Rotem Arnon-Friedman rotem.arn@weizmann.ac.il | website | WIS, Israel

Curriculum vitae

— Appointments —

2020-Today	Senior Scientist at the Department of Physics of Complex Systems, Weizmann Institute of Science
2019-2020	Postdoctoral researcher at the EECS department, UC Berkeley *Hosted by Prof. Umesh Vazirani*

— Education —

2013-2018	PhD from the Institute of Theoretical Physics, ETH-Zurich *Under the supervision of Prof. Renato Renner*
2011-2012	MSc in Computer Science, Tel-Aviv University *Under the supervision of Prof. Amnon Ta-Shma*
2007-2010	BSc in Physics and Computer Science, Tel-Aviv University

— Awards & Recognitions —

2021	Gruber Award
2019	ETH Medal Award for Outstanding Doctoral Thesis
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

— Grants —

2019-2020	Swiss National Science Foundation: Postdoc.Mobility Fellowship

— Professional Services —

PC member	QCrypt17, QIP18, QCrypt19, TQC20
Reviewer	Nature Communications, New Journal of Physics, IEEE transactions on Information Theory, PRX Quantum, Quantum, QCrypt, QIP, TQC, STOC, FOCS, Theory of Computing, Crypto

— Teaching —

2019-2020	Supervision and assistance to undergraduate and graduate students working on research projects in quantum cryptography, UC Berkeley
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

Selected Talks

Tutorials

Quantum key distribution,
BIU Winter School on Cryptography, February 15, 2021; Watch online

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

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; Watch online

Contributed Talks

Upper bounds on device-independent quantum key distribution rates and a revised Peres conjecture,
Beyond IID in Information Theory, November 9, 2020; Watch online

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; Watch online
Awarded the“Best Student Paper Award” of the conference

Entropy accumulation in device-independent protocols,
QIP17, Seattle, January 19, 2017; Watch online
Plenary talk

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

Simple and tight device-independent security proofs,
QCrypt16, Washington DC, September 12, 2016; Watch online
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; Watch online

Seminar Talks

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

Device-independent randomness amplification and privatization,
TCS seminar, Princeton, New-Jersey, May 24, 2017; Watch online
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
Quantum Computing seminar, HUJI, Jerusalem, March 12, 2015

de Finetti theorems: quantum and beyond,
CQT, Singapore, January 21, 2015
IQIM seminar, Caltech, Pasadena, June 17, 2014

— Publications —

Books

Device-Independent Quantum Information Processing: A Simplified Analysis, Rotem Arnon-Friedman, *Springer These, 2020.*

Papers

Device-independent quantum key distribution from computational assumptions, Tony Metger, Yfke Dulek, Andrea Coladangelo and Rotem Arnon-Friedman, 2020, arXiv:2010.04175

Upper bounds on device-independent quantum key distribution rates and a revised Peres conjecture, Rotem Arnon-Friedman and Felix Leditzky, 2020, arXiv:2x005.12325

Device-independent randomness amplification and privatization, Max Kessler and Rotem Arnon-Friedman, *IEEE Transactions on Information Theory, 2020* Published version.
Best Student Paper Award, QCrypt 2017.

Simple and tight device-independent security proofs, Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, *SIAM Journal on Computing, 2019.* Published version.
Best Student Paper Award, QCrypt 2016.

Device-independent certification of one-shot distillable entanglement, Rotem Arnon-Friedman and Jean-Daniel Bancal, *New Journal of Physics, 2019.* Published version.

Papers

Noise-tolerant testing of entanglement of formation, Rotem Arnon-Friedman and Henry Yuen, *International Colloquium of Automata, Languages, and Programming (ICALP), 2018.* Published version.

Practical device-independent quantum cryptography via entropy accumulation, Rotem Arnon-Friedman, Frederic Dupuis, Omar Fawzi, Renato Renner and Thomas Vidick, *Nature Communications, 2018.* Published version.

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, 2016.* Published version.

Non-signaling parallel repetition using de Finetti reductions, Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, *IEEE Transactions on Information Theory, 2016.* Published version.

de Finetti reductions for correlations, Rotem Arnon-Friedman and Renato Renner, *Journal of Mathematical Physics, 2015.* Published version.

Limits of privacy amplification against nonsignaling memory attacks, Rotem Arnon-Friedman and Amnon Ta-Shma, *Physical Review A, 2012.* Published version.

Theses

Reductions to IID in device-independent quantum information processing, Rotem Arnon-Friedman, *Doctoral thesis, 2018.* arXiv:1812.10922.
ETH Medal Award for outstanding doctoral thesis, 2019.

Towards the impossibility of non-signalling privacy amplification from time-like ordering constraints, Rotem Arnon-Friedman, Esther Hänggi, and Amnon Ta-Shma, *Master thesis, 2012.* arXiv:1205.3736.