Curriculum Vitae

Yehuda Lindell

October 21, 2018

Contact Information

Address:	Department of Computer Science Bar-Ilan University Ramat Gan, 52900, Israel.
Telephone:	+972-77-364 3515
Fax:	+972-77-364 3551
Email:	lindell(at)biu.ac.il
Home Page:	http://www.cs.biu.ac.il/~lindell/

Current Position

Professor in the Department of Computer Science, Bar-Ilan University, Israel.
Director of the Bar-Ilan Center for Research in Applied Cryptography and Cyber Security.
Incumbent of the Alter Family Chair in Cyber Security.

Research Interests

My main research interests are in the field of *cryptography*, with a focus on *secure protocols*. My research concentrates both on questions of *feasibility* and *efficiency*. The former question asks what cryptographic tasks can be realized and under what assumptions, and is related to the theoretical foundations of cryptography. The focus of the latter question is the construction of efficient cryptographic schemes and protocols that have rigorous proofs of security and correctness. This research includes the development of new models and definitions for secure computation that enable the construction of highly efficient protocols. A primary aim of my research in this area is to demonstrate that secure computation has potential for real-world use, and many real-world problems can already be solved today in practice. In many cases, there is still a long way to go in order to obtain protocols that are efficient enough to be used in practice. In these cases, I am interested in the algorithmic process of finding more and more efficient protocols.

Education

9/1998 – 8/2002: *The Weizmann Institute of Science* (Rehovot, Israel).
Ph.D. in Computer Science
Field of Research: Cryptography
Thesis: On the Composition of Secure Multi-Party Protocols.
Advisors: Oded Goldreich and Moni Naor

9/1997 – 8/1998: *Bar-Ilan University* (Ramat Gan, Israel).
M.Sc. in Computer Science, Summa cum Laude
Field of Research: Data Mining
Thesis: A Statistical Theory for Quantitative Association Rules.
Advisor: Yonatan Aumann

9/1994 – 8/1997: *Bar-Ilan University* (Ramat Gan, Israel).
B.Sc. in Computer Science and Mathematics
Summa cum Laude

Employment History

10/2011 – *present*	Professor, Bar-Ilan University, Ramat Gan, Israel.
02/2014 – *present*	Co-Founder and Chief Scientist, Dyadic Security Ltd.
03/2008 – 10/2011	Associate professor, Bar-Ilan University, Ramat Gan, Israel.
10/2004 – 02/2008	Senior Lecturer (a.k.a. assistant professor), Bar-Ilan University, Ramat Gan, Israel.
11/2004 – 12/2014	Cryptography Consultant, Safenet Inc. (previously, Aladdin), Israel.
09/2002 – 07/2004	Post-Doctoral Researcher at the Cryptography Research Group, IBM T.J.Watson Research, New York, USA.

Awards

- *Best Paper Award at the* 24*th ACM Conference on Computer and Communications Security*, 2017, for the paper Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation.
- *Best Paper Award at the* 23*rd ACM Conference on Computer and Communications Security*, 2016, for the paper High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority.
- *IBM 2006 Pat Goldberg Memorial Best Paper Award in Computer Science, Electrical Engineering and Math*, for the paper On the Composition of Authenticated Byzantine Agreement (co-authored with Anna Lysyanskaya and Tal Rabin).
- *IBM Josef Raviv Memorial Postdoctoral Fellowship,* 2002–2004.
- *The Esther Helinger Memorial Ph.D. Distinction Prize,* The Weizmann Institute of Science, 2002.
- *Award for Excellence from the Council of Higher Education, Israel,* 1999-2000, 2000-01 and 2001-02.
- *Dean's Undergraduate List of Excellence,* 1994-95, 1995-96 and 1996-97, Department of Mathematics and Computer Science, Bar-Ilan University, Ramat Gan, Israel.

Research Grants

(The amounts listed reflect my portion of the award only.)

- Hardware-Aware Cryptographic Design, Israel Science Foundation (ISF), 390,000 NIS (approx. $110,000). Co-principal investigator, *October 2016 – September 2020.*
- Efficient Two-Party and Multiparty Computation: Constructions and Implementations, Joint Israel-UK Research Grant, Israel Ministry of Science, 1,275,185 NIS (approx. $330,000). Principal Investigator (joint project with Nigel Smart), January 2015 - December 2017.
- Distributed Cryptography Module (DCM), European Research Council (ERC) Proof of Concept Grant, €149,776 (approximately $200,000). Principal investigator (personal grant), *October 2014 – April 2016.*
- High-Performance Secure Computation with Applications to Privacy and Cloud Security (HIPS), European Research Council (ERC) Consolidator Grant, €1,999,175 (approximately $2,700,000). Principal investigator (personal grant), *October 2014 – September 2019.*
- Privacy-Preserving Computation in the Cloud (PRACTICE), EU FP7 Project, approximately €340,000 (this is my portion out of approx. €680,000 for Bar-Ilan, with the overall budget of the project being €7,550,000). Principal investigator, *November 2013 – October 2016.*
- Revisiting Fundamentals of Secure Computation, Israel Science Foundation (ISF), 748,800 NIS (approx. $215,000). Principal investigator (personal grant), *October 2011 – September 2015.*
- Large Scale Privacy-Preserving Technology in the Digital World (LAST), European Research Council (ERC) Starting Grant, €1,912,316 (approximately $2,677,000). Principal investigator (personal grant), *October 2009 – September 2014.*
- Secure Computation - Bridging the Gap Between Theory and Practice, Israel Science Foundation (ISF), 584,000 NIS (approximately $146,000). Principal investigator (personal grant), *October 2007 – September 2011.*
- Privacy-Preserving Data Mining, Israel Ministry of Science and Technology Infrastructure Grant, 254,700 NIS (approximately $64,000). Principal investigator and project coordinator, *December 2005 – November 2008.*
- Feasibility and Efficiency of Secure Computation, United States-Israel Binational Science Foundation (BSF), $60,000. Principal investigator, *September 2005 – August 2009.*

Books

1. J. Katz and Y. Lindell. Introduction to Modern Cryptography, 2nd edition. CRC Press, November 2014.
2. C. Hazay and Y. Lindell. Efficient Secure Two-Party Protocols: Techniques and Constructions. Springer, November 2010.
3. J. Katz and Y. Lindell. Introduction to Modern Cryptography. CRC Press, 2007.
4. Y. Lindell. Composition of Secure Multi-Party Protocols – A Comprehensive Study. Lecture Notes in Computer Science Volume 2815 (LNCS Monograph), Springer, September 2003.

Edited Books

1. Y. Lindell (Ed.). Tutorials on the Foundations of Cryptography (Dedicated to Oded Goldreich). Springer, April 2017.

2. Y. Lindell (Ed.). The 11th International Conference on the Theory of Cryptography (TCC 2014). Lecture Notes in Computer Science, Volume 8349, Springer, 2014.

Book Chapters (Invited)

1. G. Asharov and Y. Lindell. The BGW Protocol for Perfectly-Secure Multiparty Computation. *Secure Multiparty Computation*, M. Prabhakaran and A. Sahai (Ed.), Cryptology and Information Security Series, IOS Press, 2012.

2. Y. Lindell. Secure Computation for Privacy Preserving Data Mining. In the *Encyclopedia of Data Warehousing and Mining*, J. Wang (Ed.), Idea Group Reference, 2005.

Journal Publications

1. G. Asharov, S. Halevi, Y. Lindell and T. Rabin. G. Asharov, S. Halevi, Y. Lindell and T. Rabin. Privacy-Preserving Search of Similar Patients in Genomic Data. In the 18*th Privacy Enhancing Technologies Symposium*, PoPETs 2018(4):104–124, 2018.

2. Y. Lindell and H. Zarosim. On the Feasibility of Extending Oblivious Transfer. In the *Journal of Cryptology*, 31(3):737–773, 2018.

3. S. Gueron, Y. Lindell, A. Nof and B. Pinkas. Fast Garbling of Circuits Under Standard Assumptions. In the *Journal of Cryptology*, 31(3): 798–844, 2018.

4. Y. Lindell, E. Omri and H. Zarosim. Completeness for Symmetric Two-Party Functionalities – Revisited. In the *Journal of Cryptology*, 31(3):671–697, 2018.

5. R. Cohen and Y. Lindell. Fairness Versus Guaranteed Output Delivery in Secure Multiparty Computation. In the *Journal of Cryptology*, 30(4):1157–1186, 2017.

6. G. Asharov, Y. Lindell, T. Schneier and M. Zohner. More Efficient Oblivious Transfer Extensions. In the *Journal of Cryptology*, 30(3):805–858, 2017.

7. G. Asharov and Y. Lindell. A Full Proof of the BGW Protocol for Perfectly-Secure Multiparty Computation. In the *Journal of Cryptology*, 30(1):58–151, 2017.

8. Y. Lindell. Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries. In the *Journal of Cryptology*, 29(2):456–490, 2016.

9. Y. Lindell and B. Pinkas. An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries. In the *Journal of Cryptology*, 28(2):312–350, 2015.

10. Y. Lindell. A Note on Constant-Round Zero-Knowledge Proofs of Knowledge. In the *Journal of Cryptology*, 26(4):638–654, 2013.

11. Y. Lindell and B. Pinkas. Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer. In the *Journal of Cryptology*, 25(4):680–722, 2012.

12. S.D. Gordon, C. Hazay, J. Katz and Y. Lindell. Complete Fairness in Secure Two-Party Computation. In the *Journal of the ACM*, 58(6):24 (37 pages), 2011.

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

14. Y. Lindell and H. Zarosim. Adaptive Zero-Knowledge Proofs and Adaptively Secure Oblivious Transfer. In the *Journal of Cryptology*, 24(4):761–799, 2011.

15. D. Kidron and Y. Lindell. Impossibility Results for Universal Composability in Public-Key Models and with Fixed Inputs. In the *Journal of Cryptology*, 24(3):517–544, 2011.

16. I. Haitner, Y. Ishai, E. Kushilevitz, Y. Lindell and E. Petrank. Black-Box Constructions for Secure Computation. In the *SIAM Journal on Computing*, 40(2):225–266, 2011.

17. Y. Ishai, E. Kushilevitz, J. Katz, Y. Lindell and E. Petrank. On Achieving the "Best of Both Worlds" in Secure Multiparty Computation. In the *SIAM Journal on Computing*, 40(1):122–141, 2011.

18. G. Asharov and Y. Lindell. Utility Dependence in Correct and Fair Rational Secret Sharing. In the *Journal of Cryptology*, 24(1):157–202, 2011.

19. Y. Lindell. Anonymous Authentication. In the *Journal of Privacy and Confidentiality*, 2(2):35–63, 2010.

20. C. Hazay and Y. Lindell. Efficient Protocols for Set Intersection and Pattern Matching with Security Against Malicious and Covert Adversaries. In the *Journal of Cryptology*, 23(3):422–456, 2010.

21. E. Kushilevitz, Y. Lindell and T. Rabin. Information-Theoretically Secure Protocols and Security Under Composition. In the *SIAM Journal on Computing* (SICOMP), 39(5):2090–2112, 2010.

22. Y. Aumann and Y. Lindell. Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries. In the *Journal of Cryptology*, 23(2):281–343, 2010.

23. Y. Lindell. Legally Enforceable Fairness in Secure Two-Party Computation. In the *Chicago Journal of Theoretical Computer Science*, 2009(1):1–15, 2009.

24. Y. Lindell. General Composition and Universal Composability in Secure Multi-Party Computation. In the *Journal of Cryptology*, 22(3):395–428, 2009.

25. Y. Lindell and B. Pinkas. A Proof of Security of Yao's Protocol for Secure Two-Party Computation. In the *Journal of Cryptology*, 22(2):161–188, 2009.

26. Y. Lindell and B. Pinkas. Secure Multiparty Computation for Privacy-Preserving Data Mining. In the *Journal of Privacy and Confidentiality*, 1(1):59–98, 2009.

27. Y. Lindell. Efficient Fully-Simulatable Oblivious Transfer. In the *Chicago Journal of Theoretical Computer Science*, 2008(6):1–20, 2008.

28. J. Katz and Y. Lindell. Handling Expected Polynomial-Time Strategies in Simulation-Based Proofs. In the *Journal of Cryptology*, 21(3):303–349, 2008.

29. Y. Lindell. Lower Bounds and Impossibility Results for Concurrent Self Composition. In the *Journal of Cryptology*, 21(2):200–249, 2008.

30. Y.T. Kalai, Y. Lindell and M. Prabhakaran. Concurrent Composition of Secure Protocols in the Timing Model. In the *Journal of Cryptology*, 20(4):431–492, 2007.

31. Y. Lindell, A. Lysyanskaya and T. Rabin. On the Composition of Authenticated Byzantine Agreement. In the *Journal of the ACM*, 53(6):881–917, 2006.

32. Y. Lindell. Protocols for Bounded-Concurrent Secure Two-Party Computation Without Setup Assumptions. In the *Chicago Journal of Theoretical Computer Science*, 2006(1):1–50, 2006.

33. R. Gennaro and Y. Lindell. A Framework for Password-Based Authenticated Key Exchange. In the *ACM Transactions on Information and System Security* (TISSEC), 9(2):181–234, 2006.

34. O. Goldreich and Y. Lindell. Session-Key Generation using Human Passwords Only. In the *Journal of Cryptology*, 19(3):241–340, 2006.

35. Y. Lindell. A Simpler Construction of CCA2-Secure Public-Key Encryption Under General Assumptions. In the *Journal of Cryptology*, 19(3):359–377, 2006.

36. B. Barak, Y. Lindell and S. Vadhan. Lower Bounds for Non-Black-Box Zero Knowledge. In the *Journal of Computer and System Sciences*, 72(2):321–391, 2006. (JCSS FOCS 2003 Special Issue)

37. R. Canetti, E. Kushilevitz and Y. Lindell. On the Limitations of Universally Composable Two-Party Computation Without Set-Up Assumptions. In the *Journal of Cryptology*, 19(2):135–167, 2006.

38. S. Goldwasser and Y. Lindell. Secure Computation Without Agreement. In the *Journal of Cryptology* (invited paper – special issue on new results in Byzantine Agreement), 18(3):247–287, 2005.

39. B. Barak and Y. Lindell. Strict Polynomial-Time in Simulation and Extraction. In the *SIAM Journal on Computing* (SICOMP), 33(4):783–818, 2004.

40. Y. Lindell. Parallel Coin-Tossing and Constant-Round Secure Two-Party Computation. In the *Journal of Cryptology*, 16(3):143–184, 2003.

41. Y. Aumann and Y. Lindell. A Statistical Theory for Quantitative Association Rules. In the *Journal of Intelligent Information Systems* (JIIS), 20(3):255–283, 2003.

42. Y. Lindell and B. Pinkas. Privacy Preserving Data Mining. In the *Journal of Cryptology*, 15(3):177–206, 2002.

Publications in Refereed Conferences

1. Y. Lindell and A. Nof. Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody. In the *25th ACM Conference on Computer and Communications Security* (ACM CCS), pages 1837–1854, 2018.

2. A. Barak, M. Hirt, L. Koskas and Y. Lindell. An End-to-End System for Large Scale P2P MPC-as-a-Service and Low-Bandwidth MPC for Weak Participants. In the 25*th ACM Conference on Computer and Communications Security* (ACM CCS), pages 695–712, 2018.

3. T. Araki, A. Barak, J. Furukawa, M. Keller, Y. Lindell, K. Ohara and H. Tsuchida. Generalizing the SPDZ Compiler For Other Protocols. In the 25*th ACM Conference on Computer and Communications Security* (ACM CCS), pages 880–895, 2018.

4. G. Asharov, S. Halevi, Y. Lindell and T. Rabin. Privacy-Preserving Search of Similar Patients in Genomic Data. In the 18*th Privacy Enhancing Technologies Symposium*, PoPETs 2018(4):104–124, 2018.

5. K. China, D. Genkin, K. Hamada, D. Ikarashi, R. Kikuchi, Y. Lindell and A. Nof. Fast Large-Scale Honest-Majority MPC for Malicious Adversaries. In *Advances in Cryptology – CRYPTO 2018*, Springer (LNCS 10993), pages 34–64, 2018.

6. T. Frederiksen, Y. Lindell, V. Osheter and B. Pinkas. Fast Distributed RSA Key Generation for Semi-Honest and Malicious Adversaries. In *Advances in Cryptology – CRYPTO 2018*, Springer (LNCS 10992), pages 331–361, 2018.

7. Y. Lindell and A. Yanai. Fast Garbling of Circuits over 3-Valued Logic. In the 21*st Public-Key Cryptography Conference* (PKC), Springer (LNCS 10769), pages 620–643, 2018.

8. A. Ben-Efraim, Y. Lindell and E. Omri. Efficient Scalable Constant-Round MPC via Garbled Circuits. In *Advances in Cryptology – ASIACRYPT 2017*, Springer (LNCS 10625), pages 471–498, 2017.

9. Y. Lindell and T. Rabin. Secure Two-Party Computation with Fairness – A Necessary Design Principle. In the *15th Theory of Cryptography Conference* (TCC), Springer (LNCS 10677), pages 565–580, 2017.

10. Y. Lindell and A. Nof. A Framework for Constructing Fast MPC over Arithmetic Circuits with Malicious Adversaries and an Honest-Majority. In the 24*th ACM Conference on Computer and Communications Security* (ACM CCS), pages 259–276, 2017.

11. S. Gueron and Y. Lindell. Better Bounds for Block Cipher Modes of Operation via Nonce-Based Key Derivation. In the 24*th ACM Conference on Computer and Communications Security* (ACM CCS), pages 1019–1036, 2017. **Recipient of the best paper award**.

12. Y. Lindell. Fast Secure Two-Party ECDSA Signing. In *Advances in Cryptology – CRYPTO 2017*, Springer (LNCS 10402), pages 613–644, 2017.

13. T. Araki, A. Barak, J. Furukawa, T. Lichter, Y. Lindell, A. Nof, K. Ohara, A. Watzman, and O. Weinstein. Optimized Honest-Majority MPC for Malicious Adversaries - Breaking the 1 Billion-Gate Per Second Barrier. In the *38th IEEE Security and Privacy Conference*, pages 843–862, 2017.

14. J. Furukawa, Y. Lindell, A. Nof and O. Weinstein. High-Throughput Secure Three-Party Computation for Malicious Adversaries and an Honest Majority. In *Advances in Cryptology – EUROCRYPT 2017 (II)*, Springer (LNCS 10211), pages 225–255, 2017.

15. Y. Lindell, N.P. Smart and E. Soria-Vazquez. More Efficient Constant-Round Multi-Party Computation from BMR and SHE. In the *14th Annual Theory of Cryptography Conference* (TCC 2016-B), Springer (LNCS 9985), pages 554–581, 2016.

16. T. Araki, J. Furukawa, Y. Lindell, A. Nof and K. Ohara. High-Throughput Semi-Honest Secure Three-Party Computation with an Honest Majority. In the 23*rd ACM Conference on Computer and Communications Security* (ACM CCS), pages 805–817, 2016. **Recipient of the best paper award**.

17. A. Ben-Efraim, Y. Lindell and E. Omri. Optimizing Semi-Honest Secure Multiparty Computation for the Internet. In the 23*rd ACM Conference on Computer and Communications Security* (ACM CCS), pages 578–590, 2016.

18. V. Kolesnikov, H. Krawczyk, Y. Lindell, A.J. Malozemoff and T. Rabin. Attribute-based Key Exchange with General Policies. In the 23*rd ACM Conference on Computer and Communications Security* (ACM CCS), pages 1451–1463, 2016.

19. S. Gueron and Y. Lindell. GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte. In the 22*nd ACM Conference on Computer and Communications Security* (ACM CCS), pages 109–119, 2015.

20. Y. Lindell and B. Riva. Blazing Fast 2PC in the Offline/Online Setting with Security for Malicious Adversaries. In the 22*nd ACM Conference on Computer and Communications Security* (ACM CCS), pages 579–590, 2015.

21. S. Gueron, Y. Lindell, A. Nof and B. Pinkas. Fast Garbling of Circuits Under Standard Assumptions. In the 22*nd ACM Conference on Computer and Communications Security* (ACM CCS), pages 567–578, 2015.

22. Y. Lindell, B. Pinkas, N. Smart and A. Yanai. Efficient Constant Round Multi-Party Computation Combining BMR and SPDZ. In *Advances in Cryptology – CRYPTO 2015*, Springer (LNCS 9216), pages 319–338, 2015.

23. R. Canetti, A. Cohen and Y. Lindell. A Simpler Variant of Universally Composable Security for Standard Multiparty Computation. In *Advances in Cryptology – CRYPTO 2015*, Springer (LNCS 9216), pages 3–22, 2015.

24. C. Hazay, Y. Lindell and A. Patra. Adaptively Secure Computation with Partial Erasures. In *ACM PODC 2015*, pages 291–300, 2015.

25. G. Asharov, Y. Lindell, T. Schneier and M. Zohner. More Efficient Oblivious Transfer Extensions with Security for Malicious Adversaries. In *Advances in Cryptology – EUROCRYPT 2015*, Springer (LNCS 9056), pages 673–701, 2015.

26. Y. Lindell. An Efficient Transform from Sigma Protocols to NIZK with a CRS and Non-Programmable Random Oracle. In the 12*th Theory of Cryptography Conference* (TCC), Springer (LNCS 9014), pages 93–109, 2015.

27. R. Cohen and Y. Lindell. Fairness Versus Guaranteed Output Delivery in Secure Multiparty Computation. In *Advances in Cryptology – ASIACRYPT 2014*, Part II, Springer (LNCS 8873), pages 466–485, 2014.

28. Y. Lindell and B. Riva. Cut-and-Choose Yao-Based Secure Computation in the Online/Offline and Batch Settings. In *Advances in Cryptology – CRYPTO 2014*, Springer (LNCS 8617), pages 476–494, 2014.

29. Y. Lindell, K. Nissim and C. Orlandi. Hiding the Input-Size in Secure Two-Party Computation. In *Advances in Cryptology – ASIACRYPT 2013*, Springer (LNCS 8270), pages 421–440, 2013.

30. G. Asharov, Y. Lindell and H. Zarosim Fair and Efficient Secure Multiparty Computation with Reputation Systems. In *Advances in Cryptology – ASIACRYPT 2013*, Springer (LNCS 8270), pages 201–220, 2013.

31. G. Asharov, Y. Lindell, T. Schneier and M. Zohner. More Efficient Oblivious Transfer and Extensions for Faster Secure Computation. In the 20*th ACM Conference on Computer and Communications Security* (ACM CCS), pages 535–548, 2013.

32. Y. Lindell. Fast Cut-and-Choose Based Protocols for Malicious and Covert Adversaries. In *Advances in Cryptology – CRYPTO 2013*, Springer (LNCS 8043), pages 1–17, 2013.

33. Y. Lindell and H. Zarosim. On the Feasibility of Extending Oblivious Transfer. In the *10th Annual Theory of Cryptography Conference* (TCC), Springer (LNCS 7785), pages 519–538, 2013.

34. G. Asharov, Y. Lindell and T. Rabin. A Full Characterization of Functions that Imply Fair Coin Tossing and Ramifications to Fairness. In the *10th Annual Theory of Cryptography Conference* (TCC), Springer (LNCS 7785), pages 243–262, 2013.

35. Y. Lindell, E. Omri and H. Zarosim. Completeness for Symmetric Two-Party Functionalities – Revisited. In *Advances in Cryptology – ASIACRYPT 2012*, Springer (LNCS 7658), pages 116–133, 2012.

36. Y. Lindell, E. Oxman and B. Pinkas. The IPS Compiler: Optimizations, Variants and Concrete Efficiency. In *Advances in Cryptology – CRYPTO 2011*, Springer (LNCS 6841), pages 259–276, 2011.

37. G. Asharov, Y. Lindell and T. Rabin. Perfectly-Secure Multiplication for any $t < n/3$. In *Advances in Cryptology – CRYPTO 2011*, Springer (LNCS 6841), pages 240–258, 2011.

38. S. Halevi, Y. Lindell, and B. Pinkas. Secure Computation on the Web: Computing without Simultaneous Interaction. In *Advances in Cryptology – CRYPTO 2011*, Springer (LNCS 6841), pages 132–150, 2011.

39. A. Beimel, Y. Lindell, E. Omri and I. Orlov. $1/p$-Secure Multiparty Computation without Honest Majority and the Best of Both Worlds. In *Advances in Cryptology – CRYPTO 2011*, Springer (LNCS 6841), pages 277–296, 2011.

40. Y. Lindell. Highly-Efficient Universally-Composable Commitments based on the DDH Assumption. In *Advances in Cryptology – EUROCRYPT 2011*, Springer (LNCS 6632), pages 446–466, 2011.

41. Y. Lindell and B. Pinkas. Secure Two-Party Computation via Cut-and-Choose Oblivious Transfer. In the *8th Annual Theory of Cryptography Conference* (TCC), Springer (LNCS 6597), pages 329-346, 2011.

42. D. Dachman-Soled, Y. Lindell, M. Mahmoody and T. Malkin. On the Black-Box Complexity of Optimally-Fair Coin Tossing. In the *8th Annual Theory of Cryptography Conference* (TCC), Springer (LNCS 6597), pages 450–467, 2011.

43. Y. Lindell and E. Waisbard. Private Web Search with Malicious Adversaries. In the 10*th Privacy Enhancing Technologies Symposium* (PETS), Springer (LNCS 6205), pages 220–235, 2010.

44. G. Asharov and Y. Lindell. Utility Dependence in Correct and Fair Rational Secret Sharing. In *Advances in Cryptology – CRYPTO 2009*, Springer (LNCS 5677), pages 559-576, 2009.

45. J. Alwen, J. Katz, Y. Lindell, G. Persiano, A. Shelat and I. Visconti. Collusion-Free Multiparty Computation in the Mediated Model. In *Advances in Cryptology – CRYPTO 2009*, Springer (LNCS 5677), pages 524-540, 2009.

46. Y. Lindell. Comparison-Based Key Exchange and the Security of the Numeric Comparison Mode in Bluetooth v2.1. In the *Cryptographer's Track at the RSA Conference* (CT-RSA), Springer (LNCS 5473), pages 66–83, 2009.

47. Y. Lindell. Adaptively Secure Two-Party Computation with Erasures. In the *Cryptographer's Track at the RSA Conference* (CT-RSA), Springer (LNCS 5473), pages 117–132, 2009.

48. Y. Lindell. Local Sequentiality Does Not Help for Concurrent Composition. In the *Cryptographer's Track at the RSA Conference* (CT-RSA), Springer (LNCS 5473), pages 372–388, 2009.

49. Y. Lindell and H. Zarosim. Adaptive Zero-Knowledge Proofs and Adaptively Secure Oblivious Transfer. In the *6th Annual Theory of Cryptography Conference* (TCC), Springer (LNCS 5444), pages 183–201, 2009.

50. C. Hazay and Y. Lindell. Constructions of Truly Practical Secure Protocols using Standard Smartcards. In the 15*th ACM Conference on Computer and Communications Security* (ACM CCS), pages 491–500, 2008.

51. Y. Lindell, B. Pinkas and N. Smart. Implementing Two-Party Computation Efficiently with Security Against Malicious Adversaries. In the 6*th Conference on Security and Cryptography for Networks*, Springer (LNCS 5229), pages 2–20, 2008.

52. S.D. Gordon, C. Hazay, J. Katz and Y. Lindell. Complete Fairness in Secure Two-Party Computation. In the *40th ACM Symposium on the Theory of Computing* (STOC), pages 413–422, 2008.

53. Y. Lindell. Efficient Fully-Simulatable Oblivious Transfer. In the *Cryptographer's Track at the RSA Conference* (CT-RSA), Springer (LNCS 4964), pages , 2008.

54. Y. Lindell. Legally Enforceable Fairness in Secure Two-Party Computation. In the *Cryptographer's Track at the RSA Conference* (CT-RSA), Springer (LNCS 4964), pages 121–137, 2008.

55. J. Katz and Y. Lindell. Aggregate Message Authentication Codes. In the *Cryptographer's Track at the RSA Conference* (CT-RSA), Springer (LNCS 4964), pages 155–169, 2008.

56. C. Hazay and Y. Lindell. Efficient Protocols for Set Intersection and Pattern Matching with Security Against Malicious and Covert Adversaries. In the *5th Annual Theory of Cryptography Conference* (TCC), Springer (LNCS 4948) pages 155–175, 2008.

57. Y. Lindell and B. Pinkas. An Efficient Protocol for Secure Two-Party Computation in the Presence of Malicious Adversaries. In *Advances in Cryptology – EUROCRYPT 2007*, Springer (LNCS 4515), pages 52–78, 2007.

58. Y. Aumann and Y. Lindell. Security Against Covert Adversaries: Efficient Protocols for Realistic Adversaries. In the *4th Annual Theory of Cryptography Conference* (TCC), Springer (LNCS 4392), pages 137–156, 2007.

59. C. Hazay, J. Katz, C.Y. Koo and Y. Lindell. Concurrently-Secure Blind Signatures without Random Oracles or Setup Assumptions. In the *4th Annual Theory of Cryptography Conference* (TCC), Springer (LNCS 4392), pages 323–341, 2007.

60. Y. Ishai, E. Kushilevitz, Y. Lindell and E. Petrank. On Combining Privacy with Guaranteed Output Delivery in Secure Multiparty Computation. In *Advances in Cryptology – CRYPTO 2006*, Springer (LNCS 4117), pages 483–500, 2006.

61. E. Kushilevitz, Y. Lindell and T. Rabin. Information-Theoretically Secure Protocols and Security Under Composition. In the *38th ACM Symposium on the Theory of Computing* (STOC), pages 109–118, 2006.

62. Y. Ishai, E. Kushilevitz, Y. Lindell and E. Petrank. Black-Box Constructions for Secure Multiparty Computation. In the *38th ACM Symposium on the Theory of Computing* (STOC), pages 99–108, 2006.

63. B. Barak, R. Canetti, Y. Lindell, R. Pass and T. Rabin. Secure Computation Without Authentication. In *Advances in Cryptology – CRYPTO 2005*, Springer (LNCS 3621), pages 361–377, 2005.

64. R. Canetti, S. Halevi, J. Katz, Y. Lindell, P. Mackenzie. Universally Composable Password-Based Key Exchange. In *Advances in Cryptology – EUROCRYPT 2005*, Springer (LNCS 3494), pages 404–421, 2005.

65. Y. Kalai, Y. Lindell and M. Prabhakaran. Concurrent General Composition of Secure Protocols in the Timing Model. In the *37th ACM Symposium on the Theory of Computing* (STOC), pages 644-653, 2005.

66. J. Katz and Y. Lindell. Handling Expected Polynomial-Time Strategies in Simulation-Based Security Proofs. In the *2nd Annual Theory of Cryptography Conference* (TCC), Springer (LNCS 3378), pages 128–149, 2005.

67. Y. Lindell. Lower Bounds for Concurrent Self Composition. In the *1st Theory of Cryptography Conference* (TCC), Springer (LNCS 2951), pages 203–222, 2004.

68. Y. Lindell. General Composition and Universal Composability in Secure Multi-Party Computation. In the *44th IEEE Symposium on the Foundations of Computer Science* (FOCS), pages 394–403, 2003.

69. B. Barak, Y. Lindell and S. Vadhan. Lower Bounds for Non-Black-Box Zero Knowledge. In the *44th IEEE Symposium on the Foundations of Computer Science* (FOCS), pages 384–393, 2003.

70. Y. Lindell. Brief Announcement: Impossibility Results for Concurrent Secure Two-Party Computation. In the *22nd ACM Symposium on the Principles of Distributed Computing* (PODC), page 200, 2003.

71. Y. Lindell. Bounded-Concurrent Secure Two-Party Computation Without Setup Assumptions. In the *35th ACM Symposium on the Theory of Computing* (STOC), pages 683–692, 2003.

72. R. Canetti, E. Kushilevitz and Y. Lindell. On the Limitations of Universally Composable Two-Party Computation Without Set-Up Assumptions. In *Advances in Cryptology – EUROCRYPT 2003*, Springer (LNCS 2656), pages 68–86, 2003.

73. R. Gennaro and Y. Lindell. A Framework for Password-Based Authenticated Key Exchange. In *Advances in Cryptology – EUROCRYPT 2003*, Springer (LNCS 2656), pages 524–543, 2003.

74. Y. Lindell. A Simpler Construction of CCA2-Secure Public-Key Encryption Under General Assumptions. In *Advances in Cryptology – EUROCRYPT 2003*, Springer (LNCS 2656), pages 241–254, 2003.

75. S. Goldwasser and Y. Lindell. Secure Computation Without Agreement. In the *16th International Conference on Distributed Computing* (DISC), Springer (LNCS 2508), pages 17–32, 2002.

76. Y. Lindell, A. Lysyanskaya and T. Rabin. Sequential Composition of Protocols Without Simultaneous Termination. In the *21st ACM Symposium on the Principles of Distributed Computing* (PODC), pages 203–212, 2002.

77. Y. Lindell, A. Lysyanskaya and T. Rabin. On the Composition of Authenticated Byzantine Agreement. In the *34th ACM Symposium on the Theory of Computing* (STOC), pages 514–523, 2002.

78. R. Canetti, Y. Lindell, R. Ostrovsky and A. Sahai. Universally Composable Two-Party and Multi-Party Secure Computation. In the *34th ACM Symposium on the Theory of Computing* (STOC), pages 494–503, 2002.

79. B. Barak and Y. Lindell. Strict Polynomial-Time in Simulation and Extraction. In the *34th ACM Symposium on the Theory of Computing* (STOC), pages 484–493, 2002.

80. B. Barak, O. Goldreich, S. Goldwasser and Y. Lindell. Resettably-Sound Zero-Knowledge and its Applications. In the *42nd IEEE Symposium on the Foundations of Computer Science* (FOCS), pages 116–125, 2001.

81. Y. Lindell. Parallel Coin-Tossing and Constant-Round Secure Two-Party Computation. In *Advances in Cryptology – CRYPTO 2001*, Springer (LNCS 2139), pages 171–189, 2001.

82. O. Goldreich and Y. Lindell. Session-Key Generation Using Human Passwords Only. In *Advances in Cryptology – CRYPTO 2001*, Springer (LNCS 2139), pages 408–432, 2001.

83. Y. Lindell and B. Pinkas. Privacy Preserving Data Mining. In *Advances in Cryptology – CRYPTO 2000*, Springer (LNCS 1880), pages 36–54, 2000.

84. Y. Aumann and Y. Lindell. A Statistical Theory for Quantitative Association Rules. In the *5th ACM-SIGKDD International Conference on Knowledge Discovery and Data Mining* (KDD), pages 261–270, 1999.

85. D. Landau, R. Feldman, Y. Aumann, M. Fresko, Y. Lindell, O. Lipshtat and O. Zamir, TextVis: An Integrated Visual Environment for Text Mining. In the *2nd European Symposium on Principles of Data Mining and Knowledge Discovery* (PKDD), Springer (LNCS 1510), pages 56–64, 1998.

86. R. Feldman, M. Fresko, Y. Kinar, Y. Lindell, O. Lipshtat, M. Rajman, Y. Schler and O. Zamir. Text Mining at the Term Level. In the *2nd European Symposium on Principles of Data Mining and Knowledge Discovery* (PKDD), Springer (LNCS 1510), pages 65–73, 1998.

Technical Reports

1. Y. Lindell. How To Simulate It - A Tutorial on the Simulation Proof Technique. *Cryptology ePrint Archive,* Report 2016/046, 2016.

2. Y. Ejgenberg, M. Farbstein, M. Levy and Y. Lindell. SCAPI: The Secure Computation Application Programming Interface. *Cryptology ePrint Archive,* Report #2012/629, 2012.

3. C. Hazay and Y. Lindell. A Note on Zero-Knowledge Proofs of Knowledge and the ZKPOK Ideal Functionality. *Cryptology ePrint Archive,* Report #2010/552, 2010.

4. C. Hazay and Y. Lindell. A Note on the Relation between the Definitions of Security for Semi-Honest and Malicious Adversaries. *Cryptology ePrint Archive,* Report #2010/551, 2010.

5. B. Barak, Y. Lindell and T. Rabin. Protocol Initialization for the Framework of Universal Composability. *Cryptology ePrint Archive,* Report #2004/006, 2004.

Graduate Students

Graduated:

- **Ph.D. students:**

  1. Ran Cohen. **Ph.D.**, *Studies on Full Security in Multiparty Computation.* June 2016.
  2. Hila Zarosim. *On the Complexity of Interactive Cryptographic Protocols.* **Ph.D.**, August 2014.
  3. Gilad Asharov. *Foundations of Secure Computation: Perfect Security and Fairness.* **Ph.D.**, March, 2014.
  4. Carmit Hazay. *Efficient Two-Party Computation with Simulation-Based Security.* **Ph.D.**, February 2009.

- **M.Sc. students:**

  1. Or Weinstein. *Better Combinatorics for Cut-and-Choose.* **M.Sc.**, October 2018.
  2. Ariel Nof. *Fast Garbling Of Circuits Under Standard Cryptographic Assumptions.* **M.Sc.**, September 2015.

3. Avishay Yanai. *Concretely Efficient (Constant Round) Protocol for General Secure Multiparty Computation With an Active Adversary.* **M.Sc.**, October 2015.
4. Asaf Cohen. *A Simpler Variant of Universally Composable Security for Standard Multiparty Computation.* **M.Sc.**, October 2014.
5. Tali Oberman. *Secure and Efficient Two-Party Computation for Small Circuits.* **M.Sc.**, September 2013.
6. Eli Oxman. *Efficient Secure Multiparty Computation.* **M.Sc.**, September 2011.
7. Gilad Asharov. *Utility Dependence in Correct and Fair Rational Secret Sharing.* **M.Sc.**, June 2009.
8. Hila Zarosim. *Adaptive Zero-Knowledge Proofs and Adaptively Secure Oblivious Transfer.* **M.Sc.**, October 2008.
9. Dafna Kidron. *Generalized Impossibility Results for Universal Composability: Public-Key Models, Reactive Functionalities and Fixed Inputs.* **M.Sc.**, June 2007.

Current Graduate Students:

1. Ariel Nof. **Ph.D.**, expected to graduate September 2019.
2. Avishay Yanai. **Ph.D.**, expected to graduate September 2019.
3. Hila Dahari. **M.Sc.**, expected to graduate February 2019.

PostDocs

1. Carsten Baum. **Postdoc**, 2016–2018.
2. Ben Riva. **Postdoc** (joint with Benny Pinkas), 2014–2015.
3. Claudio Orlandi. **Postdoc**, 2011–2012.
4. Eran Omri. **PostDoc**, 2009–2012.

Visitors

1. Tal Malkin. September 2013 to August 2014.
2. Arpita Patra. January to March, 2012.
3. Kobbi Nissim. September 2011 to August 2012.

Professional Activities

International Committee Membership:

1. Member of the International Evaluation Panel for the Privacy-Preserving Technologies Initiative of the National Research Foundation of Singapore, 2018.
2. Member of the ERC starting grant panel (PE6 – Computer Science and Informatics), 2017.
3. Member of the ERC starting grant panel (PE6 – Computer Science and Informatics), 2015.

Program Committee Chair:

1. The 11th Theory of Cryptography Conference (TCC), 2014

Program Committee Membership:

1. The 37th Annual Eurocrypt Conference (EUROCRYPT), 2018
2. The 34th Annual Eurocrypt Conference (EUROCRYPT), 2015
3. The 33rd Annual International Cryptology Conference (CRYPTO), 2013
4. The 31st Annual Eurocrypt Conference (EUROCRYPT), 2012
5. The 14th Intl. Conf. on Practice and Theory in Public Key Cryptography (PKC), 2011
6. The 30th Annual International Cryptology Conference (CRYPTO), 2010
7. The 28th Annual International Cryptology Conference (CRYPTO), 2008
8. International Conference on Applied Cryptography and Network Security (ACNS), 2008
9. The 5th Theory of Cryptography Conference (TCC), 2008
10. The 26th Annual International Cryptology Conference (CRYPTO), 2006
11. The 3rd Theory of Cryptography Conference (TCC), 2006
12. The 25th Annual International Cryptology Conference (CRYPTO), 2005
13. The 23rd Annual Eurocrypt Conference (EUROCRYPT), 2004

Workshop Steering Committee: Member of the steering committee for the *Theory and Practice of Multi-Party Computation* Workshop (TPMPC), held annually.

Workshop Organization:

1. The 9th Bar-Ilan Winter School on Cryptography – *Zero Knowledge*, Bar-Ilan University, February 2019.
2. The 8th Bar-Ilan Winter School on Cryptography – *Secure Key Exchange*, Bar-Ilan University, February 2018.
3. The 7th Bar-Ilan Winter School on Cryptography – *Differential Privacy: From Theory to Practice*, Bar-Ilan University, February 2017.
4. The 6th Bar-Ilan Winter School on Cryptography – *Crypto in the Cloud – Verifiable Computation and Special Encryption*, Bar-Ilan University, January 2016.
5. The 5th Bar-Ilan Winter School on Cryptography – *Advances in Practical Multiparty Computation*, Bar-Ilan University, February 2015.
6. The 4th Bar-Ilan Winter School on Cryptography – *Symmetric Encryption in Theory and in Practice*, Bar-Ilan University, January 2014.
7. The 3rd Bar-Ilan Winter School on Cryptography – *Bilinear Pairings in Cryptography*, Bar-Ilan University, February 2013.
8. Working group on *Implementations of Secure Computation Protocols*, Tel-Aviv, November 2012.

9. The 2nd Bar-Ilan Winter School on Cryptography – *Lattice-Based Cryptography and Applications*, Bar-Ilan University, February 2012.

10. The 1st Winter School on *Secure Computation and Efficiency*, Bar-Ilan University, January 2011.

11. Interdisciplinary Workshop on *Privacy – Cryptographic and Public Administration Perspectives.* Bar-Ilan University, April 2007.

Keynote Addresses

1. The 16th International Conference on Practice and Theory in Public Key Cryptography (PKC 2013), Japan. February 2013.

Invited Talks

1. High-Throughput Secure 3PC for Semi-Honest and Malicious Adversaries – Breaking the Billion-Gate per Second Barrier, Theory and Practice of Multiparty Computation Workshop, Bristol, April 2017.

2. High-Throughput Secure Computation, Real World Cryptography, New York, January 2017.

3. Secure Multiparty Computation and Privacy-Preserving Data Mining, Summer School of the EIT ICT Labs Security & Privacy in Digital Life (SPDL), Trento, June 2016.

4. Efficient Constant-Round Multiparty Computation, Theory and Practice of Multiparty Computation Workshop, Aarhus, May 2016.

5. Extremely Fast Authenticated Encryption with Full Protection Against Bad Randomness, Technion Cryptoday, December 2015.

6. Secure Multiparty Computation and Privacy-Preserving Data Mining, Summer School of the EIT ICT Labs Security & Privacy in Digital Life (SPDL), Trento, July 2015.

7. Fast Garbling of Circuits Under Standard Assumptions, Cornell Tech, NY, USA. June 2015.

8. Fast Garbling of Circuits Under Standard Assumptions, Simons Institute Workshop on Secure Computing, Berkeley, USA. June 2015.

9. Dagstuhl – Modern Cryptography and Security: An Inter-Community Dialogue, February 2015.

10. Cut-and-Choose Based Two-Party Computation in the Online/Offline and Batch Settings, Technion Cryptoday, December 2014.

11. Techniques for Efficient Secure Computation Based on Yao's Protocol, IBM Haifa Seminar, September 2014.

12. Secure Multiparty Computation and Privacy-Preserving Data Mining, Summer School of the EIT ICT Labs Security & Privacy in Digital Life (SPDL), Trento, July 2014.

13. Efficient Two-Party Secure Computation for Semi-Honest and Malicious Adversaries, Workshop on Applied Multiparty Computation, Microsoft Research, Redmond, February 2014.

14. Mitigating Server Breach with Secure Computation, The 4th Real-World Cryptography Workshop, New York, USA. January 2014

15. Highly Efficient Secure Two-Party Computation – the Road from Theory to Practice, The 6th Israel CS Theory Day at the Open University, Israel. March 2013.

16. Implementations of Secure Computation Protocols, The Check Point Institute Cryptography and Security Workshop, Tel-Aviv University, December 2012.

17. Advanced Cryptographic Techniques for Cloud Security, Workshop on *Cloud Security*, the National Information Security Authority of the Israeli Security Agency, February 2011.

18. Techniques for Efficient Secure Two-Party Computation with Malicious Adversaries, Check Point Institute *Crypto and Security Day*, Tel-Aviv University, Israel. October 2010.

19. Rational Secret Sharing: Constructions and Limitations, Workshop on the *Economics of Computer Security,* the National Information Security Authority of the Israeli Security Agency, October 2009.

20. Private Data Mining and Citizens' Rights. *CSI SX 2008,* Las Vegas, USA. April 2008.

21. Tutorial on Multiparty Computation and Privacy-Preserving Data Mining. DIMACS Workshop on *Data Privacy,* New Jersey, USA. February 2008.

22. Lecturer at ECRYPT School on Zero-Knowledge, Bertinoro, Italy. October 2006.

23. Information-Theoretically Secure Protocols and Security Under Composition. ECRYPT Workshop on *Models for Cryptographic Protocols*, Aarhus, Denmark. July 2006.

24. Secure Multiparty Computation and Privacy. *Privacy Day*, The Weizmann Institute of Science, Israel. July 2006.

25. Survey on the Secure Composition of Multiparty Protocols. Workshop on *Mathematical Problems and Techniques in Cryptology*, Centre de Recerca Matemàtica, Barcelona, Spain. June 2005.

26. Tutorial on the Secure Composition of Multiparty Protocols. DIMACS Workshop on *Security Analysis of Protocols,* New Jersey, USA. June 2004.

27. Tutorial on Secure Multiparty Computation. Workshop on *Privacy-Preserving Data Mining*, in conjunction with the *3rd IEEE International Conference on Data Mining* (ICDM), Florida, USA. November 2003.