramer. Formal Abstractions for Attested Execution Secure Processors. In *EuroCrypt'17*, pages 643–673, 2017.

55. 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.

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

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

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

59. 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.

60. 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.

61. 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.

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

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

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

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

66. 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.

67. 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.

68. 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.

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

70. 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.

71. 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.

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

73. 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.

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

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

76. 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.

77. 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

78. 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.

79. 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.

80. 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.

81. 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.

82. 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.

83. 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.

84. 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.

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

86. 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

87. 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

88. 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

89. 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.

90. 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.

91. 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.

92. 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.

93. 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.

94. 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.

95. 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.

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

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

98. 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.

99. 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.

100. 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.

101. 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.

102. 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.

103. 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.

104. 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.

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

106. 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.

107. 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.

108. 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.

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

110. 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.

111. 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.

112. 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.

113. 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.

114. 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.

115. 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.

116. 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.

117. 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.

118. 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.

119. 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.

120. 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.

121. 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.

122. 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.

123. 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.

124. 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.

125. 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.

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

127. 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.

128. 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.

129. 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.

130. 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.

131. 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.

132. 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.

133. 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.

134. 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.

135. 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.

136. 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.

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

138. 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.

139. 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.

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

141. 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.

142. 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.

143. 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.

144. 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.

145. 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.

146. 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.

147. 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.

Scientific Services

Program Commitees:

- 44th Annual International Cryptology Conference (EUROCRYPT'25)
- Advances in Financial Technologies (AFT'24)
- 37nd The International Symposium on Distributed Computing (DISC'23)
- Advances in Financial Technologies (AFT'23)
- program co-chair "Minimal Complexity Assumptions for Cryptography", 2023
- area-chair EC'22
- co-organizer of Simons program on Meta-complexity, 2023
- **Program co-Chair** 3rd International Conference on Blockchain Economics, Security and Protocols (Tokenomics'21), 2021.
- 11th Innovations in Theoretical Computer Science Conference (ITCS'21).
- 40th Annual International Cryptology Conference (EUROCRYPT'21).
- **Program co-Chair** 18th Theory of Cryptography Conference (TCC'20), 2020.
- co-organizer of Simons program on Proofs, Consensus, and Decentralizing Society, 2019
- co-organizer of Blockchain Workshop affiliated with CRYPTO'19
- co-organizer of Theory of Blockchains and Cryptocurrency affiliated with FOCS'18.
- co-organizer of Cornell-Tsinghua Workshop on Cryptography, 2017-2019.
- 38th Annual International Cryptology Conference (EUROCRYPT'19).
- 9th Innovations in Theoretical Computer Science Conference (ITCS'19).
- 32nd The International Symposium on Distributed Computing (DISC'18)
- Theoretical Aspects of Reasoning about Rationality and Knowledge (TARK'17)
- 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 (JCSS), Associate Editor since 2014.

Non-Academic Work Experience

2023-2024	*VMWare Research*, Tel-Aviv, Israel. Affiliated Researcher.
2017–2019	*ThunderCore*. Scientist. ThunderCore developed a new blockchain solution based on our research.
2013–2016	*Anonize*, Co-Founder. Anonize developed a cryptographic systems for achieving anonymity based on our research. Our system is the cornerstone of the anonymity solution used in the new *Brave* browser (founded by Brendan Eich, previously co-founder of Mozilla); 68 million active users.
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.