Gal Arnon

gal.arnon@weizmann.ac.il
galarnon42.github.io

Education

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

M.Sc. Computer Science **2017–2020**
Weizmann Institute of Science
Advised By: Prof. Guy N. Rothblum
Thesis: On Prover-Efficient Public-Coin Emulation of Interactive Proofs

B.Sc. Electrical Engineering and Computer Science **2013–2017**
Tel Aviv University
Magna Cum Laude

Research Interests

Foundations of cryptography, computational complexity and theory of computation, probabilistic proof systems in both theory and practice.

Awards

- **Esther Hellinger Memorial Prize for academic excellence**. *Awarded in 2024 by the Weizmann Institute.*
- **Best Paper Award** for "STIR: Reed–Solomon Proximity Testing with Fewer Queries". *At Advances in Cryptology, the 44th Annual International Cryptology Conference (CRYPTO 2024).*

Publications

10. **Instance Compression, Revisited**. Gal Arnon, Shany Ben-David, and Eylon Yogev.
9. **WHIR: Reed–Solomon Proximity Testing with Super-Fast Verification**. Gal Arnon, Alessandro Chiesa, Giacomo Fenzi, and Eylon Yogev. *ZKSummit 12.*
8. **Hamming Weight Proofs of Proximity with One-Sided Error**. Gal Arnon, Shany Ben-David, and Eylon Yogev. *To appear in proceedings of the 22nd Theory of Cryptography Conference (TCC 2024).*
7. **STIR: Reed–Solomon Proximity Testing with Fewer Queries**. Gal Arnon, Alessandro Chiesa, Giacomo Fenzi, and Eylon Yogev. *In proceedings of Advances in Cryptology, the 44th Annual International Cryptology Conference (CRYPTO 2024)*, Part X, pp. 380–413. **Best Paper Award**.
   Additionally appeared in ZKSummit 11 and ZKProof 6.
6. **IOPs with Inverse Polynomial Soundness Error**. Gal Arnon, Alessandro Chiesa, and Eylon Yogev. *In proceedings of the 64th IEEE Annual Symposium on Foundations of Computer Science (FOCS 2023), pp. 752–761.*
5. **A Toolbox for Barriers on Interactive Oracle Proofs**. Gal Arnon, Amey Bhangale, Alessandro Chiesa, and Eylon Yogev. *In proceedings of the 20th Theory of Cryptography Conference (TCC 2022), pp. 447–466*
4. **Hardness of Approximation for Stochastic Problems via Interactive Oracle Proofs**. Gal Arnon, Alessandro Chiesa, and Eylon Yogev. *In proceedings of the 37th Annual IEEE Conference on Computational Complexity (CCC 2022), pp. 24:1–24:16.*
3. **Min-Entropic Optimality**. Gal Arnon and Tomer Grossman. *(Manuscript.)*
2. **A PCP Theorem for Interactive Proofs and Applications**. Gal Arnon, Alessandro Chiesa, and Eylon Yogev. *In proceedings of the 41st Annual International Conference on Theory and Application of Cryptographic Techniques (EUROCRYPT 2022), pp. 64–94.*

1. **On Prover-Efficient Public-Coin Emulation of Interactive Proofs**. Gal Arnon and Guy N. Rothblum. *In proceedings of the 2nd Conference on Information-Theoretic Cryptography (ITC 2021), volume 199 of LIPIcs, pp. 3:1–3:15.*

Invited Talks

- IOPs with Inverse Polynomial Soundness Error. *ITC 2024 Highlights Track, Stanford University, United States. August 2024.*
- How to convince someone who's barely listening (even to themselves). *At Efficient Probabilistic Proofs Workshop, Bertinoro, Italy. July 2022.*

Long-Term Visits

- Proofs, Consensus, and Decentralizing Society Semester 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.*

Sub-reviewer: CCC (2024), CRYPTO (2019, 2022, 2023, 2024), ITCS (2022), SODA (2024), STOC (2025), TCC (2021, 2023)

Talks

- STIR: Reed–Solomon Proximity Testing with Fewer Queries
  - *CRYPTO 2024, Santa Barbara, United States. August 2024.*
  - *Interuniversity TCS Student Seminar, Tel Aviv University, Tel Aviv, Israel. May 2024.*
  - *Theory Lunch at the Weizmann Institute of Science, Rehovot, Israel. May 2024.*
  - *HUJI TCS Seminar, Jerusalem, Israel. May 2024.*
  - *StarkWare Industries, Netanya, Israel. April 2024.*
  - *ZKSummit 11, Athens, Greece. April 2024.*
- IOPs with Inverse Polynomial Soundness Error
  - *ITC 2024 Highlights Track, Stanford University, United States. August 2024.*
  - *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

Teaching Assistant:

- 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.*

Instructor: Mini-Course on Zero-Knowledge Proofs. *Amos de-Shalit Summer School, Weizmann Institute of Science. September 2018.*