Gal Arnon

+972542207124
gal.aronon@weizmann.ac.il
Website: galarnon42.github.io

Education

2020–Present **PhD Computer Science**, *Weizmann Institute of Science*.
(Expected Completion: Jan 2025) Advised By: Prof. Moni Naor and Dr. Eylon Yogev

2017–2020 **MSc Computer Science**, *Weizmann Institute of Science*.
(GPA: 93) Advised By: Prof. Guy N. Rothblum
Thesis: On Prover-Efficient Public-Coin Emulation of Interactive Proofs

2013–2017 **BSc Electrical Engineering and Computer Science**, *Tel Aviv University*.
Magna Cum Laude (GPA: 90.68)

- Final Project (Electrical Engineering) in collaboration with Intel Corporation, Petah Tikva, Israel.
- Final Project (Computer Science) supervised by Prof. Mooly Sagiv and Dr. Oded Padon.
- Research Project supervised by Prof. Ran Canetti.

Research Interests

Foundations of cryptography, computational complexity and theory of computation, probabilistic proof systems, the application of theory to practical problems.

Publications

1. STIR: Reed–Solomon Proximity Testing with Fewer Queries
   G. Arnon, A. Chiesa, G. Fenzi and E. Yogev. (Under submission).
2. Hamming Weight Proofs of Proximity with One-Sided Error
   G. Arnon, S. Ben-David, and E. Yogev. (Under submission).
3. IOPs with Inverse Polynomial Soundness Error
   G. Arnon, A. Chiesa, and E. Yogev. ***FOCS 2023***.
4. A Toolbox for Barriers on Interactive Oracle Proofs
   G. Arnon, A. Bhangale, A. Chiesa, and E. Yogev. ***TCC 2022***.
5. Hardness of Approximation for Stochastic Problems via Interactive Oracle Proofs
   G. Arnon, A. Chiesa, and E. Yogev. ***CCC 2022***.
6. Min-Entropic Optimality
   G. Arnon and T. Grossman. (Preprint).
7. A PCP Theorem for Interactive Proofs and Applications
   G. Arnon, A. Chiesa, and E. Yogev. ***EUROCRYPT 2022***.
8. On Prover-Efficient Public-Coin Emulation of Interactive Proofs
   G. Arnon and G. N. Rothblum. ***ITC 2021***.

Invited Workshops and Long-Term Visits

Invited Workshops
- Efficient Probabilistic Proofs
  Bertinoro, Italy. July 2022.

Long-Term Visits
- Proofs, Consensus, and Decentralizing Society Semester
  Visiting Graduate Student at the Simons Institute, UC Berkeley. August-October 2019.

Service

Workshop Organization

- Lattices Meet Hashes: Recent Advances in Post-Quantum Zero-Knowledge Proofs.
  Postdoctoral Workshop at the Bernoulli Center, EPFL, Lausanne, Switzerland. Organized together with Ngoc Khanh Nguyen. May 2023.

External reviewer CRYPTO (2019, 2022, 2023), ITCS (2022), TCC (2021, 2023), SODA (2024), CCC (2024)

Talks

- IOPs with Inverse Polynomial Soundness Error
  - *Technion TCS Seminar, Haifa, Israel. February 2024.*
  - *ZK Study Club, Virtual. October 2023.*
  - *StarkWare Industries, Netanya, Israel. September 2023.*
  - *Interuniversity TCS Student Seminar, Tel-Aviv University, Tel-Aviv, Israel. July 2023.*
  - *IST Austria TCS Seminar, Vienna, Austria. June 2023.*
- A Toolbox for Barriers on Interactive Oracle Proofs
  - *TCC 2022, Chicago, USA. November 2022.*
- How To Be Convinced While Barely Listening (Even to Yourself)
  - *EPFL CS Theory Reading Group, Lausanne, Switzerland. May 2023.*
  - *Efficient Probabilistic Proofs Workshop, Bertinoro, Italy. July 2022. (Talk given under alternate title.)*
- Hardness of Approximation for Stochastic Problems via Interactive Oracle Proofs
  - *CCC 2022, Philadelphia, USA. July 2022. (Talk given virtually.)*
- A PCP Theorem for Interactive Proofs and Applications
  - *EUROCRYPT 2022, Trondheim, Norway. May-June 2022.*
  - *Theory Lunch at the Weizmann Institute of Science, Rehovot, Israel. July 2021.*
- On Prover-Efficient Public-Coin Emulation of Interactive Proofs
  - *ITC 2021, Virtual. July 2021.*
  - *"Proofs, Consensus, and Decentralizing Society" Program Seminar at Simons Institute, Berkeley, USA. October 2019.*

Teaching

- Foundations and Frontiers of Probabilistic Proofs
  MSRI (SLMath) summer graduate school. Zurich, Switzerland. July 2023.
- Foundations and Frontiers of Probabilistic Proofs
  MSRI summer graduate school. Held virtually. July-August 2021.
- Mini-Course on Zero-Knowledge Proofs
  Amos de-Shalit Summer School, Weizmann Institute of Science. September 2018.

Languages

Native Hebrew, English

Fluent German

Programming Languages

C#, Python, Java, C, C++, Matlab