Rotem Arnon-Friedman

https://rotemaf.info/
rotemaf@berkeley.edu
UC Berkeley, California

— Appointments —

2018-Today	Postdoctoral researcher at the EECS department, UC Berkeley *Hosted by Prof. Umesh Vazirani*

— Education —

2013-2018	PhD student at the Institute of Theoretical Physics, ETH-Zurich *Under the supervision of Prof. Renato Renner*
2011-2012	MSc in Computer Science, Tel-Aviv University (Avg. grade of 94) *Under the supervision of Prof. Amnon Ta-Shma*
2007-2010	BSc in Physics and Computer Science, Tel-Aviv University (Avg. grade of 95 in CS and 90 in Physics, Magna Cum Laude)

— Awards & Recognitions —

2016-2017	Best Student Paper Award, QCrypt16, QCrypt17
2013-2015	Best Poster Award, QCrypt13, QIP14, and QIP15
2009,2011	Special Award of Excellence, Department of Computer Science, Tel-Aviv University
2010	Deans List, Tel-Aviv University
2009,2010	The Memorial Day Award of Excellence, Department of Physics, Tel-Aviv University

— Professional Services —

PC member	QCrypt17, QIP18, QCrypt19
Reviewer	STOC, FOCS, Theory of Computing, Crypto, Quantum, New Journal of Physics, IEEE transactions on Information Theory, Nature Communications

— Teaching Experience —

2014-2018	Supervision and assistance to Master students working on research projects in the QIT group, ETH-Zurich
2013-2017	Teaching assistant, Department of Physics, ETH-Zurich
2011-2012	Teaching assistant, Department of Computer Science, Tel-Aviv University
2004-2006	Sargent, School of Software Professions, Israel Defense Force Senior instructor in advanced programming classes Personal tutor to new instructors Development of teaching materials

— Publications —

Published	[1] Simple and tight device-independent security proofs, Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, *SIAM Journal on Computing 48(1)*, February 2019. Presented at QCrypt16 and QIP17. Full technical version of [3]. **Cryptography and Physics oriented;**

[2] Device-independent certification of one-shot distillable entanglement, Rotem Arnon-Friedman and Jean-Daniel Bancal, *New Journal of Physics,* January 2019. Presented at QCrypt19.
Physics oriented;

[3] Noise-tolerant testing of entanglement of formation, Rotem Arnon-Friedman and Henry Yuen, *International Colloquium of Automata, Languages, and Programming (ICALP)*, July 2018.
Physics and Theoretical CS oriented;

[4] Practical device-independent quantum cryptography via entropy accumulation, Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick, *Nature Communications 9*, January 2018. Presented at QCrypt16 and QIP17.
Short journal version of [1].
Cryptography and Physics oriented;

[5] Quantum-proof multi-source randomness extractors in the Markov model, Rotem Arnon-Friedman, Christopher Portmann, and Volkher B. Scholz, 11th *Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC)*, September 2016. Presented at QIP16 and QCrypt16.
Cryptography and Physics oriented;

[6] Non-signalling parallel repetition using de Finetti reductions, Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, *IEEE Transactions on Information Theory*, Issue: 99, January 2016.
Theoretical CS and Physics oriented;

[7] de Finetti reductions for correlations, Rotem Arnon-Friedman and Renato Renner, *Journal of Mathematical Physics* 56, 052203, May 2015.
Physics and Mathematics oriented;

[8] Limits of privacy amplification against non-signalling memory attacks, Rotem Arnon-Friedman and Amnon Ta-Shma, *Physical Reviews A* 86, 062333, December 2012. Presented at QCrypt13.
Cryptography and Physics oriented;

Preprints

[9] Reductions to IID in device-independent quantum information processing, Rotem Arnon-Friedman, arXiv:1812.10922, December 2018. PhD thesis.

[10] Device-independent randomness amplification and privatization, Max Kessler and Rotem Arnon-Friedman, arXiv:1705.04148, May 2017. Presented at QCrypt17.
Cryptography and Physics oriented;

[11] Towards the impossibility of non-signalling privacy amplification from time-like ordering constraints, Rotem Arnon-Friedman, Esther Hänggi, and Amnon
Ta-Shma, arXiv:1205.3736, May 2012. Master thesis.
Cryptography and Physics oriented;

— Selected Talks —

Contributed talks

Device-Independent certification of one-shot distillable entanglement,
QCrypt19, Montreal, August 27, 2019

Device-independent certification of entanglement measures,
Beyond IID in information theory, Sydney, July 5, 2019

Device-independent randomness amplification and privatization,
QCrypt17, Cambridge, September 22, 2017 ▶
Awarded the "Best Student Paper Award" of the conference

Entropy accumulation in device-independent protocols,
QIP17, Seattle, January 19, 2017 ▶
Plenary talk

Quantum-proof multi-source randomness extractors in the Markov model,
QCrypt16, Washington DC, September 15, 2016 ▶

Simple and tight device-independent security proofs,
QCrypt16, Washington DC, September 12, 2016 ▶
Awarded the "Best Student Paper Award" of the conference

de Finetti reductions in the context of non-local games,
Randomness in quantum physics and beyond, Barcelona,
May 6, 2015

Non-signalling parallel repetition using de Finetti reduction,
ISITS15, Lugano, May 3, 2015

Limits of privacy amplification against non-signalling memory attacks,QCrypt13, Waterloo, August 7, 2013 ▶

Invited talks

Entropy accumulation in the context of quantum key distribution,
IQC's workshop on security proofs in QKD, Waterloo, July 5, 2018.

Device-independent randomness amplification and privatization,
Trustworthy quantum information, Paris, June 19, 2017

Device-independent quantum cryptography,
Quantum science and technology general meeting, Arosa,
February 2, 2017

de Finetti reductions in the context of non-local games,
Trustworthy quantum information, Ann Arbor, July 2, 2015 ▶

Tutorials

Device-independent quantum key distribution: security proofs and practical challenges,
QCrypt19, Montreal, August 27, 2019

Seminar talks

Simple and tight device-independent security proofs,
QIT ICFO seminar, Institute of Photonic Sciences (ICFO), Barcelona, October 5, 2017

Device-independent randomness amplification and privatization,
TCS seminar, Princeton, New-Jersey, May 24, 2017 ▶

Device-independent randomness amplification and privatization,
CSAIL seminar, MIT, Cambridge, May 23, 2017

From loophole-free Bell tests to device-independent cryptography,
IQOQI seminar, University of Vienna, Vienna, February 16, 2017

Non-signalling parallel repetition using de Finetti reduction,
QIS seminar, MIT, Cambridge, June 23, 2015

Non-signalling parallel repetition using de Finetti reduction,
Quantum Computing seminar, The Hebrew University of Jerusalem, Jerusalem, March 12, 2015

de Finetti theorems: quantum and beyond,
CQT, Singapore, January 21, 2015

de Finetti theorems: quantum and beyond,
IQIM seminar, Caltech, Pasadena, June 17, 2014