Curriculum Vitae

Carmit Hazay

September 11, 2020

Contact Information

Address:	Department of Computer Engineering Bar-Ilan University Ramat-Gan 52900, Israel
Telephone:	+972-3-738-4672
Email:	carmit.hazay(at)biu.ac.il
Home Page:	http : //www.eng.biu.ac.il/hazay/

Current Position

Associate Professor in the Faculty of Engineering in Bar-Ilan University, Israel.

Research Interests

I am interested in the field of Cryptography, with a focus on secure protocols and their efficiency. This research concentrates on the problem of constructing secure protocols that are both highly efficient and have rigorous proofs of security. In my research I consider different adversarial models and definitions of security, with the aim of obtaining high efficiency and security. My focus is on both theoretical and practical efficiency as well as understanding the bottlenecks in the design of secure protocols.

Education

11/2004 - 2/2009:	*Bar-Ilan University (Ramat Gan, Israel).* **Ph.D. in Computer Science** With Highest Distinction Field of Research: Cryptography Thesis: Efficient Two-Party Computation with Simulation Based Security. Advisor: Yehuda Lindell
9/2002 - 8/2004:	*Bar-Ilan University (Ramat Gan, Israel).* **M.Sc. in Computer Science** Field of Research: Algorithms in Pattern Matching Thesis: Parameterized Matching. Advisor: Moshe Lewenstein
9/1998 - 8/2001:	*Bar-Ilan University (Ramat Gan, Israel).* **B.Sc. in Computer Science and Mathematics** Magna Cum Laude

Employment History

Academic:

8/2010 - 8/2012	Post-Doctoral Researcher	Department of Computer Science, Aarhus University, Aarhus, Denmark.
9/2009 - 8/2010	Post-Doctoral Researcher	Department of Computer Science and Applied Mathematics, Weizmann Institute & IDC, Herzeliya, Israel.
6/2008 - 7/2008	Summer Intern	IBM T. J. Watson Research Center, Hawthorne, NY.

Industrial:

9/2000 - 2/2002	Programmer	Amdocs, Israel.

Awards

Dean's award, 2002 and 2003, Department of Computer Science and Mathematics, Bar-Ilan University, Ramat Gan, Israel.

Fellowships

- Eshkol fellowship, 2006 - 2009, Ministry of Science and Technology, Israel.
- President's fellowship, 2005 - 2009, Department of Computer Science and Mathematics, Bar-Ilan University, Ramat Gan, Israel.

Research Grants

- More Efficient MPC with Malicious Security, Israel Science Foundation, 880,000 NIS (approximately $\$243,000$). Principle investigator, *October 2018-September 2022*.
- Cryptography for Secure Digital Interaction, ICT COST Action IC1306. Management committee member, *April 2014 - March 2018*.
- The Study of Efficient Delegatable Computation, Israel Ministry of Science and Technology of Infrastructures, 1,127,000 NIS (approximately $\$325,000$). Principle investigator, *December 2013-November 2016*.

Book

- **C. Hazay** and Y. Lindell. Efficient Secure Two-Party Protocols – Techniques and Constructions. Springer-Verlag, 2010.

Journal Publications

1. **C. Hazay**, P. Scholl and E. Soria-Vazquez. Low Cost Constant Round MPC Combining BMR and Oblivious Transfer. To appear Journal of Cryptology.
2. **C. Hazay** and M. Venkitasubramaniam. On the Power of Secure Two-Party Computation. In the Journal of Cryptology 33(1): 271-318 (2020).
3. **C. Hazay** and M. Venkitasubramaniam. What Security Can We Achieve within 4 Rounds? In the Journal of Cryptology 32(4): 1200-1262 (2019).

4. **C. Hazay** and A. Yanay. Constant-Round Maliciously Secure Two-Party Computation in the RAM Model. In the Journal of Cryptology 32(4): 1144-1199 (2019).

5. **C. Hazay** and M. Venkitasubramaniam. On Black-Box Complexity of Universally Composable Security in the CRS model. In the Journal of Cryptology 32(3): 635-689 (2019).

6. **C. Hazay**, G. L. Mikkelsen, T. Rabin, T. Toft and A. A. Nicolosi. Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting. In the Journal of Cryptology 32(2): 265-323 (2019).

7. **C. Hazay**. Oblivious Polynomial Evaluation and Secure Set-Intersection from Algebraic PRFs. In the Journal of Cryptology 31(2): 537-586 (2018).

8. S. Faust, **C. Hazay** and D. Venturi. Outsourced Pattern Matching. In the International Journal of Information Security 17(3): 327-346 (2018).

9. **C. Hazay** and A. Patra. One-Sided Adaptively Secure Two-Party Computation. In the Journal of Cryptology 30(1): 321-371 (2017).

10. G. Asharov, R. Canetti and **C. Hazay**. Towards a Game Theoretic View of Secure Computation. In the Journal of Cryptology 29(4): 879-926 (2016).

11. S. Faust, **C. Hazay**, J. B. Nielsen, P. S. Nordholt and A. Zottarel. Signature Schemes Secure against Hard-to-Invert Leakage. In the Journal of Cryptology 29(2): 422-455 (2016).

12. **C. Hazay**, A. Lopez-Alt, H. Wee and D. Wichs. Leakage-Resilient Cryptography from Minimal Assumptions. In the Journal of Cryptology 29(3): 514-551 (2016).

13. M. J. Freedman, **C. Hazay**, K. Nissim and B. Pinkas. Efficient Set Intersection with Simulation-Based Security. In the Journal of Cryptology 29(1): 115-155 (2016).

14. R. Cole, **C. Hazay**, M. Lewenstein and D. Tsur. Two Dimensional Parameterized Matching. In ACM Transactions on Algorithms 11(2): 12:1-12:30 (2014).

15. R. Gennaro, **C. Hazay** and J. Sorensen. Automata Evaluation and Text Search Protocols with Simulation Based Security. In the Journal of Cryptology 29(2): 243-282 (2016).

16. **C. Hazay** and T. Toft. Computationally Secure Pattern Matching in the Presence of Malicious Adversaries. In the Journal of Cryptology 27(2): 358-395 (2014).

17. **C. Hazay**, A. Jagmohan, D. Klinc, H. Krawczyk and T. Rabin. On Compressing Data Encrypted with Block Ciphers. In IEEE Transactions on Information Theory 58(11): 6989-7001 (2012).

18. **C. Hazay** and K. Nissim. Efficient Set Operations in the Presence of Malicious Adversaries. In the Journal of Cryptology 25(3): 383-433 (2012).

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

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. **C. Hazay**, M. Lewenstein and D. Sokol. Approximate Parameterized Matching. In ACM Transactions on Algorithms 3(3): 15, 2007.

Publications in Refereed Conferences

1. M. Chen, **C. Hazay**, Y. Ishai, Y. Kashnikov, D. Micciancio, T. Riviere, a. shelat, M. Venkitasubramaniam and R. Wang. Diogenes: Lightweight Scalable RSA Modulus Generation with a Dishonest Majority. In IEEE Symposium on Security and Privacy (S&P), 2021.

2. J. Abascal, **C. Hazay**, M. H. Faghihi Sereshgi, Y. Ishai and M. Venkitasubramaniam. Is the Classical GMW Paradigm Practical? The Case of Non-Interactive Actively Secure 2PC. In the ACM Conference on Computer and Communications Security (ACM CCS), 2020.

3. R. Bhadauria, Z. Fang, **C. Hazay**, M. Venkitasubramaniam, T. Xie and Y. Zhang. Ligero++: A New Optimized Sublinear IOP. In the ACM Conference on Computer and Communications Security (ACM CCS), 2020.

4. **C. Hazay** and M. Lilintal. Gradual GRAM and Secure Computation for RAM Programs. In the Conference on Security and Cryptography for Networks (SCN), Springer-Verlag (LNCS 12238), pages 233-252, 2020.

5. R. Bhadauria and **C. Hazay**. Multi-Clients Verifiable Computation via Conditional Disclosure of Secrets. In the Conference on Security and Cryptography for Networks (SCN), Springer-Verlag (LNCS 12238), pages 150-172, 2020.

6. **C. Hazay**, A. Shelat and M. Venkitasubramaniam. Going Beyond Dual Execution: MPC for Functions with Efficient Verification. In Public Key Cryptography (PKC) Springer-Verlag (LNCS 12111), pages 328-356, 2020.

7. **C. Hazay**, R. Pass and M. Venkitasubramaniam. Which Languages Have 4-Round Fully Black-Box Zero-Knowledge Arguments from One-Way Functions? In EUROCRYPT Springer-Verlag (LNCS 12106), pages 599-619, 2020.

8. **C. Hazay**, M. Venkitasubramaniam and M. Weiss. The Price of Active Security in Cryptographic Protocols. In EUROCRYPT Springer-Verlag (LNCS 12106), pages 184-215, 2020.

9. **C. Hazay**, A. Marcedone, Y. Ishai and M. Venkitasubramaniam. LevioSA: Lightweight Secure Arithmetic Computation. In the ACM Conference on Computer and Communications Security (ACM CCS), pages 327-344, 2019.

10. M. Byali, **C. Hazay**, A. Patra and S. Singla. Fast Actively Secure Five-Party Computation with Security Beyond Abort. In the ACM Conference on Computer and Communications Security (ACM CCS), pages 1573-1590, 2019.

11. **C. Hazay**, E. Orsini, P. Scholl and E. Soria-Vazquez. Concretely Efficient Large-Scale MPC with Active Security (or, TinyKeys for TinyOT). In ASIACRYPT, Springer-Verlag (LNCS 11274), pages 86-117, 2018.

12. **C. Hazay** and M. Venkitasubramaniam. Round-Optimal Fully Black-Box Zero-Knowledge Arguments from One-Way Permutations. In TCC, Springer-Verlag (LNCS 11239), pages 263-285, 2018.

13. S. Halevi, **C. Hazay**, A. Polychroniadou and M. Venkitasubramaniam. Round-Optimal Secure Multi-Party Computation. In CRYPTO, Springer-Verlag (LNCS 10993), pages 488-520, 2018.

14. **C. Hazay**, E. Orsini, P. Scholl and E. Soria-Vazquez. TinyKeys: A New Approach to Efficient Multi-Party Computation. In CRYPTO, Springer-Verlag (LNCS 10993), pages 3-33, 2018.

15. **C. Hazay**, Y. Ishai, M. Venkitasubramaniam. Actively Secure Garbled Circuits with Constant Communication Overhead in the Plain Model. In the Theory of Cryptography Conference (TCC), Springer-Verlag (LNCS 10678), pages 3-39, 2017.

16. **C. Hazay**, P. Scholl and E. Soria-Vazquez. Low Cost Constant Round MPC Combining BMR and Oblivious Transfer. In ASIACRYPT, Springer-Verlag (LNCS 10624), pages 598-628, 2017.

17. S. Ames, **C. Hazay**, Y. Ishai, M. Venkitasubramaniam. Ligero: Lightweight Sublinear Arguments Without a Trusted Setup. In the ACM Conference on Computer and Communications Security (ACM CCS), pages 2087-2104 2017.

18. **C. Hazay** and M. Venkitasubramaniam. Scalable Multi-Party Private Set-Intersection. In Public Key Cryptography (PKC), Springer-Verlag (LNCS 10174), pages 175-203, 2017.

19. **C. Hazay**, A. Polychroniadou and M. Venkitasubramaniam. Constant-Round Adaptively Secure Protocols in the Tamper-Proof Hardware Model. In Public Key Cryptography (PKC), Springer-Verlag (LNCS 10175), pages 428-460, 2017.

20. **C. Hazay** and A. Yanay. Constant-Round Maliciously Secure Two-Party Computation in the RAM Model. In the Theory of Cryptography Conference (TCC-B), Springer-Verlag (LNCS 9985), pages 521-553, 2016.

21. **C. Hazay** and M. Venkitasubramaniam. Composable Adaptive Secure Protocols without Setup under Polytime Assumptions. In the Theory of Cryptography Conference (TCC-B), Springer-Verlag (LNCS 9985), pages 400-432, 2016.

22. **C. Hazay**, A. Polychroniadou and M. Venkitasubramaniam. Composable Security in the Tamper-Proof Hardware Model under Minimal Complexity. In the Theory of Cryptography Conference (TCC-B), Springer-Verlag (LNCS 9985), pages 367-399, 2016.

23. **C. Hazay** and M. Venkitasubramaniam. What Security Can We Achieve within 4 Rounds? In the Conference on Security and Cryptography for Networks (SCN), pages 486-505, 2016.

24. **C. Hazay** and H. Zarosim. The Feasibility of Outsourced Database Search in the Plain Model. In the Conference on Security and Cryptography for Networks (SCN), pages 313-332, 2016.

25. **C. Hazay** and M. Venkitasubramaniam. On the Power of Secure Two-Party Computation. In CRYPTO, Springer-Verlag (LNCS 9815), pages 397-429, 2016.

26. **C. Hazay**, A. Patra and B. Warinschi. Selective Opening Security for Receivers. In ASIACRYPT, Springer-Verlag (LNCS 9453), pages 443-469, 2015.

27. **C. Hazay** and M. Venkitasubramaniam. On Black-Box Complexity of Universally Composable Security in the CRS model. In ASIACRYPT, Springer-Verlag (LNCS 9453), pages 183-209, 2015.

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

29. **C. Hazay**. Oblivious Polynomial Evaluation and Secure Set-Intersection from Algebraic PRFs. In the Theory of Cryptography Conference (TCC), Springer-Verlag (LNCS 9015), pages 90-120, 2015.

30. **C. Hazay** and A. Patra. One-Sided Adaptively Secure Two-Party Computation. In the Theory of Cryptography Conference (TCC), Springer-Verlag (LNCS 8349), pages 368-393, 2014.

31. S. Faust, **C. Hazay** and D. Venturi. Outsourced Pattern Matching. In ICALP, Springer-Verlag (LNCS 7966), pages 545-556, 2013.

32. **C. Hazay**, A. Lopez-Alt, H. Wee and D. Wichs. Leakage-Resilient Cryptography from Minimal Assumptions. In EUROCRYPT, Springer-Verlag (LNCS 7658), pages 160-176, 2013.

33. S. Faust, **C. Hazay**, J. B. Nielsen, P. S. Nordholt and A. Zottarel. Signature Schemes Secure against Hard-to-Invert Leakage. In ASIACRYPT, Springer-Verlag (LNCS 7658), pages 98-115, 2012.

34. A. Akavia, S. Goldwasser and **C. Hazay**. Distributed Public Key Schemes Secure against Continual Leakage. In PODC, pages 155-164, 2012.

35. I. Damgård, S. Faust and **C. Hazay**. Secure Two-Party Computation with Low Communication. In the Theory of Cryptography Conference (TCC), Springer-Verlag (LNCS 7194), pages 54-74, 2012.

36. **C. Hazay**, G. L. Mikkelsen, T. Rabin and T. Toft. Efficient RSA Key Generation and Threshold Paillier in the Two-Party Setting. In CT-RSA, Springer-Verlag (LNCS 7178), pages 313-331, 2012.

37. G. Asharov, R. Canetti and **C. Hazay**. Towards a Game Theoretic View of Secure Computation. In EUROCRYPT, Springer-Verlag (LNCS 6632), pages 426-445, 2011.

38. **C. Hazay** and T. Toft. Computationally Secure Pattern Matching in the Presence of Malicious Adversaries. In ASIACRYPT, Springer-Verlag (LNCS 6477), pages 195-212, 2010.

39. R. Gennaro, **C. Hazay** and J. Sorensen. Text Search Protocols with Simulation Based Security. In Public Key Cryptography (PKC), pages 332-350, 2010.

40. **C. Hazay** and K. Nissim. Efficient Set Operations in the Presence of Malicious Adversaries. In Public Key Cryptography (PKC), pages 312-331, 2010.

41. **C. Hazay**, A. Jagmohan, D. Klinc, H. Krawczyk and T. Rabin. On Compressing Data Encrypted with Block Ciphers. In Data Compression Conference, 213-222, 2009.

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

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

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

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

46. **C. Hazay**, M. Lewenstein and D. Tzur. Faster Algorithm for 2D parameterized Matching. In the Symposium on Combinatorial Pattern Matching (CPM). pages 266-279, 2005.

47. **C. Hazay**, M. Lewenstein and D. Sokol. Approximate parameterized matching. In the European Symposium on Algorithms (ESA), pages 414-425, 2004.

Technical Reports

1. **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.

2. **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.

3. **C. Hazay** and Y. Lindell. Efficient Oblivious Polynomial Evaluation with Simulation-Based Security. Cryptology ePrint Archive, Report #2009/459, 2009.

Other Publications

- **C. Hazay**. Secure Two-Party Computation. Galileo Magazine, Bar-Ilan University, February 2010.

Patents

- **C. Hazay**, A. Jagmohan, D. Klinc, H. Krawczyk and T. Rabin. Compressing encrypted data without the encryption key. US patent 20110103580, May 2011.

Professional Activities

Program Committee Membership:

1. The Cryptographer's Track at the RSA Conference (CT-RSA), 2021.
2. The International Conference on Cryptology in India (Indocrypt), 2021.
3. The International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), 2020.
4. ACM Conference on Computer and Communications Security (ACM CCS), 2019.
5. The International Cryptography Conference (CRYPTO), 2019.
6. The International Symposium on Cyber Security Cryptography and Machine Learning (CSCML), 2018.
7. The Conference on Security and Cryptography for Networks (SCN), 2018.
8. The International Conference on Practice and Theory in Public Key Cryptography (PKC), 2018.
9. The International Conference on Cryptology in India (Indocrypt), 2017.
10. Theory of Cryptography Conference (TCC), 2017.
11. The International Conference on Practice and Theory in Public Key Cryptography (PKC), 2017.
12. The International Conference on Cryptology in India (Indocrypt), 2016.
13. The International Conference on Information Theoretic Security (ICITS), 2016.
14. The International Cryptography Conference (CRYPTO), 2015.
15. The International Conference on Practice and Theory in Public Key Cryptography (PKC), 2015.
16. The International Conference on Practice and Theory in Public Key Cryptography (PKC), 2013.
17. The Nordic Conference on Secure IT Systems (NordSec), 2012.
18. The International Conference on Practice and Theory in Public Key Cryptography (PKC), 2011.
19. The International Cryptography Conference (CRYPTO), 2010.

Workshop Organization:

- Workshops chair, The International Cryptography Conference (CRYPTO), August 2021.
- Workshops chair, The International Cryptography Conference (CRYPTO), August 2020.
- Bar-Ilan Winder School on Information Theoretic Cryptography. Bar-Ilan university, Israel, February 2020.
- Workshops chair, The International Cryptography Conference (CRYPTO), August 2019.
- Workshop on Secure Computation Theory and Applications. Aarhus University, Denmark, June 2012.

Graduate Students

Current:

- Rishabh Bhadauria. **Ph.D.** expected to graduate October 2022.
- Efrat Cohen. **M.Sc.** expected to graduate October 2021.

Graduated:

- Mor Lilintal. **M.Sc.** graduated February 2019.
- Avishay Yanay. **Ph.D.** (joint with Yehuda Lindell), graduated July 2019.
- Raviv Moses. **M.Sc.** graduated September 2019.