BAR ALON

ba714@georgetown.edu

POSITION

I am a Postdoc at the Department of Computer Science at Georgetown University, hosted by Prof. Muthuramakrishnan Venkitasubramaniam. Previously, I was a postdoc at Ben-Gurion University, hosted by Prof. Amos Beimel.

EDUCATION

Ph.D. in Computer Science, *2019 - 2024*
Ariel University, Ariel, Israel
Advisors: Prof. Boaz Ben-Moshe, Prof. Eran Omri
Thesis title: Secure Multiparty Computation With Full Security In Different Models

M.Sc. in Mathematics and Computer Science, *2016 - 2018*
Ariel University, Ariel, Israel
Advisor: Dr. Eran Omri
Thesis title: Almost-Optimally Fair Multiparty Coin-Tossing with Nearly Three-Quarters Malicious
Graduated summa cum laude

B.Sc. in Mathematics and Computer Science, *2013 - 2016*
Ariel University, Ariel, Israel
Graduated magna cum laude

TEACHING

- Spring 2023, Logic and Set Theory
- Fall 2022/23, Probability for Computer Science 1 (jointly taught)
- Fall 2020/21, Algorithmic Number Theory (jointly taught).
- I was a teaching assistant (multiple times) for the following courses.
  - Automata and Formal Languages 1
  - Discrete Mathematics
  - Probability for Computer Science 1 and 2
  - Logic and Set Theory
  - Algorithmic Number Theory

HONORS AND AWARDS

- Dean's honor for undergraduate studies, Ariel University 2016.
- Dean's honor for undergraduate studies, Ariel University 2015.
- President's honor for undergraduate studies, Ariel University 2014.

PUBLICATIONS (REVERSE CHRONOLOGICAL ORDER)

[1] Bar Alon and Naty Peter. Dynamic security: A realistic approach to adaptive security with applications to strong FaF security. Cryptology ePrint Archive, Paper 2025/988, 2025.

[2] Bar Alon, Benjamin Saldman, and Eran Omri. New techniques for analyzing fully secure protocols: A case study of solitary output secure computation. Cryptology ePrint Archive, Paper 2025/522, 2025.

[3] Bar Alon, Amos Beimel, and Or Lasri. Simplified pir and cds protocols and improved linear secret-sharing schemes. In *Theory of Cryptography: 23rd International Conference, TCC 2025, Aarhus, Denmark, December 15, 2025, Proceedings, Part II*, page 365398, Berlin, Heidelberg, 2025. Springer-Verlag.

[4] Bar Alon and Amos Beimel. On the definition of malicious private information retrieval. In Niv Gilboa, editor, *6th Conference on Information-Theoretic Cryptography, ITC 2025, University of California, Santa Barbara, CA, USA, August 16-17, 2025*, volume 343 of *LIPIcs*, pages 8:1–8:23. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025.

[5] Bar Alon, Amos Beimel, Tamar Ben David, Eran Omri, and Anat Paskin-Cherniavsky. New upper bounds for evolving secret sharing via infinite branching programs. In Elette Boyle and Mohammad Mahmoody, editors, *Theory of Cryptography - 22nd International Conference, TCC 2024, Milan, Italy, December 2-6, 2024, Proceedings, Part IV*, volume 15367 of *Lecture Notes in Computer Science*, pages 548–580. Springer, 2024.

[6] Bar Alon, Moni Naor, Eran Omri, and Uri Stemmer. MPC for tech giants (GMPC): enabling gulliver and the lilliputians to cooperate amicably. In Leonid Reyzin and Douglas Stebila, editors, *Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part VIII*, volume 14927 of *Lecture Notes in Computer Science*, pages 74–108. Springer, 2024.

[7] Bar Alon, Eran Omri, and Muthuramakrishnan Venkitasubramaniam. Can alice and bob guarantee output to carol? In Marc Joye and Gregor Leander, editors, *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*, volume 14655 of *Lecture Notes in Computer Science*, pages 32–61. Springer, 2024.

[8] Bar Alon, Amos Beimel, and Eran Omri. Three party secure computation with friends and foes. In Guy N. Rothblum and Hoeteck Wee, editors, *Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part II*, volume 14370 of *Lecture Notes in Computer Science*, pages 156–185. Springer, 2023.

[9] Bar Alon and Eran Omri. On secure computation of solitary output functionalities with and without broadcast. In Guy N. Rothblum and Hoeteck Wee, editors, *Theory of Cryptography - 21st International Conference, TCC 2023, Taipei, Taiwan, November 29 - December 2, 2023, Proceedings, Part II*, volume 14370 of *Lecture Notes in Computer Science*, pages 94–123. Springer, 2023.

[10] Bar Alon, Olga Nissenbaum, Eran Omri, Anat Paskin-Cherniavsky, and Arpita Patra. On perfectly secure two-party computation for symmetric functionalities with correlated randomness. In Eike Kiltz and Vinod Vaikuntanathan, editors, *Theory of Cryptography - 20th International Conference, TCC 2022, Chicago, IL, USA, November 7-10, 2022, Proceedings, Part II*, volume 13748 of *Lecture Notes in Computer Science*, pages 532–561. Springer, 2022.

[11] Bar Alon, Hao Chung, Kai-Min Chung, Mi-Ying Huang, Yi Lee, and Yu-Ching Shen. Round efficient secure multiparty quantum computation with identifiable abort. In Tal Malkin and Chris Peikert, editors, *Advances in Cryptology - CRYPTO 2021 - 41st Annual International Cryptology Conference, CRYPTO 2021, Virtual Event, August 16-20, 2021, Proceedings, Part I*, volume 12825 of *Lecture Notes in Computer Science*, pages 436–466. Springer, 2021.

[12] Bar Alon, Ran Cohen, Eran Omri, and Tom Suad. On the power of an honest majority in three-party computation without broadcast. In Rafael Pass and Krzysztof Pietrzak, editors, *Theory of*

Cryptography - 18th International Conference, TCC 2020, Durham, NC, USA, November 16-19, 2020, Proceedings, Part II, volume 12551 of *Lecture Notes in Computer Science*, pages 621–651. Springer, 2020.

[13] Bar Alon, Eran Omri, and Anat Paskin-Cherniavsky. MPC with friends and foes. In Daniele Micciancio and Thomas Ristenpart, editors, *Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part II*, volume 12171 of *Lecture Notes in Computer Science*, pages 677–706. Springer, 2020.

[14] Bar Alon and Anat Paskin-Cherniavsky. On perfectly secure 2PC in the ot-hybrid model. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography - 17th International Conference, TCC 2019, Nuremberg, Germany, December 1-5, 2019, Proceedings, Part I*, volume 11891 of *Lecture Notes in Computer Science*, pages 561–595. Springer, 2019.

[15] Bar Alon and Eran Omri. Almost-optimally fair multiparty coin-tossing with nearly three-quarters malicious. In Martin Hirt and Adam D. Smith, editors, *Theory of Cryptography - 14th International Conference, TCC 2016-B, Beijing, China, October 31 - November 3, 2016, Proceedings, Part I*, volume 9985 of *Lecture Notes in Computer Science*, pages 307–335, 2016.