Carmit Hazay, Professor
Faculty of Engineering, Bar-Ilan University

carmit.hazay@biu.ac.il
https://www.eng.biu.ac.il/hazay/



Education

2004 – 2009 **Ph.D., Computer Science, Bar-Ilan University** With Highest Distinction.
Thesis title: *Efficient Two-Party Computation with Simulation Based Security.*
Advisor: Yehuda Lindell

2002 – 2004 **M.Sc. Computer Science, Bar-Ilan University**
Thesis title: *Parameterized Matching.*
Advisor: Moshe Lewenstein

1998 – 2001 **B.Sc. Computer Science and Mathematics, Bar-Ilan University** Magna Cum Laude.

Employment History

2022 – current **Professor.** Faculty of Engineering, Bar-Ilan University, Ramat-Gan, Israel

2016 – 2022 **Associate Professor.** Faculty of Engineering, Bar-Ilan University, Ramat-Gan, Israel

2012 – 2016 **Senior Lecturer.** Faculty of Engineering, Bar-Ilan University, Ramat-Gan, Israel

2010 – 2012 **Post-Doctoral Researcher.** Department of Computer Science, Aarhus University, Aarhus, Denmark

2009 – 2010 **Post-Doctoral Researcher.** Department of Computer Science and Applied Mathematics, Weizmann Institute & IDC, Herzeliya, Israel

2008 **Summer Intern.** IBM T. J. Watson Research Center, Hawthorne, NY

Research Publications

Journal Articles

1. Hazay, C., Venkitasubramaniam, M., & Weiss, M. (2025). Protecting distributed primitives against leakage: Equivocal secret sharing and more. *J. Cryptol.*, *38*(1), 1. doi:10.1007/S00145-024-09524-3

2. Hazay, C., Venkitasubramaniam, M., & Weiss, M. (2024). The price of active security in cryptographic protocols. *J. Cryptol.*, *37*(3), 30. doi:10.1007/S00145-024-09509-2

3. Ames, S., Hazay, C., Ishai, Y., & Venkitasubramaniam, M. (2023). Ligero: Lightweight sublinear arguments without a trusted setup. *Des. Codes Cryptogr.*, *91*(11), 3379–3424. doi:10.1007/S10623-023-01222-8

4. Hazay, C., Ishai, Y., & Venkitasubramaniam, M. (2023). Actively secure garbled circuits with constant communication overhead in the plain model. *J. Cryptol.*, *36*(3), 26. doi:10.1007/s00145-023-09465-3

5. Levi, I., & Hazay, C. (2023). Garbled circuits from an SCA perspective free XOR can be quite expensive. . *IACR Trans. Cryptogr. Hardw. Embed. Syst.*, *2023*(2), 54–79. doi:10.46586/tches.v2023.i2.54-79

6. Gordon, S. D., Hazay, C., & Le, P. H. (2022). Fully secure PSI via mpc-in-the-head. *Proc. Priv. Enhancing Technol.*, *2022*(3), 291–313. doi:10.56553/popets-2022-0073

7. Hazay, C., & Lilintal, M. (2022). Gradual GRAM and secure computation for RAM programs. *J. Comput. Secur.*, *30*(1), 197–229. doi:10.3233/JCS-200107

8. Hazay, C., Orsini, E., Scholl, P., & Soria-Vazquez, E. (2022). Tinykeys: A new approach to efficient multi-party computation. *J. Cryptol.*, *35*(2), 13. doi:10.1007/s00145-022-09423-5

9. Hazay, C., Venkitasubramaniam, M., & Weiss, M. (2022b). Zk-pcps from leakage-resilient secret sharing. *J. Cryptol.*, *35*(4), 23. doi:10.1007/s00145-022-09433-3

10. Halevi, S., Hazay, C., Polychroniadou, A., & Venkitasubramaniam, M. (2021). Round-optimal secure multi-party computation. *J. Cryptol.*, *34*(3), 19. doi:10.1007/s00145-021-09382-3

11. Hazay, C., Scholl, P., & Soria-Vazquez, E. (2020). Low cost constant round MPC combining BMR and oblivious transfer. *J. Cryptol.*, *33*(4), 1732–1786. doi:10.1007/s00145-020-09355-y

12. Hazay, C., & Venkitasubramaniam, M. (2020). On the power of secure two-party computation. *J. Cryptol.*, *33*(1), 271–318. doi:10.1007/s00145-019-09314-2

13. Hazay, C., Mikkelsen, G. L., Rabin, T., Toft, T., & Nicolosi, A. A. (2019). Efficient RSA key generation and threshold paillier in the two-party setting. *J. Cryptol.*, *32*(2), 265–323. doi:10.1007/s00145-017-9275-7

14. Hazay, C., & Venkitasubramaniam, M. (2019a). On black-box complexity of universally composable security in the CRS model. *J. Cryptol.*, *32*(3), 635–689. doi:10.1007/s00145-019-09326-y

15. Hazay, C., & Venkitasubramaniam, M. (2019b). What security can we achieve within 4 rounds? *J. Cryptol.*, *32*(4), 1200–1262. doi:10.1007/s00145-019-09323-1

16. Hazay, C., & Yanai, A. (2019). Constant-round maliciously secure two-party computation in the RAM model. *J. Cryptol.*, *32*(4), 1144–1199. doi:10.1007/s00145-019-09321-3

17. Faust, S., Hazay, C., & Venturi, D. (2018). Outsourced pattern matching. *Int. J. Inf. Sec.*, *17*(3), 327–346. doi:10.1007/s10207-017-0374-0

18. Hazay, C. (2018). Oblivious polynomial evaluation and secure set-intersection from algebraic prfs. *J. Cryptol.*, *31*(2), 537–586. doi:10.1007/s00145-017-9263-y

19. Hazay, C., & Patra, A. (2017). Efficient one-sided adaptively secure computation. *J. Cryptol.*, *30*(1), 321–371. doi:10.1007/s00145-015-9222-4

20. Asharov, G., Canetti, R., & Hazay, C. (2016). Toward a game theoretic view of secure computation. *J. Cryptol.*, *29*(4), 879–926. doi:10.1007/s00145-015-9212-6

21. Faust, S., Hazay, C., Nielsen, J. B., Nordholt, P. S., & Zottarel, A. (2016). Signature schemes secure against hard-to-invert leakage. *J. Cryptol.*, *29*(2), 422–455. doi:10.1007/s00145-015-9197-1

22. Freedman, M. J., Hazay, C., Nissim, K., & Pinkas, B. (2016). Efficient set intersection with simulation-based security. *J. Cryptol.*, *29*(1), 115–155. doi:10.1007/s00145-014-9190-0

23. Gennaro, R., Hazay, C., & Sorensen, J. S. (2016). Automata evaluation and text search protocols with simulation-based security. *J. Cryptol.*, *29*(2), 243–282. doi:10.1007/s00145-014-9193-x

24. Hazay, C., López-Alt, A., Wee, H., & Wichs, D. (2016). Leakage-resilient cryptography from minimal assumptions. *J. Cryptol.*, *29*(3), 514–551. doi:10.1007/s00145-015-9200-x

25. Cole, R., Hazay, C., Lewenstein, M., & Tsur, D. (2014). Two-dimensional parameterized matching. *ACM Trans. Algorithms*, *11*(2), 12:1–12:30. doi:10.1145/2650220

26. Hazay, C., & Toft, T. (2014). Computationally secure pattern matching in the presence of malicious adversaries. *J. Cryptol.*, *27*(2), 358–395. doi:10.1007/s00145-013-9147-8

27. Hazay, C., & Nissim, K. (2012). Efficient set operations in the presence of malicious adversaries. *J. Cryptol.*, *25*(3), 383–433. doi:10.1007/s00145-011-9098-x

28. Klinc, D., Hazay, C., Jagmohan, A., Krawczyk, H., & Rabin, T. (2012). On compression of data encrypted with block ciphers. *IEEE Trans. Inf. Theory*, *58*(11), 6989–7001. doi:10.1109/TIT.2012.2210752

29 Gordon, S. D., Hazay, C., Katz, J., & Lindell, Y. (2011). Complete fairness in secure two-party computation. *J. ACM*, *58*(6), 24:1–24:37. doi:10.1145/2049697.2049698

30 Hazay, C., & Lindell, Y. (2010a). Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries. *J. Cryptol.*, *23*(3), 422–456. doi:10.1007/s00145-008-9034-x

31 Hazay, C., Lewenstein, M., & Sokol, D. (2007). Approximate parameterized matching. *ACM Trans. Algorithms*, *3*(3), 29. doi:10.1145/1273340.1273345

Conference Proceedings

1 Couteau, G., Hazay, C., Hegde, A., & Kumar, N. (2025a). Breaking the $1/\lambda$-rate barrier for arithmetic garbling. In S. Fehr & P. Fouque (Eds.), *Advances in cryptology - EUROCRYPT 2025 - 44th annual international conference on the theory and applications of cryptographic techniques, madrid, spain, may 4-8, 2025, proceedings, part VI* (Vol. 15606, pp. 182–213). doi:10.1007/978-3-031-91095-1_7

2 Couteau, G., Hazay, C., Hegde, A., & Kumar, N. (2025b). ømega ($1/\lambda$)-rate boolean garbling scheme from generic groups. In Y. T. Kalai & S. F. Kamara (Eds.), *Advances in cryptology - CRYPTO 2025 - 45th annual international cryptology conference, santa barbara, ca, usa, august 17-21, 2025, proceedings, part IV* (Vol. 16003, pp. 489–521). doi:10.1007/978-3-032-01884-7_16

3 Faust, S., Hazay, C., Kretzler, D., Rometsch, L., & Schlosser, B. (2025). Non-interactive threshold BBS+ from pseudorandom correlations. In A. Patra (Ed.), *Topics in cryptology - CT-RSA 2025 - cryptographers' track at the RSA conference 2025, san francisco, ca, usa, april 28-may 1, 2025, proceedings* (Vol. 15598, pp. 198–222). doi:10.1007/978-3-031-88661-4_9

4 Acharya, A., Hazay, C., Kolesnikov, V., & Prabhakaran, M. (2024). Malicious security for SCALES: outsourced computation with ephemeral servers. In *Advances in cryptology - CRYPTO 2024 - 44th annual international cryptology conference*.

5 Albouy, T., Frey, D., Gelles, R., Hazay, C., Raynal, M., Schiller, E. M., … Zikas, V. (2024a). Brief announcement: Towards optimal communication byzantine reliable broadcast under a message adversary. In D. Alistarh (Ed.), *38th international symposium on distributed computing, DISC 2024, october 28 to november 1, 2024, madrid, spain* (Vol. 319, 41:1–41:7). doi:10.4230/LIPICS.DISC.2024.41

6 Albouy, T., Frey, D., Gelles, R., Hazay, C., Raynal, M., Schiller, E. M., … Zikas, V. (2024b). Near-optimal communication byzantine reliable broadcast under a message adversary. In S. Bonomi, L. Galletta, E. Rivière, & V. Schiavoni (Eds.), *28th international conference on principles of distributed systems, OPODIS 2024, december 11-13, 2024, lucca, italy* (Vol. 324, 14:1–14:29). doi:10.4230/LIPICS.OPODIS.2024.14

7 Berti, F., Hazay, C., & Levi, I. (2024). Sflr-sfot: Leakage-resilient oblivious transfer. In *SCN* (pp. 182–204).

8 Hazay, C., Heath, D., Kolesnikov, V., Venkitasubramaniam, M., & Yang, Y. (2024). Logrobin++: Optimizing proofs of disjunctive statements in vole-based zk. In *Advances in cryptology - ASIACRYPT 2024 - 30th international conference*.

9 Hazay, C., Venkitasubramaniam, M., & Wang, R. (2024). Ligetron: Lightweight scalable end-to-end zero-knowledge proofs. post-quantum zk-snarks on a browser. In *IEEE symposium on security and privacy, SP*.

10 Hazay, C., & Yang, Y. (2024). Toward malicious constant-rate 2pc via arithmetic garbling. In M. Joye & G. Leander (Eds.), *Advances in cryptology - EUROCRYPT 2024 - 43rd annual international conference on the theory and applications of cryptographic techniques, zurich, switzerland, may 26-30, 2024, proceedings, part V* (Vol. 14655, pp. 401–431). doi:10.1007/978-3-031-58740-5_14

11 Yang, Y., Heath, D., Hazay, C., Kolesnikov, V., & Venkitasubramaniam, M. (2024). Tight ZK CPU: batched ZK branching with cost proportional to evaluated instruction. In *Proceedings of the 2024 ACM SIGSAC conference on computer and communications security, CCS*.

12 Acharya, A., Ashur, T., Cohen, E., Hazay, C., & Yanai, A. (2023). A new approach to garbled circuits. In M. Tibouchi & X. Wang (Eds.), *Applied cryptography and network security - 21st international conference, ACNS 2023, kyoto, japan, june 19-22, 2023, proceedings, part II* (Vol. 13906, pp. 611–641). doi:10.1007/978-3-031-33491-7_23

13 Acharya, A., Hazay, C., Poburinnaya, O., & Venkitasubramaniam, M. (2023). Best of both worlds - revisiting the spymasters double agent problem. In H. Handschuh & A. Lysyanskaya (Eds.), *Advances in cryptology - CRYPTO 2023 - 43rd annual international cryptology conference, CRYPTO 2023, santa barbara, ca, usa, august 20-24, 2023, proceedings, part I* (Vol. 14081, pp. 328–359). doi:10.1007/978-3-031-38557-5_11

14 Bangalore, L., Sereshgi, M. H. F., Hazay, C., & Venkitasubramaniam, M. (2023). Flag: A framework for lightweight robust secure aggregation. In J. K. Liu, Y. Xiang, S. Nepal, & G. Tsudik (Eds.), *Proceedings of the 2023 ACM asia conference on computer and communications security, ASIA CCS 2023, melbourne, vic, australia, july 10-14, 2023* (pp. 14–28). doi:10.1145/3579856.3595805

15 Bhadauria, R., Hazay, C., Venkitasubramaniam, M., Wu, W., & Zhang, Y. (2023). Private polynomial commitments and applications to MPC. In A. Boldyreva & V. Kolesnikov (Eds.), *Public-key cryptography - PKC 2023 - 26th IACR international conference on practice and theory of public-key cryptography, atlanta, ga, usa, may 7-10, 2023, proceedings, part II* (Vol. 13941, pp. 127–158). doi:10.1007/978-3-031-31371-4_5

16 Faust, S., Hazay, C., Kretzler, D., & Schlosser, B. (2023a). Putting the online phase on a diet: Covert security from short macs. In M. Rosulek (Ed.), *Topics in cryptology - CT-RSA 2023 - cryptographers' track at the RSA conference 2023, san francisco, ca, usa, april 24-27, 2023, proceedings* (Vol. 13871, pp. 360–386). doi:10.1007/978-3-031-30872-7_14

17 Faust, S., Hazay, C., Kretzler, D., & Schlosser, B. (2023b). Statement-oblivious threshold witness encryption. In *36th IEEE computer security foundations symposium, CSF 2023, dubrovnik, croatia, july 10-14, 2023* (pp. 17–32). doi:10.1109/CSF57540.2023.00026

18 Hazay, C., Venkitasubramaniam, M., & Weiss, M. (2023a). Beyond mpc-in-the-head: Black-box constructions of short zero-knowledge proofs (invited to journal of cryptology). In G. N. Rothblum & H. Wee (Eds.), *Theory of cryptography - 21st international conference, TCC 2023, taipei, taiwan, november 29 - december 2, 2023, proceedings, part I* (Vol. 14369, pp. 3–33). doi:10.1007/978-3-031-48615-9_1

19 Hazay, C., Venkitasubramaniam, M., & Weiss, M. (2023b). Your reputation's safe with me: Framing-free distributed zero-knowledge proofs. In G. N. Rothblum & H. Wee (Eds.), *Theory of cryptography - 21st international conference, TCC 2023, taipei, taiwan, november 29 - december 2, 2023, proceedings, part I* (Vol. 14369, pp. 34–64). doi:10.1007/978-3-031-48615-9_2

20 Yang, Y., Heath, D., Hazay, C., Kolesnikov, V., & Venkitasubramaniam, M. (2023). Batchman and robin: Batched and non-batched branching for interactive ZK (ccs 2023 distinguished paper award). In W. Meng, C. D. Jensen, C. Cremers, & E. Kirda (Eds.), *Proceedings of the 2023 ACM SIGSAC conference on computer and communications security, CCS 2023, copenhagen, denmark, november 26-30, 2023* (pp. 1452–1466). doi:10.1145/3576915.3623169

21 Acharya, A., Hazay, C., Kolesnikov, V., & Prabhakaran, M. (2022). SCALES - MPC with small clients and larger ephemeral servers. In E. Kiltz & V. Vaikuntanathan (Eds.), *Theory of cryptography - 20th international conference, TCC 2022, chicago, il, usa, november 7-10, 2022, proceedings, part II* (Vol. 13748, pp. 502–531). doi:10.1007/978-3-031-22365-5_18

22 Bangalore, L., Bhadauria, R., Hazay, C., & Venkitasubramaniam, M. (2022). On black-box constructions of time and space efficient sublinear arguments from symmetric-key primitives. In E. Kiltz & V. Vaikuntanathan (Eds.), *Theory of cryptography - 20th international conference, TCC 2022, chicago, il, usa, november 7-10, 2022, proceedings, part I* (Vol. 13747, pp. 417–446). doi:10.1007/978-3-031-22318-1_15

23 Chandran, G. R., Hazay, C., Hundt, R., & Schneider, T. (2022). Comparison-based MPC in star topology. In S. D. C. di Vimercati & P. Samarati (Eds.), *Proceedings of the 19th international conference on security*

and cryptography, SECRYPT 2022, lisbon, portugal, july 11-13, 2022 (pp. 69–82). doi:10.5220/0011144100003283

24 de Castro, L., Hazay, C., Ishai, Y., Vaikuntanathan, V., & Venkitasubramaniam, M. (2022). Asymptotically quasi-optimal cryptography. In O. Dunkelman & S. Dziembowski (Eds.), *Advances in cryptology - EUROCRYPT 2022 - 41st annual international conference on the theory and applications of cryptographic techniques, trondheim, norway, may 30 - june 3, 2022, proceedings, part I* (Vol. 13275, pp. 303–334). doi:10.1007/978-3-031-06944-4_11

25 Faust, S., Hazay, C., Kretzler, D., & Schlosser, B. (2022). Financially backed covert security. In G. Hanaoka, J. Shikata, & Y. Watanabe (Eds.), *Public-key cryptography - PKC 2022 - 25th IACR international conference on practice and theory of public-key cryptography, virtual event, march 8-11, 2022, proceedings, part II* (Vol. 13178, pp. 99–129). doi:10.1007/978-3-030-97131-1_4

26 Hazay, C., Venkitasubramaniam, M., & Weiss, M. (2022a). Protecting distributed primitives against leakage: Equivocal secret sharing and more. In D. Dachman-Soled (Ed.), *3rd conference on information-theoretic cryptography, ITC 2022, july 5-7, 2022, cambridge, ma, USA* (Vol. 230, 3:1–3:24). doi:10.4230/LIPIcs.ITC.2022.3

27 Chen, M., Hazay, C., Ishai, Y., Kashnikov, Y., Micciancio, D., Riviere, T., … Wang, R. (2021). Diogenes: Lightweight scalable RSA modulus generation with a dishonest majority. In *42nd IEEE symposium on security and privacy, SP 2021, san francisco, ca, usa, 24-27 may 2021* (pp. 590–607). doi:10.1109/SP40001.2021.00025

28 Faust, S., Hazay, C., Kretzler, D., & Schlosser, B. (2021). Generic compiler for publicly verifiable covert multi-party computation. In A. Canteaut & F. Standaert (Eds.), *Advances in cryptology - EUROCRYPT 2021 - 40th annual international conference on the theory and applications of cryptographic techniques, zagreb, croatia, october 17-21, 2021, proceedings, part II* (Vol. 12697, pp. 782–811). doi:10.1007/978-3-030-77886-6_27

29 Hazay, C., Venkitasubramaniam, M., & Weiss, M. (2021). Zk-pcps from leakage-resilient secret sharing. In S. Tessaro (Ed.), *2nd conference on information-theoretic cryptography, ITC 2021, july 23-26, 2021, virtual conference* (Vol. 199, 6:1–6:21). doi:10.4230/LIPIcs.ITC.2021.6

30 Abascal, J., Sereshgi, M. H. F., Hazay, C., Ishai, Y., & Venkitasubramaniam, M. (2020). Is the classical GMW paradigm practical? the case of non-interactive actively secure 2pc. In J. Ligatti, X. Ou, J. Katz, & G. Vigna (Eds.), *CCS '20: 2020 ACM SIGSAC conference on computer and communications security, virtual event, usa, november 9-13, 2020* (pp. 1591–1605). doi:10.1145/3372297.3423366

31 Bhadauria, R., Fang, Z., Hazay, C., Venkitasubramaniam, M., Xie, T., & Zhang, Y. (2020). Ligero++: A new optimized sublinear IOP. In J. Ligatti, X. Ou, J. Katz, & G. Vigna (Eds.), *CCS '20: 2020 ACM SIGSAC conference on computer and communications security, virtual event, usa, november 9-13, 2020* (pp. 2025–2038). doi:10.1145/3372297.3417893

32 Bhadauria, R., & Hazay, C. (2020). Multi-clients verifiable computation via conditional disclosure of secrets. In C. Galdi & V. Kolesnikov (Eds.), *Security and cryptography for networks - 12th international conference, SCN 2020, amalfi, italy, september 14-16, 2020, proceedings* (Vol. 12238, pp. 150–171). doi:10.1007/978-3-030-57990-6_8

33 Hazay, C., & Lilintal, M. (2020). Gradual GRAM and secure computation for RAM programs (invited to journal of computer security). In C. Galdi & V. Kolesnikov (Eds.), *Security and cryptography for networks - 12th international conference, SCN 2020, amalfi, italy, september 14-16, 2020, proceedings* (Vol. 12238, pp. 233–252). doi:10.1007/978-3-030-57990-6_12

34 Hazay, C., Pass, R., & Venkitasubramaniam, M. (2020). Which languages have 4-round fully black-box zero-knowledge arguments from one-way functions? In A. Canteaut & Y. Ishai (Eds.), *Advances in cryptology - EUROCRYPT 2020 - 39th annual international conference on the theory and applications of cryptographic techniques, zagreb, croatia, may 10-14, 2020, proceedings, part III* (Vol. 12107, pp. 599–619). doi:10.1007/978-3-030-45727-3_20

35 Hazay, C., Shelat, A., & Venkitasubramaniam, M. (2020). Going beyond dual execution: MPC for functions with efficient verification. In A. Kiayias, M. Kohlweiss, P. Wallden, & V. Zikas (Eds.), *Public-key cryptography - PKC 2020 - 23rd IACR international conference on practice and theory of public-key cryptography, edinburgh, uk, may 4-7, 2020, proceedings, part II* (Vol. 12111, pp. 328–356). doi:10.1007/978-3-030-45388-6_12

36 Hazay, C., Venkitasubramaniam, M., & Weiss, M. (2020). The price of active security in cryptographic protocols. In A. Canteaut & Y. Ishai (Eds.), *Advances in cryptology - EUROCRYPT 2020 - 39th annual international conference on the theory and applications of cryptographic techniques, zagreb, croatia, may 10-14, 2020, proceedings, part II* (Vol. 12106, pp. 184–215). doi:10.1007/978-3-030-45724-2_7

37 Byali, M., Hazay, C., Patra, A., & Singla, S. (2019). Fast actively secure five-party computation with security beyond abort. In L. Cavallaro, J. Kinder, X. Wang, & J. Katz (Eds.), *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, CCS 2019, london, uk, november 11-15, 2019* (pp. 1573–1590). doi:10.1145/3319535.3345657

38 Hazay, C., Ishai, Y., Marcedone, A., & Venkitasubramaniam, M. (2019). Leviosa: Lightweight secure arithmetic computation. In L. Cavallaro, J. Kinder, X. Wang, & J. Katz (Eds.), *Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, CCS 2019, london, uk, november 11-15, 2019* (pp. 327–344). doi:10.1145/3319535.3354258

39 Halevi, S., Hazay, C., Polychroniadou, A., & Venkitasubramaniam, M. (2018). Round-optimal secure multi-party computation. In H. Shacham & A. Boldyreva (Eds.), *Advances in cryptology - CRYPTO 2018 - 38th annual international cryptology conference, santa barbara, ca, usa, august 19-23, 2018, proceedings, part II* (Vol. 10992, pp. 488–520). doi:10.1007/978-3-319-96881-0_17

40 Hazay, C., Orsini, E., Scholl, P., & Soria-Vazquez, E. (2018a). Concretely efficient large-scale MPC with active security (or, tinykeys for tinyot). In T. Peyrin & S. D. Galbraith (Eds.), *Advances in cryptology - ASIACRYPT 2018 - 24th international conference on the theory and application of cryptology and information security, brisbane, qld, australia, december 2-6, 2018, proceedings, part III* (Vol. 11274, pp. 86–117). doi:10.1007/978-3-030-03332-3_4

41 Hazay, C., Orsini, E., Scholl, P., & Soria-Vazquez, E. (2018b). Tinykeys: A new approach to efficient multi-party computation. In H. Shacham & A. Boldyreva (Eds.), *Advances in cryptology - CRYPTO 2018 - 38th annual international cryptology conference, santa barbara, ca, usa, august 19-23, 2018, proceedings, part III* (Vol. 10993, pp. 3–33). doi:10.1007/978-3-319-96878-0_1

42 Hazay, C., & Venkitasubramaniam, M. (2018). Round-optimal fully black-box zero-knowledge arguments from one-way permutations. In A. Beimel & S. Dziembowski (Eds.), *Theory of cryptography - 16th international conference, TCC 2018, panaji, india, november 11-14, 2018, proceedings, part I* (Vol. 11239, pp. 263–285). doi:10.1007/978-3-030-03807-6_10

43 Ames, S., Hazay, C., Ishai, Y., & Venkitasubramaniam, M. (2017). Ligero: Lightweight sublinear arguments without a trusted setup. In B. Thuraisingham, D. Evans, T. Malkin, & D. Xu (Eds.), *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security, CCS 2017, dallas, tx, usa, october 30 - november 03, 2017* (pp. 2087–2104). doi:10.1145/3133956.3134104

44 Hazay, C., Ishai, Y., & Venkitasubramaniam, M. (2017). Actively secure garbled circuits with constant communication overhead in the plain model. In Y. Kalai & L. Reyzin (Eds.), *Theory of cryptography - 15th international conference, TCC 2017, baltimore, md, usa, november 12-15, 2017, proceedings, part II* (Vol. 10678, pp. 3–39). doi:10.1007/978-3-319-70503-3_1

45 Hazay, C., Polychroniadou, A., & Venkitasubramaniam, M. (2017). Constant round adaptively secure protocols in the tamper-proof hardware model. In S. Fehr (Ed.), *Public-key cryptography - PKC 2017 - 20th IACR international conference on practice and theory in public-key cryptography, amsterdam, the netherlands, march 28-31, 2017, proceedings, part II* (Vol. 10175, pp. 428–460). doi:10.1007/978-3-662-54388-7_15

46 Hazay, C., Scholl, P., & Soria-Vazquez, E. (2017). Low cost constant round MPC combining BMR and oblivious transfer. In T. Takagi & T. Peyrin (Eds.), *Advances in cryptology - ASIACRYPT 2017 - 23rd international conference on the theory and applications of cryptology and information security, hong kong, china, december 3-7, 2017, proceedings, part I* (Vol. 10624, pp. 598–628). doi:10.1007/978-3-319-70694-8_21

47 Hazay, C., & Venkitasubramaniam, M. (2017). Scalable multi-party private set-intersection. In S. Fehr (Ed.), *Public-key cryptography - PKC 2017 - 20th IACR international conference on practice and theory in public-key cryptography, amsterdam, the netherlands, march 28-31, 2017, proceedings, part I* (Vol. 10174, pp. 175–203). doi:10.1007/978-3-662-54365-8_8

48 Hazay, C., Polychroniadou, A., & Venkitasubramaniam, M. (2016). Composable security in the tamper-proof hardware model under minimal complexity. In M. Hirt & A. D. Smith (Eds.), *Theory of cryptography - 14th international conference, TCC 2016-b, beijing, china, october 31 - november 3, 2016, proceedings, part I* (Vol. 9985, pp. 367–399). doi:10.1007/978-3-662-53641-4_15

49 Hazay, C., & Venkitasubramaniam, M. (2016a). Composable adaptive secure protocols without setup under polytime assumptions. In M. Hirt & A. D. Smith (Eds.), *Theory of cryptography - 14th international conference, TCC 2016-b, beijing, china, october 31 - november 3, 2016, proceedings, part I* (Vol. 9985, pp. 400–432). doi:10.1007/978-3-662-53641-4_16

50 Hazay, C., & Venkitasubramaniam, M. (2016b). On the power of secure two-party computation. In M. Robshaw & J. Katz (Eds.), *Advances in cryptology - CRYPTO 2016 - 36th annual international cryptology conference, santa barbara, ca, usa, august 14-18, 2016, proceedings, part II* (Vol. 9815, pp. 397–429). doi:10.1007/978-3-662-53008-5_14

51 Hazay, C., & Venkitasubramaniam, M. (2016c). What security can we achieve within 4 rounds? In V. Zikas & R. D. Prisco (Eds.), *Security and cryptography for networks - 10th international conference, SCN 2016, amalfi, italy, august 31 - september 2, 2016, proceedings* (Vol. 9841, pp. 486–505). doi:10.1007/978-3-319-44618-9_26

52 Hazay, C., & Yanai, A. (2016). Constant-round maliciously secure two-party computation in the RAM model. In M. Hirt & A. D. Smith (Eds.), *Theory of cryptography - 14th international conference, TCC 2016-b, beijing, china, october 31 - november 3, 2016, proceedings, part I* (Vol. 9985, pp. 521–553). doi:10.1007/978-3-662-53641-4_20

53 Hazay, C., & Zarosim, H. (2016). The feasibility of outsourced database search in the plain model. In V. Zikas & R. D. Prisco (Eds.), *Security and cryptography for networks - 10th international conference, SCN 2016, amalfi, italy, august 31 - september 2, 2016, proceedings* (Vol. 9841, pp. 313–332). doi:10.1007/978-3-319-44618-9_17

54 Hazay, C. (2015). Oblivious polynomial evaluation and secure set-intersection from algebraic prfs. In Y. Dodis & J. B. Nielsen (Eds.), *Theory of cryptography - 12th theory of cryptography conference, TCC 2015, warsaw, poland, march 23-25, 2015, proceedings, part II* (Vol. 9015, pp. 90–120). doi:10.1007/978-3-662-46497-7_4

55 Hazay, C., Lindell, Y., & Patra, A. (2015). Adaptively secure computation with partial erasures. In C. Georgiou & P. G. Spirakis (Eds.), *Proceedings of the 2015 ACM symposium on principles of distributed computing, PODC 2015, donostia-san sebastián, spain, july 21 - 23, 2015* (pp. 291–300). doi:10.1145/2767386.2767400

56 Hazay, C., Patra, A., & Warinschi, B. (2015). Selective opening security for receivers. In T. Iwata & J. H. Cheon (Eds.), *Advances in cryptology - ASIACRYPT 2015 - 21st international conference on the theory and application of cryptology and information security, auckland, new zealand, november 29 - december 3, 2015, proceedings, part I* (Vol. 9452, pp. 443–469). doi:10.1007/978-3-662-48797-6_19

57 Hazay, C., & Venkitasubramaniam, M. (2015). On black-box complexity of universally composable security in the CRS model. In T. Iwata & J. H. Cheon (Eds.), *Advances in cryptology - ASIACRYPT 2015 - 21st international conference on the theory and application of cryptology and information security, auckland,*

new zealand, november 29 - december 3, 2015, proceedings, part II (Vol. 9453, pp. 183–209). doi:10.1007/978-3-662-48800-3_8

58 Hazay, C., & Patra, A. (2014). One-sided adaptively secure two-party computation. In Y. Lindell (Ed.), *Theory of cryptography - 11th theory of cryptography conference, TCC 2014, san diego, ca, usa, february 24-26, 2014. proceedings* (Vol. 8349, pp. 368–393). doi:10.1007/978-3-642-54242-8_16

59 Faust, S., Hazay, C., & Venturi, D. (2013). Outsourced pattern matching. In F. V. Fomin, R. Freivalds, M. Z. Kwiatkowska, & D. Peleg (Eds.), *Automata, languages, and programming - 40th international colloquium, ICALP 2013, riga, latvia, july 8-12, 2013, proceedings, part II* (Vol. 7966, pp. 545–556). doi:10.1007/978-3-642-39212-2_48

60 Hazay, C., López-Alt, A., Wee, H., & Wichs, D. (2013). Leakage-resilient cryptography from minimal assumptions. In T. Johansson & P. Q. Nguyen (Eds.), *Advances in cryptology - EUROCRYPT 2013, 32nd annual international conference on the theory and applications of cryptographic techniques, athens, greece, may 26-30, 2013. proceedings* (Vol. 7881, pp. 160–176). doi:10.1007/978-3-642-38348-9_10

61 Akavia, A., Goldwasser, S., & Hazay, C. (2012). Distributed public key schemes secure against continual leakage. In D. Kowalski & A. Panconesi (Eds.), *ACM symposium on principles of distributed computing, PODC '12, funchal, madeira, portugal, july 16-18, 2012* (pp. 155–164). doi:10.1145/2332432.2332462

62 Damgård, I., Faust, S., & Hazay, C. (2012). Secure two-party computation with low communication. In R. Cramer (Ed.), *Theory of cryptography - 9th theory of cryptography conference, TCC 2012, taormina, sicily, italy, march 19-21, 2012. proceedings* (Vol. 7194, pp. 54–74). doi:10.1007/978-3-642-28914-9_4

63 Faust, S., Hazay, C., Nielsen, J. B., Nordholt, P. S., & Zottarel, A. (2012). Signature schemes secure against hard-to-invert leakage. In X. Wang & K. Sako (Eds.), *Advances in cryptology - ASIACRYPT 2012 - 18th international conference on the theory and application of cryptology and information security, beijing, china, december 2-6, 2012. proceedings* (Vol. 7658, pp. 98–115). doi:10.1007/978-3-642-34961-4_8

64 Hazay, C., Mikkelsen, G. L., Rabin, T., & Toft, T. (2012). Efficient RSA key generation and threshold paillier in the two-party setting. In O. Dunkelman (Ed.), *Topics in cryptology - CT-RSA 2012 - the cryptographers' track at the RSA conference 2012, san francisco, ca, usa, february 27 - march 2, 2012. proceedings* (Vol. 7178, pp. 313–331). doi:10.1007/978-3-642-27954-6_20

65 Asharov, G., Canetti, R., & Hazay, C. (2011). Towards a game theoretic view of secure computation. In K. G. Paterson (Ed.), *Advances in cryptology - EUROCRYPT 2011 - 30th annual international conference on the theory and applications of cryptographic techniques, tallinn, estonia, may 15-19, 2011. proceedings* (Vol. 6632, pp. 426–445). doi:10.1007/978-3-642-20465-4_24

66 Gennaro, R., Hazay, C., & Sorensen, J. S. (2010). Text search protocols with simulation based security. In P. Q. Nguyen & D. Pointcheval (Eds.), *Public key cryptography - PKC 2010, 13th international conference on practice and theory in public key cryptography, paris, france, may 26-28, 2010. proceedings* (Vol. 6056, pp. 332–350). doi:10.1007/978-3-642-13013-7_20

67 Hazay, C., & Nissim, K. (2010). Efficient set operations in the presence of malicious adversaries. In P. Q. Nguyen & D. Pointcheval (Eds.), *Public key cryptography - PKC 2010, 13th international conference on practice and theory in public key cryptography, paris, france, may 26-28, 2010. proceedings* (Vol. 6056, pp. 312–331). doi:10.1007/978-3-642-13013-7_19

68 Hazay, C., & Toft, T. (2010). Computationally secure pattern matching in the presence of malicious adversaries. In M. Abe (Ed.), *Advances in cryptology - ASIACRYPT 2010 - 16th international conference on the theory and application of cryptology and information security, singapore, december 5-9, 2010. proceedings* (Vol. 6477, pp. 195–212). doi:10.1007/978-3-642-17373-8_12

69 Klinc, D., Hazay, C., Jagmohan, A., Krawczyk, H., & Rabin, T. (2009). On compression of data encrypted with block ciphers. In J. A. Storer & M. W. Marcellin (Eds.), *2009 data compression conference (DCC 2009), 16-18 march 2009, snowbird, ut, USA* (pp. 213–222). doi:10.1109/DCC.2009.71

70 Gordon, S. D., Hazay, C., Katz, J., & Lindell, Y. (2008). Complete fairness in secure two-party computation. In C. Dwork (Ed.), *Proceedings of the 40th annual ACM symposium on theory of computing, victoria, british columbia, canada, may 17-20, 2008* (pp. 413–422). doi:10.1145/1374376.1374436

71 Hazay, C., & Lindell, Y. (2008a). Constructions of truly practical secure protocols using standard smartcards. In P. Ning, P. F. Syverson, & S. Jha (Eds.), *Proceedings of the 2008 ACM conference on computer and communications security, CCS 2008, alexandria, virginia, usa, october 27-31, 2008* (pp. 491–500). doi:10.1145/1455770.1455832

72 Hazay, C., & Lindell, Y. (2008b). Efficient protocols for set intersection and pattern matching with security against malicious and covert adversaries. In R. Canetti (Ed.), *Theory of cryptography, fifth theory of cryptography conference, TCC 2008, new york, usa, march 19-21, 2008* (Vol. 4948, pp. 155–175). doi:10.1007/978-3-540-78524-8_10

73 Hazay, C., Katz, J., Koo, C., & Lindell, Y. (2007). Concurrently-secure blind signatures without random oracles or setup assumptions. In S. P. Vadhan (Ed.), *Theory of cryptography, 4th theory of cryptography conference, TCC 2007, amsterdam, the netherlands, february 21-24, 2007, proceedings* (Vol. 4392, pp. 323–341). doi:10.1007/978-3-540-70936-7_18

74 Hazay, C., Lewenstein, M., & Tsur, D. (2005). Two dimensional parameterized matching. In A. Apostolico, M. Crochemore, & K. Park (Eds.), *Combinatorial pattern matching, 16th annual symposium, CPM 2005, jeju island, korea, june 19-22, 2005, proceedings* (Vol. 3537, pp. 266–279). doi:10.1007/11496656_23

75 Hazay, C., Lewenstein, M., & Sokol, D. (2004). Approximate parameterized matching. In S. Albers & T. Radzik (Eds.), *Algorithms - ESA 2004, 12th annual european symposium, bergen, norway, september 14-17, 2004, proceedings* (Vol. 3221, pp. 414–425). doi:10.1007/978-3-540-30140-0_38

Books and Chapters

1 Hazay, C., & Lindell, Y. (2010b). *Efficient secure two-party protocols - techniques and constructions*. doi:10.1007/978-3-642-14303-8

Research Grants

ISF — New Advances in Arithmetic Garbling, Israel Science Foundation. Principal Investigator, October 2025-September 2029.

Algorand — MEGA-ACE: Multidisciplinary Educational Global Alliance for Algorand Center of Excellence, Algorand Foundation. *August 2022-September 2024.*

BSF — Secure Multi-Party Computation Over Noisy Networks, United States -– Israel Binational Science Foundation. Joint with Ran Gelles, October 2021-September 2025.

ISF — More Efficient MPC with Malicious Security, Israel Science Foundation, 880,000 NIS. Principal Investigator, October 2018-September 2022.

COST — Cryptography for Secure Digital Interaction, ICT COST Action IC1306. Management committee member, *April 2014 - March 2018.*

Min. Sci. — The Study of Efficient Delegatable Computation, Israel Ministry of Science and Technology of Infrastructures. Principle investigator, *December 2013-November 2016.*

Awards and Fellowships

Awards

2024 — **Rector's Award for Scientific Innovation**. Bar-Ilan University.

2023 — **Distinguished Paper**. ACM CCS.

Awards and Fellowships (continued)

2002, 2003 **Dean's Award**. Bar-Ilan University.

Fellowships

2006-2009 **Eshkol Fellowship**. Awarded by the Ministry of Science and Technology, Israel.

2005-2009 **BIU President Fellowship**. Awarded by the president of Bar-Ilan University.

Professional Activities

Program Chair

2022 **Director of Program Excellence.** Female junior high students, Bar-Ilan university.

Program Committee Chair

2023 **EUROCRYPT Program Co-Chair**

2022 **CRYPTO Workshops Chair**

EUROCRYPT Area Chair

2021 **CRYPTO Workshops Chair**

2020 **CRYPTO Workshops Chair**

2019 **CRYPTO Workshops Chair**

Program Committee Membership

2024 **TCC**

2021 **TCC, CT-RSA, INDOCRYPT**

2020 **EUROCRYPT, INDOCRYPT**

2019 **ACM-CCS, CRYPTO**

2018 **CSCML, SCN, PKC**

2017 **INDOCRYPT, TCC, PKC**

2016 **INDOCRYPT, ICITS**

2015 **CRYPTO, PKC**

2013 **PKC**

2012 **NordSec**

2011 **PKC**

2010 **CRYPTO**

Workshop Organization

2022 **Bar-Ilan Winter School.** Advances in Secure Computation.

2021 **Bar-Ilan Winter School.** Cryptography in a Quantum World.

2020 **Bar-Ilan Winter School.** Information Theoretic Cryptography.

2012 **TPMPC, Denmark.** Secure Computation – Theory and Applications.

Graduate Students

Current

Postdoc — **Francesco Berti**, joint with Itamar Levi

Ph.D. — **Robert Hanhan**, joint with Itamar Levi

Jialiu Cheng

Graduated

Avishay Yanay, joint with Yehuda Lindell

Rishabh Bhadauria

Anasuya Acharya

M.Sc. — **Raviv Moses**

Mor Lilintal

Efrat Cohen

Rahul B. S.