Curriculum Vitae

Alon Rosen

Current Position

2021–present Professor - Faculty Department of Decision Sciences.
Bocconi University, Milan, Italy.

Education

1994–1997 B.Sc. in Mathematics and Computer Science (Magna Cum Laude).
Hebrew University, Jerusalem, Israel.

1997–1999 M.Sc. in Computer Science (advisor: Moni Naor).
Weizmann Institute of Science, Rehovot, Israel.
Thesis: *Pseudo-Random Functions and Factoring.*

1999–2003 Ph.D. in Computer Science (advisors: Oded Goldreich, Moni Naor).
Weizmann Institute of Science, Rehovot, Israel.
Thesis: *The Round-Complexity of Black-Box Concurrent Zero-Knowledge.*

Employment History

1987–1994 Military Service.
Pilot: 1991-1994 Flight instructor - Israeli Air-Force Academy.

2003–2005 Postdoctoral Fellow - Cryptography and Information Security Group.
CSAIL, MIT, Cambridge, MA,

2005–2007 Postdoctoral Fellow - Center for Research on Computation and Society.
DEAS, Harvard University, Cambridge, MA, USA.

2007–2011 Lecturer - Efi Arazi School of Computer Science
Herzliya Interdisciplinary Center (IDC), Herzliya, Israel.

2011–2013 Senior Lecturer - Efi Arazi School of Computer Science
Herzliya Interdisciplinary Center (IDC), Herzliya, Israel.

2013–2017 Associate Professor - Efi Arazi School of Computer Science
Herzliya Interdisciplinary Center (IDC), Herzliya, Israel.

2017–2021 Professor - Efi Arazi School of Computer Science
Herzliya Interdisciplinary Center (IDC), Herzliya, Israel.

Languages

- **Hebrew:** mother tongue.
- **English, Italian:** fluent.
- **French:** average.

Awards

- *Award for excellence from the Council of Higher Education*, Israel, 1999–2003.
- *The Elchanan E. Bondi Memorial Ph.D. Distinction Prize*, Weizmann Institute, 2004.
- *Rothschild Postdoctoral Fellowship*, 2003-2004.
- *Award for Excellence in Research.* IDC Herzliya, 2010.
- *Award for Excellence in Teaching.* IDC Herzliya, 2012.
- *Award for Excellence in Research.* IDC Herzliya, 2015.
- *TCC Test of Time Award* (with Chris Peikert), for the TCC 2006 paper titled ”Efficient Collision Resistant Hashing from Worst-Case Assumptions on Cyclic Lattices”, 2017.

Grants

- United States - Israel Binational Science Foundation (BSF) - *Composition of Cryptographic Protocols* (with Ran Canetti and Rafael Pass). Grant No. 2006317 (106,000 USD).
- Israel Science Foundation (ISF) - *Utility Based Cryptography.* Grant No. 334/08 (4 x 143,000 NIS).
- United States - Israel Binational Science Foundation (BSF) - *Fast Cryptography from Algebraic Lattices* (with Chris Peikert). Grant No. 2010296 (112,000 USD).
- European Research Council (ERC) Starting Grant - *Fast and Sound Cryptography: From Theoretical Foundations to Practical Constructions* (1,498,000 EUR).
- Israel Science Foundation (ISF) - *New Directions in Oblivious Cryptography* (with Moni Naor). Grant No. 1255/12 (4 x 235,000 NIS).
- NSF-BSF Cyber Security Grant - *Horizons of Symmetric-Key Cryptography* (with Chris Peikert and Gil Segev). 3 x 100,000 USD (Israeli PIs).
- TAU Interdisciplinary Cyber Research Center (ICRC) - *Anonymous and Secure Electronic Voting: Protecting our Democratic Infrastructure* (with Amnon Ta Shma). 2 x 200,000 ILS.
- MIT-Israel Seed Fund - *Bridging the Theory and Practice of Pseudo-random Functions* (with Vinod Vaikuntanathan). 15,000 USD.
- Israel Ministry of Science Technology and Space, India-Israel Joint Research Cooperation - *Efficiency of Secure Computation* (with Shweta Agrawal, Yuval Ishai, Eyal Kushilevitz, Manoj Prabhakharan and Vinod Prabhakharan). 2 x 200,000 ILS (Israeli PIs).
- Israel Science Foundation (ISF) - *Cryptographic Hardness of Structured Search Problems.* Grant No. 1399/17 (4 x 260,000 NIS).
- Horizon 2020 Consortium member - *EU PROMETHEUS: PRivacy preserving pOst-quantuM systEms from advanced crypTograpHic mEchanisms* (400,000 EUR).
- European Research Council (ERC) Advanced Grant - *Fine-Grained Cryptography* (2,493,750 EUR).

Teaching

- *Introduction to Cryptography* (with Salil Vadhan). Harvard University (cs120), Fall 2006.
- *Privacy and Technology* (with Allan Friedman, Mike Smith and Jim Waldo). Harvard University (cs199r), Spring 2007.
- *Cryptography and Game Theory* (with Ran Canetti). Tel Aviv University, Fall 2009.
- *Programming workshop on Cryptographic Voting.* IDC, Fall + Spring 2010, 2011.
- *Discrete Mathematics.* IDC, Fall 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2015, 2016, 2017, 2018, 2019, 2020.
- *Computability and Complexity.* IDC, Spring 2008, 2009, 2010, 2011, 2012, 2013.
- *Cryptography.* IDC, Spring 2008, 2009, 2010, 2011, 2012, 2018, 2019, 2020. Fall 2015, 2016.
- *Coding Theory.* IDC, Spring 2014.
- *Seminar: Topics in the Theory of Computer Science.* IDC, Spring 2014, 2016, 2018.
- *Research Pearls in the Theory of Computer Science.* IDC, Spring 2017.
- *Excellence program in CS*, IDC, Fall 2018, Spring 2019, 2020. Fall 2019, 2020.

Advising/supervision

- Noam Livne (PhD (2010), Weizmann Institute of Science and IDC Herzliya).
- Margarita Vald (PhD, Tel Aviv University and IDC Herzliya).
- Carmit Hazay (Postdoc (2008), IDC Herzliya and Weizmann Institute of Science).
- Arbel Peled (MSc (2016), IDC Herzliya).
- Ronen Gradwohl, Gil Segev (Research assistants, IDC Herzliya).
- Mor Weiss (Postdoc (2018-2020), IDC Herzliya).
- Giulia Alberini, Prabhanjan Ananth, Akshay Kamath, Carsten Baum, Daniel Masny, Prashant Vasudevan, Chris Williamson, Adam Sealfon, Jessica Sorell (FACT Center Interns, IDC).
- Marshall Ball, Deepesh Data, Siyao Guo, Pavel Hubacek, Chethan Kamath, Silas Richelson, Abhishek Bhrushundi, Antigoni Polychroniadou, Manuel Sabin, Aikaterini Sotiraki, Apoorvaa Deshpande, Pratik Soni, Alex Block, Rex Fernando (FACT Center Research Fellows, IDC).

Publications

Books

1. **A. Rosen**. *Concurrent Zero-Knowledge.* Series on Information Security and Cryptography. Springer-Verlag, ISBN: 3540329382, 2006.
2. A. Bogdanov and **A. Rosen**. Pseudorandom Functions: Three Decades Later. *Tutorials on the Foundations of Cryptography.* Springer International Publishing, ISBN: 978331957048-8, DOI: 10.1007/97833195704883, pages 79-158, 2017.
3. Dennis Hofheinz and **A. Rosen**. 17th International Conference, TCC 2019, Nuremberg, Germany, December 15, 2019, *Proceedings, Parts I and II.* ISBN 978-3-030-36032-0, 2019.

Journal papers

4. M. Naor, O. Reingold and **A. Rosen**. Pseudo-Random Functions and Factoring. *SIAM Journal on Computing (SICOMP)* Vol. 31 (5), pages 1383-1404, 2002.
5. R. Canetti, J. Kilian, E. Petrank and **A. Rosen**. Black-Box Concurrent Zero-Knowledge Requires (almost) Logarithmically many Rounds. *SIAM Journal on Computing (SICOMP)* Vol. 32 (1), pages 1-47, 2002.
6. D. Harnik, M. Naor, O. Reingold and **A. Rosen**. Completeness in Two-Party Secure Computation - A Computational View. In *Journal of Cryptology*, Vol. 19 (4) , pages 521-552, 2006.
7. Y. Z. Ding, D. Harnik, R. Shaltiel and **A. Rosen**. Constant-Round Oblivious Transfer in the Bounded-Storage Model. In *Journal of Cryptology*, Vol. 20 (2) , pages 165-202, 2007.
8. R. Pass and **A. Rosen**. New and Improved Constructions of Non-Malleable Cryptographic Protocols. **Invited** to special issue of selected papers from *STOC 2005*, *SIAM Journal on Computing (SICOMP)*, Vol. 38 (2), pages 702-752, 2008.
9. R. Pass and **A. Rosen**. Concurrent Non-Malleable Commitments. **Invited** to special issue of selected papers from *FOCS 2006*, *SIAM Journal on Computing (SICOMP)* Vol. 37 (6), pages 1891-1925, 2008.
10. **A. Rosen** and G. Segev. Chosen Ciphertext Security via Correlated Products. In *SIAM Journal on Computing (SICOMP)* Vol. 39 (7), pages 3058-3088, 2010.
11. R. Pass, **A. Rosen**, and W. D. Tseng. A Non-Black-Box Public-Coin Parallel Zero-Knowledge Argument. In *Journal of Cryptology*, Vol. 26 (1), pages 1-10, 2013.
12. D. M. Freeman, O. Goldreich, E. Kiltz, **A. Rosen** and G. Segev. More Constructions of Lossy and Correlation-Secure Trapdoor Functions. In *Journal of Cryptology*, Vol. 26 (1), pages 39-74, 2013.
13. A. Bogdanov and **A. Rosen**. Input Locality and Hardness Amplification. **Invited** to *Journal of Cryptology* (selected from *TCC 2011* program), Vol. 26 (1), pages 144-171, 2013.
14. R. Gradwohl, N. Livne, and **A. Rosen**. Sequential Rationality in Cryptographic Protocols. In *ACM Transactions on Economics and Computation* (no IF), Vol. 1 (1), 2013.
15. Y. Li, H. Yao, M. Chen, S. Jaggi, and **A. Rosen**. RIPPLE Authentication for Network Coding. Accepted to *IEEE/ACM Transactions on Networking*, 2013.
16. B. Applebaum, A. Bogdanov and **A. Rosen**. A Dichotomy for Local epsilon-biased Generators. In *Journal of Cryptology*, Vol. 29 (3): pages 577-596, 2016.
17. N. Bitansky, R. Canetti, O. Paneth and **A. Rosen**. On the Existence of Extractable One-Way Functions. In *SIAM Journal on Computing (SICOMP)* Vol. 45 (5), pages 1910-1952, 2016.
18. **A. Rosen**, G. Segev and I. Shahaf. Can PPAD Hardness be Based on Standard Cryptographic Assumptions?. In *Journal of Cryptology*, Vol. 34 (1): pages 1-65 ,2021.
19. V. Goyal, S. Richelson, **A. Rosen** and M. Vald. An Algebraic Approach to Non-malleability. Submitted to *SIAM Journal on Computing (SICOMP)* Vol. 50 (5), pages 1537-1579, 2021.

Submitted

20. I. Komargodski, T. Moran, M. Naor, R. Pass, **A. Rosen**, E. Yogev. One-Way Functions and (Im)perfect Obfuscation. Submitted to *SIAM Journal on Computing (SICOMP).*

21. S. Guo, P. Hubacek, **A. Rosen** and M. Vald. Delegating Computation to Rational Provers. Submitted to *Journal of Cryptology.*

22. A. Bogdanov, S. Guo, D. Masny, S. Richelson and **A. Rosen**. On the Hardness of Learning with Rounding over Small Modulus.

In preparation

23. K. Pietrzak, **A. Rosen** and G. Segev. Lossy Functions Do Not Amplify Well, 2016. **Invited** to *Journal of Cryptology* (selected from *TCC 2012* program).

24. **A. Rosen**. A Note on Constant-Round Zero-Knowledge Proofs for NP, 2016.

25. A. Banerjee, C. Peikert and **A. Rosen**. Pseudorandom Functions and Lattices, 2016.

Conference papers

26. M. Naor, O. Reingold and **A. Rosen**. Pseudo-Random Functions and Factoring. *Proceedings of the 32nd Annual Symposium on Theory of Computing (STOC 2000)*, pages 11-20, 2000.

27. **A. Rosen**. A Note on the Round-Complexity of Concurrent Zero-Knowledge. *Advances in Cryptology (CRYPTO 2000)*, Springer LNCS 1880, pages 451-468, 2000.

28. R. Canetti, J. Kilian, E. Petrank and **A. Rosen**. Black-Box Concurrent Zero-Knowledge Requires $\tilde{\Omega}(\log n)$ Rounds. *Proceedings of the 33rd Annual Symposium on Theory of Computing (STOC 2001)*, pages 570-579, 2001.

29. M. Prabhakaran, **A. Rosen** and A. Sahai. Concurrent Zero-Knowledge with Logarithmic Round Complexity. *Proceedings of the 43rd Annual IEEE Symposium on Foundations of Computer Science (FOCS 2002)*, pages 366-375, 2002.

30. R. Pass and **A. Rosen**. Bounded-Concurrent Secure Two-Party Computation in a Constant number of Rounds. *Proceedings of the 44th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2003)*, pages 404-503, 2003.

31. Y. Z. Ding, D. Harnik, R. Shaltiel, **A. Rosen**. Constant-Round Oblivious Transfer in the Bounded-Storage Model. *1st Theory of Cryptography Conference (TCC 2004)*, pages 446-472, 2004.

32. **A. Rosen**. A Note on Constant-Round Zero-Knowledge Proofs for NP. *1st Theory of Cryptography Conference (TCC 2004)*, pages 191-202, 2004.

33. D. Harnik, M. Naor, O. Reingold and **A. Rosen**. Completeness in Two-Party Secure Computation - A Computational View. *Proceedings of the 36th annual symposium on Theory of Computing (STOC 2004)*, pages 252-261, 2004.

34. D. Harnik, J. Kilian, M. Naor, O. Reingold and **A. Rosen**. On Robust Combiners for Oblivious Transfer and other Primitives. *Advances in Cryptology (EUROCRYPT 2005)*, p. 96-113, 2005.

35. 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.

36. R. Pass and **A. Rosen**. Concurrent Non-Malleable Commitments. *Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2005)*, 2005.

37. C. Peikert and **A .Rosen**. Efficient Collision-Resistant Hashing From Worst-Case Assumptions on Cyclic Lattices. *3rd Theory of Cryptography Conference (TCC 2006)*, pages 145-166, 2006. Awarded the **TCC Test of Time Award, 2017**.

38. 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.

39. C. Peikert and **A. Rosen**. Lattices that Admit Logarithmic Worst-Case to Average-Case Connection Factors. In *Proceedings of the 39th annual symposium on Theory of Computing (STOC 2007)*, pages 478-487, 2007.

40. V. Lyubashevsky, D. Micciancio, C. Peikert and **A. Rosen**. SWIFFT: A Modest Proposal for FFT Hashing. In *15th Fast Software Encryption Workshop (FSE 2008)*, 2008.

41. S.J. Ong, D. Parkes, **A. Rosen** and S. Vadhan. Fairness with an Honest Minority and a Rational Majority. In *6th Theory of Cryptography Conference (TCC 2009)*, 2009.

42. **A. Rosen** and G. Segev. Chosen Ciphertext Security via Correlated Products. In *6th Theory of Cryptography Conference (TCC 2009)*, 2009.

43. I. Haitner, **A. Rosen** and R. Shaltiel. On the (Im)Possibility of Arthur-Merlin Witness Hiding Protocols. In *6th Theory of Cryptography Conference (TCC 2009)*, 2009.

44. Y. Li, H. Yao, M. Chen, S. Jaggi and **A. Rosen**. RIPPLE Authentication for Network Coding. In *INFOCOM 2010.*

45. D. M. Freeman, O. Goldreich, E. Kiltz, **A. Rosen** and G. Segev. More Constructions of Lossy and Correlation-Secure Trapdoor Functions. In *13th International Conference on Practice and Theory in Public Key Cryptography (PKC 2010)*, 2010.

46. R. Gradwohl, N. Livne and **A. Rosen**. Sequential Rationality in Cryptographic Protocols. In *Proceedings of the 51st Annual IEEE Symposium on Foundations of Computer Science FOCS 2010)*, 2010.

47. **A. Rosen** and a. shelat. Optimistic Concurrent Zero-Knowledge. In *Advances in Cryptology (ASIACRYPT 2010)*, 2010.

48. A. Bogdanov and **A. Rosen**. Input Locality and Hardness Amplification. In *8th Theory of Cryptography Conference (TCC 2011)*, 2011.

49. K. Pietrzak, **A. Rosen** and G. Segev. Lossy Functions Do Not Amplify Well. In *9th Theory of Cryptography Conference (TCC 2012)*, 2012.

50. B. Applebaum, A. Bogdanov and **A. Rosen**. A Dichotomy for Local epsilon-biased Generators. In *9th Theory of Cryptography Conference (TCC 2012)*, 2012.

51. A. Banerjee, C. Peikert and **A. Rosen**. Pseudorandom Functions and Lattices. In *Advances in Cryptology (EUROCRYPT 2012)*, 2012.

52. J. Ben-Nun, N. Farhi, M. Llewellyn, B. Riva, **A. Rosen**, A. Ta-Shma and D. Wikström. A New Implementation of a Dual (Paper and Cryptographic) Voting System. In *5th International Conference on Electronic Voting (EVOTE 2012)*, 2012.

53. P. Hubacek, J.B. Nielsen and **A. Rosen**. Limits on the Power of Cryptographic Cheap Talk. In *Advances in Cryptology (CRYPTO 2013)*, 2013.

54. S. Guo, P. Hubacek, **A. Rosen** and M. Vald. Rational Arguments: Non-Interactive Delegation with Sublinear Verification. In *5th Conference on Inoovations in Theoretical Computer Science (ITCS 2014)*, 2014.

55. A. Akavia, A. Bogdanov, S. Guo, A. Kamath and **A. Rosen**. Candidate Weak Pseudorandom Functions in AC0$\circ$MOD2. In *5th Conference on Innovations in Theoretical Computer Science (ITCS 2014)*, 2014.

56. S. Agrawal, P. Ananth, V. Goyal, M. Prabhakaran and **A. Rosen**. Lower Bounds for Protocols in the Hardware Token Model. In *11th Theory of Cryptography Conference (TCC 2014)*, 2014.

57. A. Banerjee, H. Brenner, G. Leurent, C. Peikert and **A. Rosen**. SPRING: Fast Pseudorandom Functions via Rounded Ring Products. In *21st Fast Software Encryption Workshop (FSE 2014)*, 2014.

58. N. Bitansky, R. Canetti, O. Paneth and **A. Rosen**. On the Existence of Extractable One-Way Functions. In *Proceedings of the 46th annual symposium on Theory of Computing (STOC 2014)*, 2014.

59. N. Bitansky, R. Canetti, H. Cohn, S. Goldwasser, Y. Tauman Kalai, O. Paneth and **A. Rosen**. The Impossibility of Obfuscation with Auxiliary Input or a Universal Simulator. In *Advances in Cryptology (CRYPTO 2014)*, 2014.

60. H. Brenner, L. Gaspar, G. Leurent, F.-X. Standaert and **A Rosen**. FPGA implementations of SPRING And their Countermeasures against Side-Channel Attacks. In *16th Workshop on Cryptographic Hardware and Embedded Systems (CHES 2014)*, 2014.

61. I. Komargodski, T. Moran, M. Naor, R. Pass, **A. Rosen** and E. Yogev. One-Way Functions and (Im)perfect Obfuscation. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2014)*, 2014.

62. V. Goyal, S. Richelson, **A. Rosen** and M. Vald. An Algebraic Approach to Non-malleability. In *Proceedings of the 55th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2014)*, 2014.

63. G. Alberini, T. Moran and **A. Rosen**. Public Verification of Private Effort. In *12th Theory of Cryptography Conference (TCC 2015)*, 2015.

64. B. Hemenway, R. Ostrovsky and **A. Rosen**. Non-Committing Encryption from Φ-Hiding. In *12th Theory of Cryptography Conference (TCC 2015)*, 2015.

65. I. Carboni Oliveira, S. Guo, T. Malkin and **A. Rosen**. The Power of Negations in Cryptography. In *12th Theory of Cryptography Conference (TCC 2015)*, 2015.

66. N. Bitansky, O. Paneth and **A. Rosen**. On the Cryptographic Hardness of Finding a Nash Equilibrium. In *Proceedings of the 56th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2015)*, 2015.

67. H. Brenner, V. Goyal, S. Richelson, **A. Rosen** and M. Vald. Fast Non-Malleable Commitments. In *22nd ACM Conference on Computer and Communications Security (CCS 2015)*, 2015.
68. S. Guo, P. Hubacek, **A. Rosen** and M. Vald. Rational Sum-Checks. In *13th Theory of Cryptography Conference (TCC 2016-A)*, 2016.
69. B. Hemenway, R. Ostrovsky, S. Richelson and **A. Rosen**. Adaptive Security with Quasi-Optimal Rate. In *13th Theory of Cryptography Conference (TCC 2016-A)*, 2016.
70. A. Bogdanov, S. Guo, D. Masny, S. Richelson and **A. Rosen**. On the Hardness of Learning with Rounding over Small Modulus. In *13th Theory of Cryptography Conference (TCC 2016-A)*, 2016.
71. M. Ball, **A. Rosen**, M. Sabin and P. Vasudevan. Average-Case Fine-Grained Hardness. In *Proceedings of the 49th annual symposium on Theory of Computing (STOC 2017)*, 2017.
72. S. Agrawal and **A. Rosen**. Functional Encryption for Bounded Collusions, Revisited. In *15th Theory of Cryptography Conference (TCC 2017)*, 2017.
73. **A. Rosen**, G. Segev and I. Shahaf. Can PPAD Hardness be Based on Standard Cryptographic Assumptions?. In *15th Theory of Cryptography Conference (TCC 2017)*, 2017.
74. P. Hubacek, **A. Rosen** and M. Vald. An Efficiency-Preserving Transformation from Honest-Verifier Statistical Zero-Knowledge to Statistical Zero-Knowledge. In *Advances in Cryptology (EUROCRYPT 2018)*, 2018.
75. M. Ball, **A. Rosen**, M. Sabin and P. Vasudevan. Proofs of Work from Worst-Case Assumptions. In *Advances in Cryptology (CRYPTO 2018)*, 2018.
76. E. Boyle, S. Klein, **A. Rosen** and G. Segev. Securing Abe's Mix-net Against Malicious Verifiers via Witness Indistinguishability. In *11th Conference on Security and Cryptography for Networks (SCN 2018)*, 2018.
77. A. R. Choudhuri, P. Hubáček, C. Kamath, K. Pietrzak, **A. Rosen**, and G. N. Rothblum. Finding a Nash Equilibrium is No Easier than Breaking Fiat-Shamir. In *Proceedings of the 51st annual symposium on Theory of Computing (STOC 2019)*, 2019.
78. M. Ball, E. Boyle, A. Degwekar, A. Deshpande, **A. Rosen**, V. Vaikuntanathan and P. Vasudevan. Cryptography from Information Loss In *11th Conference on Innovations in Theoretical Computer Science (ITCS 2020)*, 2020.
79. S. Guo, P. Kamath, **A. Rosen** and K. Sotiraki. Limits on the Efficiency of (Ring) LWE based Non-Interactive Key Exchange. In *23rd International Conference on Practice and Theory in Public Key Cryptography (PKC 2020)*, 2020.
80. S. Agrawal, Y. Ishai, E. Kushilevitz, V. Narayanan, M. Prabhakaran V. Prabhakaran and **A. Rosen**. Cryptography from One-Way Communication: On Completeness of Finite Channels. In *Advances in Cryptology (ASIACRYPT 2020)*, 2020.
81. M. Abe, M. Ambrona, A. Bogdanov, M. Ohkubo and **A. Rosen**. Non-interactive Composition of Sigma-Protocols via Share-then-Hash. In *Advances in Cryptology (ASIACRYPT 2020)*, 2020.
82. S. Agrawal, Y. Ishai, E. Kushilevitz, V. Narayanan, M. Prabhakaran V. Prabhakaran and **A. Rosen**. Anti-Correlation via Anti-Concentration: Secure Computation from One-Way Noisy Communication. In *Advances in Cryptology (CRYPTO 2021)*, 2021.

83. A. Block, J. Holmgren, **A. Rosen**, R. Rothblum and P. Soni. Public-Coin Zero-Knowledge Arguments with (almost) Minimal Time and Space Overheads. In *Advances in Cryptology (CRYPTO 2021)*, 2021.

84. M. Abe, M. Ambrona, A. Bogdanov, M. Ohkubo and **A. Rosen**. Acyclicity Programming for Sigma-Protocols. In *19th Theory of Cryptography Conference (TCC 2021)*, 2021.

Workshop papers

85. V. Lyubashevsky, D. Micciancio, C. Peikert and **A. Rosen**. Provably Secure FFT Hashing. In *2nd NIST Cryptographic Hash Function Workshop*, 2006.

86. Y. Arbitman, G. Dogon, V. Lyubashevsky, D. Micciancio, C. Peikert and **A. Rosen**. SWIFFTX: A Proposal for the SHA-3 Standard, 2008. In *1st NIST SHA-3 Candidate Conference*, 2009.

Talks

Conferences

- EUROCRYPT 2020, May 2020, **invited speaker**.
- The 15th Theory of Cryptography Conference (TCC 2017), Baltimore, USA, Nov. 2017, **invited speaker**.
- INDOCRYPT 2015, Bangalore, India, December 2015, **invited speaker**.
- The 9th Theory of Cryptography Conference (TCC 2012), Taormina, Italy, Mar. 2012.
- The 16th Annual International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2010), Singapore, December 2010.
- The 7th Theory of Cryptography Conference (TCC 2010), Zurich, Switzerland, Feb. 2010.
- The 6th Theory of Cryptography Conference (TCC 2009), San Francisco, California, USA, March 2009.
- The 6th Theory of Cryptography Conference (TCC 2009), San Francisco, California, USA, March 2009.
- The 15th Fast Software Encryption Workshop (FSE 2008), Lausanne, Switzerland, Feb. 2008.
- The 46th Symposium on Foundations of Computer Science (FOCS 2005), Pittsburgh, Pennsylvania, USA, November 2005.
- The 1st Theory of Cryptography Conference (TCC 2004), Cambridge, Massachusetts, USA, February 2004.
- The 43rd Symposium on Foundations of Computer Science (FOCS 2002), Vancouver, British Columbia, Canada, November 2002.
- The 33rd Annual Symposium on Theory of Computing (STOC 2001), Hersonissos, Crete, Greece, July 2001.
- The 20th Annual International Cryptology Conference (CRYPTO 2000), Santa Barbara, California, USA, August 2000.
- The 32nd annual Symposium on Theory of Computing (STOC 2000), Portland, Oregon, USA, May 2000.

Workshops

- Lower Bounds in Cryptography, Bertinoro, Italy, July 2019.
- Bar-Ilan Winter School on Zero Knowledge, January 2019.
- Societal Concerns in Algorithms and Data Analysis, Weizmann Institute, December 2018.
- FOCS Workshop on "Total Functions in Computation, Communication and Cryptography", Paris, France, Oct. 2018.
- FOCS Workshop on "Theory of Blockchains and Cryptocurrency", Paris, France, Oct. 2018.
- Lattice Cryptography and Algorithms, Bertinoro, Italy, May 2018.
- Workshop in honor of Oded Goldreich's 60th birthday, Weizmann Institute, April 2017.
- Cryptography, Oberwolfach, Germany, January 2017.
- Cryptography and its Interactions: Learning Theory, Coding Theory, and Data Structures (participant), DIMACS, USA, July 2016.
- Recent Advances in Cryptography, IIT Delhi, India, December 2014.
- Cryptography, Oberwolfach, Germany, July 2014.
- Lattice Day, Bangalore, India, December 2013.
- Mysore Park Theory Workshop, Mysore, India, August 2013.
- The 2nd TCE Summer Course on Computer Security, Technion, Haifa, Israel, July 2013.
- Leakage, Tampering and Viruses, Warsaw, Poland, June 2013.
- Verifiable Voting Schemes - from Theory to Practice, Luxembourg March 2013.
- Public-Key Cryptography. Dagstuhl, Germany, September 2011.
- Mini-workshop on the Theory of Computing, Chinese University of Hong Kong, August 2010.
- Solution Concepts for Extensive Games (participant), Aarhus, Denmark, June 2010.
- Technion Cryptoday, June 2010, Haifa, Israel.
- Decentralized Mechanism Design, Distributed Computing, and Cryptography, Princeton, USA, June 2010.
- Public-Key Encryption and Cryptographic Protocols, Bertinoro, Italy, May 2009.
- Voting and Internet, Tel Aviv University School of Management, Israel, January 2009.
- Theoretical Foundations of Practical Information Security. Dagstuhl, Germany, Dec. 2008.
- Open Web Application Security Project Conference, Herzliya, Israel, September 2008.
- Foundations of secure multi-party computation and zero-knowledge and its applications. IPAM UCLA, Los Angeles, USA, November 2006.

Seminars

- ISG Research Seminar, Royal Holloway University London, January 2021.
- NTT Japan Crypto Seminar (3 talks), Tokyo, Japan, February 2020.
- Bocconi University, Milano, Italy, December 2019.

- GTACS Seminar, Weizmann Institute, Rehovot, Israel, January 2019.
- GTACS Seminar, Weizmann Institute, Rehovot, Israel, March 2017.
- I-CORE Day, Weizmann Institute, Rehovot, Israel, April 2016.
- NTT Japan Crypto Seminar (4 talks), Tokyo, Japan, March 2016.
- Theory Seminar, MICROSOFT Research Bangalore, India, December 2015.
- GTACS Seminar, Tel Aviv-Yaffo Academic College, Israel, December 2014.
- Charles River Crypto Day, MIT, Cambridge, MA, October 2014.
- ENS Lyon Arithmetic and Computing Seminar, Lyon, France, October 2014.
- Theory Seminar, Chinese University of Hong Kong, August 2014.
- Theory of Computation Seminar, Hebrew University, Jerusalem, Israel, June 2014.
- State of Israel Committee on Electronic Voting, Israel, May 2014.
- Theory of Computation Seminar, Tel Aviv University, Israel, April 2012.
- Cryptography and Complexity Seminar, Weizmann Institute of Science, Israel, January 2012.
- Theory Seminar, MICROSOFT Research Bangalore, India, November 2010.
- Check Point Institute for Information Security day, October 2010.
- ITCSC Seminar, Chinese University of Hong Kong, July 2010.
- Check Point Technologies R&D group meeting, Tel Aviv, Israel, December 2009.
- Computer Science Colloquium, Tel Aviv University, Israel, November 2009.
- ITCSC Seminar, Chinese University of Hong Kong, July 2009.
- E-Government Course, Lauder School of Government, IDC Herzliya, June 2009.
- Security Theater, Electrical Engineering School, Tel Aviv University, Israel, June 2009.
- Cryptography and Complexity Seminar, Weizmann Institute of Science, Israel, April 2009.
- ITCS Seminar, Tsinghua University, Beijing, China, April 2009.
- Business School Seminar, Hebrew University, Jerusalem, Israel, January 2009.
- Law and Technology Seminar, Tel Aviv University, Israel, December 2008.
- Cryptography and Information Security Seminar, MIT, August 2008.
- Theory of Computation Seminar, Hebrew University, Jerusalem, Israel, July 2008.
- Theory of Computation Seminar, Haifa University, Israel, June 2008.
- ITCS Seminar, Tsinghua University, Beijing, China, April 2008.
- Seminar on Foundations of Privacy, Weizmann Institute of Science, Israel, December 2007.
- Computer Science Colloquium, Tel Aviv University, Israel, December 2006.
- Computer Science Colloquium, Harvard University, February 2006.

- Computer Science Seminar, IDC Herzliya, Israel, January 2006.
- Electrical Engineering Systems Seminar, Tel Aviv University, Israel, January 2006.
- Computer Science Colloquium, Technion, Israel, December 2005.
- Computer Science Colloquium, Haifa University, Israel, December 2005.
- Theory of Computation Seminar, Harvard University, October 2005.
- CRCS Seminar, Harvard University, September 2005.
- Computer Science Colloquium, Hebrew University, Israel, January 2005.
- Theory of Computation Seminar, Princeton University, December 2003.
- Weekly Seminar, MICROSOFT Research SVC, November 2002.
- Cryptography and Information Security Seminar, MIT, November 2002.
- Theory of Computation Seminar, Harvard University, November 2002.
- Cryptographic Research Group Seminar, IBM T.J. Watson Research Center, November 2002.
- Cryptography and Complexity Seminar, Weizmann Institute of Science, Israel, October 2002.
- Computer Science Colloquium, Technion, Israel, June 2001.
- Computer Science Theory Seminar, Hebrew University, Israel, May 2001.
- Cryptography and Complexity Seminar, Weizmann Institute of Science, Israel, April 2001.
- Cryptography and Complexity Seminar, Weizmann Institute of science, Israel, January 2001.
- Cryptographic Research Group Seminar, IBM T.J. Watson Research Center, August 2000.
- Cryptographic Research Group Seminar, IBM T.J. Watson Research Center, July 2000.
- AFLB Seminar, Stanford University, May 2000.
- Computer Science Seminar, IBM Almaden Research Center, May 2000.

Visits

- IBM Almaden Research Center, May 11-17, 2000.
- IBM T.J. Watson Research Center, Hawthorne, NY, USA, Jun-Sep 2000.
- Princeton University December 8-12, 2003.
- UCLA, Los Angeles, November 5-10, 2004.
- Rutgers University, January 23-27, 2006.
- IPAM, Los Angeles, October 25-28 and November 13-17, 2006.
- Tsinghua University, Beijing, April 15-20, 2008.
- Fudan University, Shanghai, April 21-27, 2008.
- MIT, Cambridge Massachusetts, July 27-August 22, 2008.
- SRI International, Menlo Park, California, March 18-19, 2009.

- Tsinghua University, Beijing, April 4-16, 2009.
- Chinese University of Hong Kong, July 1-28, 2009.
- MICROSOFT Research, Cambridge, MA, August 1-19, 2009.
- Chinese University of Hong Kong, July 15-August 15, 2010.
- Northwestern University, October 19-22, 2010.
- MICROSOFT Research, Bangalore, India, November 30-December 5, 2010.
- Tata Institute for Fundamental Research, Mumbai, India, December 9-11, 2010.
- UCLA, Los Angeles, June 29-August 15, 2011.
- Chinese University of Hong Kong, July 5-12, 2012.
- IST Austria, Vienna, August 7-10, 2012.
- Chinese University of Hong Kong, July 3-8, 2013.
- Chinese University of Hong Kong, August 3-26, 2014.
- ENS Lyon, October 15-18, 2014.
- MIT, Cambridge Massachusetts, October 19-24, 2014.
- IIT Delhi, December 17-23, 2014.
- Simons Institute for the Theory of Computing, June 1-August 14, 2015.
- Chinese University of Hong Kong, October 4-10, 2015.
- IST Austria, Vienna, January 29-31, 2016.
- NTT Japan. Feb 29-March 4, 2016.
- Chinese University of Hong Kong, June 15-21, 2016.
- Chinese University of Hong Kong, October 1-10, 2016.
- Chinese University of Hong Kong, June 8-13, 2017.
- Chinese University of Hong Kong, July 11-19, 2017.
- MIT, Cambridge Massachusetts, November 9-12, 2017.
- MIT, Cambridge Massachusetts, February 2-8, 2018.
- Chinese University of Hong Kong, July 16-26, 2018.
- IST Austria, Vienna, August 5-8, 2018.
- IIT Bombay, November 7-10, 2018.
- Chinese University of Hong Kong, April 11-17, 2019.
- Bocconi University, December 12-14, 2019.
- NTT Japan. Feb 12-Feb 21, 2020.

Services to the Scientific Community

Journal Editorials: Associate Editor, *Journal of Cryptology*, 2015-

Award committees: TCC test-of-time award committee (2021-2023).

Conference Program Committees: Served on the program committee of

- TCC 2005, February 10-12, 2005, Cambridge, MA.
- EUROCRYPT 2007, May 20-24, 2007, Barcelona, Spain.
- CRYPTO 2008, August 17-21, 2008, Santa Barbara, CA.
- EVT/WOTE 2009, August 10-14, 2009, Montreal, Canada.
- TCC 2010, February 9-11, 2010, Zurich, Switzerland.
- PKC 2010, May 26-28, 2010, Paris, France.
- PKC 2012, May 21-23, 2012, Darmstadt, Germany.
- SCN 2012, Sep 5-7, 2012, Amalfi, Italy.
- TCC 2013, March 3-6, 2013, Tokyo, Japan.
- ASIACRYPT 2014, December 7-11, 2014, Kaohsiung, Taiwan.
- EUROCRYPT 2015, April 26-30, 2015, Sofia, Bulgaria.
- TCC 2016-B, November 1-3, 2016, Beijing, China.
- FSTTCS 2017. December 11-15, 2017, Kanpur, India.
- EUROCRYPT 2018. April 29-May 3, 2018, Tel Aviv, Israel.
- ICALP 2018. July 9-13, 2018, Prague, Czech Republic.
- TCC 2018, November 12-14, 2018, Goa, India.
- TCC 2019, December 1-4, 2019, Nuremberg, Germany (**program co-chair**).
- CRYPTO 2020, August 17-21, 2020, Santa Barbara, CA.
- TCC 2020, November 2020, Virtual.
- TCC 2021, November 2021, Durham, NC.

Grant Panel membership:

- Israel Science Foundation (ISF) in the area of CS - panel member.
- US - Israel Binational Science Foundation (BSF) in the area of CS - panel member.
- US National Science Foundation (NSF) - panel member.
- US - Israel Binational Science Foundation (BSF) in the area of CS - **panel chair**.

Workshops: co-organizer of the following workshops

- Electronic Voting. May 17-18, 2009, IDC Herzliya and Tel Aviv University.
- Verifiable Elections and the Public, July 10-15, 2011, Dagstuhl, Germany.

- First Cryptography in the Desert Workshop, February 9-12, 2013, Mizpeh Ramon, Israel.
- Second Cryptography in the Desert Workshop, January 7-10, 2016, Sde Boker, Israel.
- Crypto in the Gallilee Workshop, April 27-29, 2018, Maalot-Tarshiha, Israel.

Seminars: co-organizer of weekly Greater Tel-Aviv Area Cryptography seminar (GTACS), jointly with TAU, BIU, and Weizmann 2012-2021.

Journal Refereeing: Journal of Cryptology, SIAM Journal on Computing (SICOMP), Journal of the ACM (JACM), Information and Computation, Communications of the ACM (CACM), Theoretical Computer Science (TCS).

Conference Refereeing (2001-present): EUROCRYPT, CRYPTO, ASIACRYPT, STOC, FOCS, SODA, TCC, FSTCCS, ITCS, ICALP.

Thesis Committees:

- Yoni Moses, Itay Berman, Eyal Widder (MSc committee member, TAU).
- Iddo Bentov, Daniel Genkin (PhD candidacy examiner, Technion).
- Chin Ho Lee, Sham Yik Kin, Chiwang Chang (MSc committee member, CUHK).
- Adeline Langlois (PhD committee member, ENS Lyon).
- Chethan Kamath (PhD committee member, IST Austria).
- Iddo Bentov, Mor Weiss (PhD committee member, Technion).
- Bernardo David (PhD committee member, Aarhus University).
- Guille Pascual Perez (PhD committee member, IST Austria).

Industry Involvement

Consulting:

- Advisory board, Porticor Inc. (`http://www.porticor.com`), 2012-2015 (acquired by Intuit).
- Advisor, Kindite Inc. (`https://www.kindite.com/`), 2016-2019 (acquired by RingCentral).
- Consultant, Intuit Inc. (`https://www.intuit.com/`), 2017-2018.
- Lead cryptography researcher, Identiq Inc. (`https://www.identiq.com/`), 2019-

Patents:

- Paper Voting with Cryptographic Assurance (with Ben Riva and Amnon Ta Shma), 2011.
- Methods and Devices for Securing Keys When Key-Management Processes are Subverted by an Adversary (with Gilad Parann-Nisani and Yaron Sheffer), 2014.
- Homomorphic Key Derivation (with Gleb Keselman and Yaron Sheffer), 2018.