Rotem Arnon-Friedman

Zurich, Switzerland

rotema@itp.phys.ethz.ch
https://rotemaf.info/

Education

2013-Today	PhD student in the Institute of Theoretical Physics, ETH-Zurich
2011-2012	MSc in Computer Science, Tel-Aviv University (Avg. grade of 94)
2007-2010	BSc in Physics and Computer Science, Tel-Aviv University (Avg. grade of 95 in CS and 90 in Physics, Magna Cum Laude)
2000-2004	Hagimnasia Ha'ivrit High School (Advanced placement in Mathematics, Physics, Electronics and English)

Awards & Recognitions

2017	Best Student Paper Award, QCrypt17
2016	Best Student Paper Award, QCrypt16
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

Teaching & Research

2013-Today	PhD student in quantum information theory. Under the supervision of Prof. Renato Renner
2014-Today	Supervision and assistance to Master students working on research projects in the QIT group, ETH-Zurich
2013-Today	Teaching assistant, Department of Physics, ETH-Zurich
2011-2012	Teaching assistant, Department of Computer Science, Tel-Aviv University
2011-2012	Master thesis in quantum information theory & cryptography (privacy amplification against non-signalling adversaries). Under the supervision of Prof. Amnon Ta-Shma
2009	Summer project for excellent students (development of numerical simulations describing the chemical evolution of galaxies). Under the supervision of Prof. Ariel Sternberg

Committees

2017	Program committee member QCrypt17 Program committee member QIP18

Professional Experience

2007-2009	Programmer at Compedia Ltd. Game development, Internal Management System, Research of new technologies
2004-2006	Sargent, School of Software Professions, Israel Defence Force Senior instructor in advanced programming classes Personal tutor to new instructors Development of classes' materials

Publications

Max Kessler and Rotem Arnon-Friedman, Device-independent randomness amplification and privatization, arXiv:1705.04148, May 2017.
Presented at QCrypt17.

Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, Simple and tight device-independent security proofs, arXiv:1607.01797, July 2016.
Presented at QCrypt16 and QIP17.

Rotem Arnon-Friedman, Christopher Portmann, and Volkher B. Scholz, Quantum-proof multi-source randomness extractors in the Markov model, 11th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2016), LIPIcs: 2016:6683, September 2016.
Presented at QIP16 and QCrypt16.

Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, Non-signalling parallel repetition using de Finetti reductions, IEEE Transactions on Information Theory, Issue: 99, January 2016.

Rotem Arnon-Friedman and Renato Renner, de Finetti reductions for correlations, J. Math. Phys. 56, 052203, May 2015.

Rotem Arnon-Friedman and Amnon Ta-Shma, Limits of privacy amplification against non-signalling memory attacks, Phys. Rev. A 86, 062333, December 2012.
Presented at QCrypt13.

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

Selected Talks

Device-independent randomness amplification and privatization (**contributed talk**), QCrypt17, Cambridge, September 22, 2017.
Awarded the “Best Student Paper Award” of the conference.

Device-independent randomness amplification and privatization (**invited talk**), trustworthy quantum information, Paris, June 19, 2017.

Device-independent randomness amplification and privatization, TCS seminar, Princeton, New-Jersey, May 24, 2017. [video]

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.

Device-independent quantum cryptography, QSIT (quantum science and technology) general meeting, Arosa, February 2, 2017.

Entropy accumulation in device-independent protocols (**plenary talk**), QIP17, Seattle, January 19, 2017. [video]

Quantum-proof multi-source randomness extractors in the Markov model (**contributed talk**), QCrypt16, Washington DC, September 15, 2016. [video]

Simple and tight device-independent security proofs (**contributed talk**), QCrypt16, Washington DC, September 12, 2016. [video]
Awarded the “Best Student Paper Award” of the conference.

de Finetti reductions in the context of non-local games (**invited talk**), trustworthy quantum information, Ann Arbor, July 2, 2015. [video]

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

de Finetti reductions in the context of non-local games (**contributed talk**), randomness in quantum physics and beyond, Barcelona, May 6, 2015.

Non-signalling parallel repetition using de Finetti reduction (**contributed talk**), ISITS15, Lugano, May 3, 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.

Limits of privacy amplification against non-signalling memory attacks (**contributed talk**), QCrypt13, Waterloo, August 7, 2013. [video]