Renato Renner

Institute for Theoretical Physics
ETH Zurich
8093 Zurich, Switzerland
renner@ethz.ch

Personal Information

Born December 11, 1974, in Lucerne, Switzerland
Swiss citizen, from Andermatt and Lucerne
Married, four children
Languages: German, English, French

Education

2001–2005	PhD (Dr. sc. nat.), Department of Computer Science, ETH Zurich, Switzerland Thesis: *Security of Quantum Key Distribution* (supervisor: Prof. Ueli Maurer)
1997–2000	Studies of theoretical physics, ETH Zurich, Switzerland
1996	Military service (Officers school of the Swiss Army Signal Corps)
1995	Studies of physics (premier propédeutique), EPF Lausanne, Switzerland
1990–1994	Matura Typus C, Obergymnasium, Kantonsschule Lucerne, Switzerland

Employment History

since 2007	Professor at the Institute for Theoretical Physics, ETH Zurich, Switzerland (first as tenure track assistant professor, since 2015 as full professor)
2005–2007	Postdoctoral researcher at the Centre for Quantum Computation, University of Cambridge, United Kingdom
2000–2005	Teaching and research assistant in the Department of Computer Science at ETH Zurich, Switzerland
1997–2000	Part-time job as a teaching assistant in the Department of Mathematics at ETH Zurich, Switzerland
1996/1998	Occasionally working as a teacher at Kantonsschule Lucerne, Switzerland

Selected Awards, Grants, and Fellowships

ALEA Award of the AVETH 2018; Teaching Award (Golden Owl) from the ETH Zurich Physics Student Association, 2017 and 2011; TCC Test of Time Award 2016 from the International Association for Cryptologic Research (IACR); Fellowship at the Stellenbosch Institute for Advanced Study, Fall 2015; CRM Aisenstadt Chair, Fall 2011; ERC Starting Independent Researcher Grant, 2010–2015; Best Dissertation Award by the German Chapter of the ACM; ETH Medal for the PhD thesis; ETH Medal for the diploma thesis; third prize of the European Union Contest for Young Scientists; Matura-Preis (university entrance exam, award for best results); Best Project Award at the Young Scientists Contest Switzerland (SJF).

Teaching

- Advanced Topics in Quantum Information Theory (2011, 2012); together with Matthias Christandl and Atac Imamoglu
- Classical Mechanics (2010, 2013)
- Electrodynamics (2010, 2018)
- General Relativity (2018)
- Philosophical Aspects of Quantum Physics (2016, 2017); together with Norman Sieroka
- Proseminar in Theoretical Physics (2008, 2009, 2014)
- Quantum Mechanics I (2008, 2011)
- Quantum Mechanics II (2012)
- Quantum Information Processing (2015, 2016)
- Quantum Information Theory (2007, 2008, 2009, 2010, 2011, 2012, 2015, 2016)
- Theory of Heat (2013, 2014, 2017, 2019)
- Supervision of master, bachelor, and semester projects

Selected Guest Lectures, Tutorials, Invited Talks, and Other Presentations

- Quantum theory cannot consistently describe the use of itself, Distinguished Lectures on Quantum Software, CWI, Amsterdam, the Netherlands, March 14, 2019.
- Agent-compatibility as a criterion for physical theories, Workshop on Encapsulated Agents in Quantum Theory, Boston USA, March 9, 2019.
- Quantum theory cannot consistently describe the use of itself (invited talk), APS March Meeting, Boston, USA, March 8, 2019.
- Security proofs for quantum key distribution (invited lecture), Quantum Computing Winter School and Hackathon, Sochi, Russia, February 19, 2019.
- Information-theoretic limits to the accuracy of clocks, SFB-FoQuS Conference, Innsbruck, Austria, February 7, 2019.
- Security of quantum cryptography (invited tutorial), IDQ Winter School, Les Diablerets, Switzerland, January 23, 2019.
- Quantum thermodynamics, ETH Physical Chemistry Colloquium, Zurich, Switzerland, December 4, 2018.
- Beyond Schrödigner's cat, Theoretical Physics Colloquium of the University of Konstanz, Konstanz, Germany, November 26, 2018.
- Quantenphysik — ein 100-jähriges Rätsel, Forum "Interface" at the Fachhochschule Nordostschweiz, Windisch, Switzerland, October 22, 2018.
- Quantum computing and cryptography, Swiss Digital Summit, Zurich, Switzerland, September 27, 2018.

- Epistemic logic in a quantum world, Conference on Logic and the Philosophy of Sciences, Lugano, Switzerland, September 22, 2018.
- Discovering physical concepts with neural networks, Conference on Quantum Machine Learning Plus (QML+), Innsbruck, September 19, 2018.
- Entropy accumulation, Steklov Mathematical Institute Conference, Moscow, Russia, September 13, 2018.
- True randomness (colloquium talk), MIPT-QUANT 2018, Moscow, Russia, September 11, 2018.
- Recovery of lost quantum information, SwissMAP General Meeting, Grindelwald, Switzerland, September 10, 2018.
- The finiteness of security (tutorial), QCrypt 2018, Shanghai, China, August 28, 2018.
- Entropy accumulation: the theorem and a conjecture, Beyond IID in Information Theory Conference, Cambridge, United Kingdom, July 23, 2018.
- Lectures in quantum foundations, Boulder School for Condensed Matter and Materials Physics, Boulder, USA, July 9–11, 2018.
- Quantum mechanics cannot consistently describe the use of itself, 4th Seefeld Workshop on Quantum Information, Seefeld, Austria, July 3, 2018.
- Randomness amplification, Seminar Talk, IBM Rüschlikon, Switzerland, June 29, 2018.
- Cryptography in the age of quantum computing, EURECOM Seminar on Quantum Computing, Sophia Antipolis, France, May 24, 2018.
- Security of quantum cryptography, Secure Quantum Communications School, Baiona, Spain, May 7, 2018.
- Quantum information and foundations, Workshop on Quantum Information, Boston, USA, April 23, 2018.
- Quantum theory cannot consistently describe the use of itself, Quantum Information in Cosmology, Copenhagen, Denmark, April 10, 2018.
- Quantum theory cannot consistently describe the use of itself, Conference on Observers in Quantum and Foil Theories, Waterloo, Canada, April 5, 2018.
- Forschung im Zeitalter der künstlichen Intelligenz, Swiss Physics Olympiad, Aarau, Switzerland, March 25, 2018.
- Quantenkryptographie, Vortragsreihe der Technischen Gesellschaft Zürich (TGZ), Zurich, Switzerland, March 19, 2018.
- Device-independent quantum cryptography (plenary talk), DPG-Frühjahrstagung der Sektion AMOP, Erlangen, Germany, March 8, 2018.
- Quantum Information Theory (tutorial), QSIT Winter School, Arosa, Switzerland, February 5, 2018.
- Quantum cryptography (invited tutorial), IDQ Winter School, Les Diablerets, Switzerland, January 24, 2018.
- Quantum theory cannot consistently describe the use of itself, Workshop on Quantum Information and Foundations, Hong Kong, China, January 8, 2018.

- Quantum cryptography, Lecture at the Moscow Institute for Science and Technology, Moscow, Russia, December 6, 2017.
- Approximate recoverability of quantum information, Seminar Talk at the Steklov Mathematical Institute, Moscow, Russia, December 6, 2017.
- Can quantum mechanics describe an agent who uses quantum mechanics?, Workshop on Indeterminism, Geneva, Switzerland, November 17, 2017.
- Consistency between Maxwell's demons, Quantum Thermodynamics Conference, Cambridge, USA, October 31, 2017.
- Can quantum mechanics be valid on large scales?, Caltech Physics Colloquium, Pasadena, USA, October 5, 2017.
- Quantum cryptography, Digital Festival, Zurich, Switzerland, September 15, 2017.
- Tutorial on the foundations of quantum cryptography, QKD Summer School, Waterloo, Canada, August 23 and 24, 2017.
- Quantum randomness, ICE-4 Conference, Madrid, Spain, July 13, 2017.
- Tutorial on quantum information theory, ICE-4 Summer School, Madrid, Spain, July 11, 2017.
- Tutorial on interpretations of quantum theory, Solstice of Foundations Summer School, Zurich, Switzerland, June 19 and 21, 2017.
- Quantum mechanics as a multi-agent theory, Participatory Realism Conference, Stellenbosch, South Africa, June 7, 2017.
- Can quantum mechanics be considered self-consistent?, New Directions in the Foundations of Physics, Tarquinia, Italy, May 27, 2017.
- A quantum information thought experiment, SANDU International Conference on Quantum Physics, Danube Delta, Romania, May 23, 2017.
- Recovery of lost quantum information, Spectral Days Conference, Stuttgart, Germany, April 4, 2017.
- Thermodynamics as a multi-agent theory, Fifth Quantum Thermodynamics Conference, Oxford, United Kingdom, March 14, 2017.
- Security definitions in quantum cryptography, BSI Meeting, Erlangen, Germany, February 23, 2017.
- The de Finetti theorem and entropy accumulation (invited tutorial), Lectures in Quantum Information Theory, January 26 and 27, Innsbruck, Austria, 2017.
- Security of quantum cryptography (invited tutorial), IDQ Winter School, Les Diablerets, Switzerland, January 18, 2017.
- An information-theoretic view on the foundations of quantum theory, SFB FOQUS Meeting, Vienna, Austria, December 15, 2016.
- Quantum thermodynamics, Weizmann Institute Quantum Information Workshop, Rehovot, Israel, November 23, 2016.
- True randomness from quantum devices, Hebrew University Quantum Information Workshop, Jerusalem, Israel, November 21, 2016

- From quantum cryptography to the foundations of physics, Physics Colloquium of the University of Basel, Basel, November 18, 2016.
- An information-theoretic view on the Copenhagen interpretation, QMath Kick-Off Meeting, Copenhagen, Denmark, November 7, 2016.
- What does quantum information teach us about the quantum world?, IMPRS Kick-Off Meeting, Munich, Germany, October 28, 2016.
- Recovery of lost quantum information, Workshop on Subfactor Theory, Quantum Field Theory, and Quantum Information, Boston, USA, October 9, 2016.
- Wigner's friends disagree: a thought experiment to question the foundations of quantum theory, Colloquium of the ICFO, Barcelona, Spain, October 7, 2016.
- Single-world interpretations of quantum theory cannot be self-consistent, Conference on Quantum Phenomena, Gdansk, Poland, September 22, 2016.
- An extension of the Wigner's friend gedankenexperiment, It From Qubit Workshop, Perimeter Institute for Theoretical Physics, Waterloo, Canada, July 27, 2016.
- Entropy accumulation, Third Seefeld Workshop on Quantum Information, Seefeld, Austria, June 28, 2016.
- Single-world interpretations of quantum theory cannot be self-consistent, Physics Colloquium of the University of Innsbruck, Austria, April 6, 2016.
- Quantum key distribution (invited tutorial), Winter School on Quantum Security, Darmstadt, Germany, January 25, 2016.
- Security of quantum cryptography (invited tutorial), IDQ Winter School, Les Diablerets, Switzerland, January 20, 2016.
- How much work does it cost to process information?, Colloquium of the Institute of Science and Technology (IST), Vienna, Austria, January 18, 2016.
- Quantum theory without probabilities, GDR IQFA — 6th Colloquium, Paris, France, November 19, 2015.
- Is the existence of randomness an axiom of quantum theory?, Workshop on the Foundations of Randomness, Stellenbosch, South Africa, October 26, 2015.
- Recovery of quantum information, Heilbronn Annual Conference, Bristol, United Kingdom, September 17, 2015.
- Quantifying the randomness of nature, Conference on Quantum Information Processing and Communication (QIPC), Leeds, United Kingdom, September 16, 2015.
- Tutorial on the foundations of quantum theory, IDEA League School, Zurich, Switzerland, September 10, 2015.
- A quantum information approach to time, Asian Quantum Information Science Conference (AQIS), Seoul, South Korea, August 25, 2015.
- Tutorial on the security of quantum cryptography, QKD Summer School, Waterloo, Canada, August 18 and 19, 2015.
- The role of randomness in experiments, Conference on Quantum Systems and Technology, Ascona, Switzerland, June 9, 2015.

- The Born rule without probabilities, Conference on Randomness in Quantum Physics and Beyond, Barcelona, Spain, May 6, 2015.
- Why classical cryptographers should care about quantum adversaries, IEEE International Workshop on Information Theory (ITW), Jerusalem, Israel, May 1, 2015.
- How to avoid the need for free choice, Workshop on Agency and (Quantum) Physics, Innsbruck, Austria, April 2, 2015.
- Woran glauben wir morgen?, Treffpunkt Science City, ETH Zurich, Switzerland, March 15, 2015
- Tutorial in quantum thermodynamics, IDEA League School, Aachen, Germany, February 23–25, 2015.
- Is Bohmian Mechanics self-consistent?, Trimestre: Le Monde Quantique, Institut Des Hautes Études Scientifiques (IHES), Bures-sur-Yvette, France, February 18, 2015.
- Conditional mutual information, The Third Peter Whittle Colloquium, Cambridge, United Kingdom, January 28, 2015.
- Quantum information security (invited tutorial), IDQ Winter School, Les Diablerets, Switzerland, January 21, 2015.
- Quantum information theory (invited tutorial), QSIT Student School, Arosa, Switzerland, January 6, 2015.
- Randomness in nature, TU Delft QuTech Colloquium, Delft, the Netherlands, December 4, 2014.
- Informatik als Unterrichtsfach am Gymnasium, KSGR Herbsttagung, Berne, Switzerland, November 26, 2014.
- Is the wave function in one-to-one correspondence with reality?, Munich Physics Colloquium, Munich, Germany, November 17, 2014.
- Non-contextuality and free choice (invited talk), Workshop on Quantum Contextuality, National University of Singapore, Singapore, November 4, 2014.
- Quantum cryptography — if secure is not enough, ETH Math-Phys Alumni Lecture 2014, Zurich, Switzerland, October 30, 2014.
- Randomness in physics, Physics Colloquium of the University of Stuttgart, Germany, October 28, 2014.
- Von Bits und Qbits — auf dem Weg zum Quantencomputer, Öffentliche NWG-Vortragsreihe an der Universität St. Gallen, Switzerland, October 22, 2014.
- Quantifying security (invited tutorial), QCrypt 2014, Paris, France, September 1, 2014.
- Quantum thermodynamics (invited lecture series), QUTE-Europe Summer School, Smolenice Castle, Slovakia, from August 25 to August 27, 2014.
- Randomness and free choice in experiment (invited talk), Gordon Research Conference on Quantum Science, Stonehill College, Easton MA, USA, July 31, 2014.
- The freedom of choice assumption and its implications (invited talk), Quantum (Un)Speakables II, University of Vienna, Austria, June 22, 2014.
- Quantum key distribution and information theory (invited tutorial), Spring School on Quantum Physics and Computer Science, Sèvres, France, June 16, 2014.

- Axiomatic approach towards single-shot entropies (invited talk), Beyond I.I.D. Workshop, National University of Singapore, Singapore, May 21, 2014.
- A quantum information perspective on Maxwell's demon, Physikalisches Kolloquium, Goethe Universität Frankfurt am Main, Germany, April 30, 2014.
- Reliable quantum state tomography, MIT Seminar on Quantum Information, Boston, USA, April 2, 2014.
- Randomness amplification (invited talk), NIST-UMD Workshop on Quantum Information and Computer Science, Maryland, USA, April 1, 2014.
- Quantum foundations and thermodynamics (invited lecture series), The 31st Jerusalem Winter School in Theoretical Physics, Jerusalem, Israel, from December 30, 2013 to January 2, 2014.
- One-shot entropies from thermodynamics (invited talk), Programme on Mathematical Challenges in Quantum Information, Cambridge, United Kingdom, December 5, 2013.
- Is the wave function in one-to-one correspondence with reality? (invited talk), Institute for Interdisciplinary Information Sciences Seminar, Tsinghua University, November 15, 2013.
- Landauer's principle revisited (invited talk), Hot Topics in Physical Informatics Conference, Changsha, China, November 12, 2013.
- Quantum cryptography with local Bell tests, Hot Topics in Physical Informatics Conference, Changsha, China, November 11, 2013.
- Quantentechnologie für und gegen Spione, Physikalische Gesellschaft Zürich, Zurich, Switzerland, November 7, 2013.
- Does freedom of choice imply that the wave function is real? (invited talk), Q+ Hangout, October 29, 2013.
- Is quantum cryptography secure against hacking attacks? (invited talk), Korea Institute for Advanced Study Seminar, Seoul, South Korea, October 18, 2013.
- A quantitative Landauer's principle (invited talk), Conference on Noise, Information & Complexity at the Quantum Scale, Erice, Italy, October 8, 2013.
- How secure is quantum cryptography? (invited talk), SPIE Security and Defence Conference, Dresden, Germany, September 23, 2013.
- Gambling against the second law of thermodynamics (public lecture), National University of Singapore, Singapore, September 10, 2013.
- Information and work, tutorial, Program on Mathematical Horizons for Quantum Physics 2, Singapore Institute for Mathematical Sciences, Singapore, September 9, 2013.
- The physics of cryptography (invited talk), QCrypt 2013, Waterloo, Canada, August 5, 2013.
- Security of quantum key distribution (invited tutorial), QKD Summer School, Waterloo, Canada, July 30 and 31, 2013.
- A proof of the data processing inequality based on smooth entropy (invited talk), Conference on Entropy in Quantum Mechanics: Recent Advances, Cergy-Pontoise, France, June 26, 2013.
- Quantum information theory (invited tutorial), 13th International School on Formal Methods for the Design of Computer, Communication and Software Systems: Dynamical Systems, Bertinoro, Italy, June 18 and 19, 2013.

- How secure is quantum cryptography? (invited talk), Conference on Laser and Electro Optics (CLEO), San Jose, USA, June 11, 2013.
- On the non-extendibility of quantum theory (invited talk), The Quantum Landscape: Generalizations of Quantum Theory and Experimental Tests, Waterloo, Canada, May 27, 2013.
- Smooth entropy in physics and information theory (keynote talk), Workshop on the Mathematics of Information-Theoretic Cryptography, Leiden, the Netherlands, May 23, 2013
- A quantitative Landauer's principle (invited talk), Workshop on Equilibration and Thermalization in Quantum Systems, Stellenbosch, South Africa, April 16, 2013.
- The wave function is as real as it can be (invited talk), Workshop on Physics and Information, Paris, France, April 9, 2013.
- The freedom of choice assumption and its implications (invited talk), APS March Meeting 2013, Baltimore, USA, March 21, 2013.
- Quantencomputer (public lecture), Naturwissenschaftliche Gesellschaft Winterthur, Switzerland, March 8, 2013.
- Einführung in die Quantenphysik (lecture for high school students), Kantonsschule Büelrain, Winterthur, Switzerland, March 4, 2013.
- On the completeness of quantum theory (invited talk), Quo Vadis Quantum Physics Workshop, Natal, Brazil, February 26, 2013.
- Quantum information theory (invited tutorial), QSIT Student School, Arosa, Switzerland, January 29, 2013.
- Quantum information security (invited tutorial), IDQ Winter School, Les Diablerets, Switzerland, January 23, 2013.
- Defeating the i.i.d. constraint, Beyond I.I.D. in Information Theory Workshop, Cambridge, United Kingdom, January 8, 2013.
- Quantum cryptography: towards device-independence (invited talk), Topical Research Meetings on Physics: Quantum Technologies — Taking Concepts Through to Implementations, London, United Kingdom, December 17, 2012.
- Smooth entropy (invited talk), WECIQ 2012, Fortaleza, Brazil, October 9, 2012.
- Device-independent security for quantum cryptography (invited talk), SPIE Security and Sensing Conference, Edinburgh, United Kingdom, September 25, 2012.
- Towards security proofs for practical quantum cryptography (invited talk), QUANT2012 Workshop, University of California, Los Angeles, USA, August 29, 2012.
- On the notion of free choice in physics (invited talk), Workshop on Quantum Physics of Information, Shanghai, China, August 27, 2012.
- A theory of information for physics (plenary talk), International Congress on Mathematical Physics, Aalborg, Denmark, August 8, 2012.
- Reliable quantum state tomography (invited talk), 11th International Conference on Quantum Communication, Measurement and Computing (QCMC), Vienna, Austria, July 31, 2012.
- Is a system's wave function in one-to-one correspondence with its elements of reality? (invited talk), Workshop on Quantum Information Theory, Seefeld, Austria, July 2, 2012.

- Is the wave function in one-to-one correspondence to the elements of reality? (invited talk), Workshop on the Occasion of Nicolas Gisin's 60th Birthday, Val d'Illiez, Switzerland, May 30, 2012.
- Free randomness amplification (invited talk), CTIC Workshop on Quantum Information Science, Tsinghua University, Beijing, China, May 23, 2012.
- Free randomness can be amplified, CQIF Seminar, University of Cambridge, United Kingdom, May 3, 2012.
- No extension of quantum theory can have improved predictive power (invited talk), International Workshop: From Quantum Foundations to Quantum Fluids, Toulouse, France, April 4, 2012.
- The thermodynamic meaning of negative (conditional) entropy, Quantum Computation & Information Seminar, University of Bristol, United Kingdom, April 3, 2012.
- Exploiting the quantum laws (invited talk), Young Researchers in Mathematics Conference (YRM 2012), Bristol, United Kingdom, April 2, 2012.
- On the non-extendibility of quantum theory (invited talk), Workshop on Quantum Mechanics: From Foundations to Quantum Information Science, Center for Interdisciplinary Research, Bielefeld, Germany, March 1, 2012.
- Is quantum theory informationally complete? (invited talk), Colloquium of the Dipartimento di Fisica, Università di Pavia, Pavia, Italy, February 9, 2012.
- Quantum information (tutorial), NCCR QSIT Student School, Arosa, Switzerland, January 31, 2012.
- Theoretical and practical security in quantum cryptography (keynote speech), 4th Winter School on Practical Quantum Cryptography, Les Diablerets, January 25, 2012.
- Free randomness amplification, CHIST-ERA Meeting on Device-Independent Quantum Information Processing, Geneva, Switzerland, November 24, 2011.
- An information-theoretic view on thermalization (invited talk), Workshop on Quantum Information in Quantum Many-Body Physics, Montreal, Canada, October 20, 2011.
- Information security in a quantum world (invited talk), Annual Doctoral Workshop on Mathematical and Engineering Methods in Computer Science (MEMICS), Lednice, Czech Republic, October 14, 2011.
- What does quantum cryptography tell us about quantum physics? (invited lecture), André Aisenstadt Chair Lecture, Montreal, Canada, October 12, 2011.
- Free randomness amplification (invited talk), Quantum Computer Science Workshop, Montreal, Canada, October 5, 2011.
- Entanglement witnessing and cryptography using uncertainty relations (invited talk), HIPERCOM Workshop, Paris, France, September 27, 2011.
- Quantum information theory (invited tutorial), QIPC School, Diavolezza, Switzerland, September 2, 2011.
- Information-theoretical security of QKD (invited lecture), QKD Summer School, Waterloo, Canada, July 26 and 27, 2011.
- Privacy amplification and composable security (invited talk), QKD Post Processing Workshop, Vienna, Austria, July 7, 2011.

- Quantum cryptography (invited lecture), Canadian Summer School on Quantum Information, Sherbrooke, Canada, June 13, 2011.
- Informatik im Unterricht, Tagung der Konferenz Schweizerischer Gymnasialrektorinnen und Gymnasialrektoren 2011, Payerne, Switzerland, May 31, 2011.
- Quantum-resilient randomness extraction (invited talk), 5th International Conference on Information Theoretic Security, Amsterdam, the Netherlands, May 22, 2011.
- The decoupling theorem (invited talk), QCS Project Workshop, Riga, Latvia, May 20, 2011.
- The uncertainty principle in the presence of quantum memory (invited talk), KCIK Symposium 2011, Sopot, Poland, May 14, 2011.
- How fundamental is the uncertainty principle? (invited talk), Conference on Conceptual Foundations and Foils for Quantum Information Processing, Waterloo, Canada, May 12, 2011.
- What does quantum information theory tell us about thermodynamics? (invited talk), QIPA 2011, Allahabad, India, February 19, 2011.
- Informatik als wissenschaftliche Denkweise, SCHILW-Tag (Lehrerfortbildung), Kantonsschule Alpenquai, Lucerne, Switzerland, January 27, 2011.
- Theory of quantum cryptography (keynote speech), Winter School on Quantum Cryptography, Les Diablerets, Switzerland, January 19, 2011.
- A quantum information-theoretic perspective on thermodynamics, Physics Colloquium, University of Düsseldorf, Germany, December 16, 2010.
- Information als Grundbaustein des Universums, Ringvorlesung der Wissenschaftshistorischen Kommission, ETH Zurich, Switzerland, November 9, 2010.
- Cryptography without trusted devices (invited talk), Workshop on Post-Quantum Security Models, Paris, France, October 11, 2010,
- On the non-extendibility of quantum theory, Workshop on New Directions in Quantum Theory, ETH Zurich, Switzerland, July 29, 2010.
- Quantum cryptography (invited tutorial), Advanced School in Quantum Information Processing and Quantum Cryptography, Montreal, Canada, June 21 and June 22, 2010.
- Tomography with finite data and implications to quantum cryptography (invited talk), Workshop on Theory and Realisation of Practical Quantum Key Distribution, Waterloo, Canada, June 16, 2010.
- Randomness extraction relative to quantum information (invited talk), 7th Central European Quantum Information Processing Workshop (CEQIP), Valtice, Czech Republic, June 4, 2010.
- Provable post-quantum security (invited talk), International Workshop on Post-Quantum Cryptography, Darmstadt, Germany, May 26, 2010.
- The non-extendibility of quantum theory, CoQuS Colloquium, University of Vienna, Austria, May 3, 2010.
- Min-entropy sampling (invited talk), Workshop on Cryptography from Storage Imperfections, Caltech, USA, March 21, 2010.
- Basic principles of quantum-secured key agreement (keynote speech), Winter School on Quantum Cryptography, Les Diablerets, Switzerland, February 10, 2010.

- Why should cryptographers care about quantum physics? (keynote lecture), Quantum Communication Workshop 2010, Oslo, Norway, February 1, 2010.
- Quantum key distribution secure against hacking attacks, Université de Montréal, Montreal, Canada, December 22, 2009.
- Quanteninformation, Collegium generale, University of Berne, Switzerland, December 16, 2009.
- Security against quantum mechanical adversaries (invited talk), International Conference on Quantum Communication and Quantum Networking, Sorrento Peninsula, Naples, Italy, October 26, 2009.
- Quantum cryptography, Security Zone Meeting, Zurich, Switzerland, September 23, 2009.
- Security of continuous variable quantum cryptography (invited talk), NATO Advanced Research Workshop on Quantum Cryptography and Computing: Theory and Implementation, Gdansk, Poland, September 9, 2009.
- Optimal decoupling (invited talk), International Congress on Mathematical Physics, Prague, Czech Republic, August 6, 2009.
- De Finetti and entropies (invited talk), Workshop on Quantum Marginals and Density Matrices, Fields Institute, Canada, July 29, 2009.
- Smooth entropies (invited talk), Cambridge Summer Workshop on Quantum Information Theory, Cambridge, United Kingdom, July 6, 2009.
- Postselection as a tool in quantum information (invited talk), 4th Feynman Festival, Olomouc, Czech Republic, June 23, 2009.
- Security against quantum adversaries, Distinguished Lecture Series of the Center for Advanced Security Research, University of Darmstadt, Germany, June 4, 2009.
- Quantum attacks against non-quantum cryptosystems, Information Security Seminar, Royal Holloway University of London, United Kingdom, May 7, 2009.
- Beyond standard quantum information theory, Theory Seminar, University of Basel, Switzerland, April 2, 2009.
- Aspects of security in quantum cryptography (invited tutorial), Winter School on Quantum Key Distribution, Les Diablerets, Switzerland, January 21, 2009.
- Non-asymptotic information theory (invited talk), 423. Wilhelm und Else Heraeus-Seminar, Bad Honnef, Germany, November 5, 2008.
- Fundamentals of quantum information security (invited talk), SECOQC QKD Conference, Vienna, Austria, October 9, 2008.
- Entropy sampling (invited talk), 9th International Conference on Quantum Communication, Measurement and Computing (QCMC), Calgary, Canada, August 23, 2008.
- Security proofs in quantum cryptography (invited tutorial), Information Security in a Quantum World, Summer School, Waterloo, Canada, August 9, 2008.
- Induction and quantum cryptography (invited talk), 5th European Congress of Mathematics (ECM), Mini-Symposium on Mathematics of Cryptology, Amsterdam, the Netherlands, July 16, 2008.
- Future directions in provably secure cryptography (keynote speech), International Cryptology Workshop and Conference 2008, Kuala Lumpur, Malaysia, June 11, 2008.

- Provable security in cryptography (invited tutorial), International Cryptology Workshop and Conference 2008, Kuala Lumpur, Malaysia, June 9, 2008.
- Extracting classical randomness in a quantum world (invited talk), IEEE Information Theory Workshop (ITW), Porto, Portugal, May 9, 2008.
- On induction in quantum mechanics, Seminar in Theoretical Physics, Geneva, Switzerland, April 18, 2008.
- Quantum versions of de Finetti's theorem, Winter Meeting in Mathematical Physics, Zurich, Switzerland, February 22, 2008.
- Quantum extractors (invited talk), Third Workshop on Theory of Quantum Computation, Communication, and Cryptography (TQC), Tokyo, Japan, February 1, 2008.
- Generalized entropies (invited talk), Eleventh Workshop on Quantum Information Processing (QIP), New Delhi, India, December 20, 2007.
- Symmetries and the interpretation of experimental data (invited talk), Twelfth Congress of Philosophy and Foundations of Science, New Delhi, India, December 19, 2007.
- On the difficulty of extracting randomness from partially untrusted quantum devices, Seminar at HP Labs Bristol, United Kingdom, December 5, 2007.
- Tutorial in information-theoretic and quantum cryptography (invited tutorial), EIDMA/DIAMANT minicourse, Eindhoven, the Netherlands, October 8–12, 2007.
- De Finetti theorems as a precondition to doing science (invited talk), Workshop on Operational Probabilistic Theories as Foils to Quantum Theory, Cambridge, United Kingdom, July 9, 2007.
- Tutorial in quantum cryptography (invited tutorial), Seventh Canadian Summer School on Quantum Information, Waterloo, Canada, May 27–31, 2007.
- Can we justify the i.i.d. assumption? (invited talk), International Conference on Information Theoretic Security (ICITS), Madrid, Spain, May 26, 2007.
- Non-asymptotic quantum information theory, Seminar at the National University of Singapore, Singapore, April 26, 2007.
- Symmetrie impliziert Unabhängigkeit (invited talk), Jahrestreffen des Beirats der Universitätsprofessorinnen und -professoren in der Gesellschaft für Informatik (GIBU), Dagstuhl, Germany, April 3, 2007.
- Tutorial in quantum cryptography (invited tutorial), Theory of Cryptography Conference (TCC), Amsterdam, the Netherlands, February 24, 2007.
- Tutorial in quantum key distribution, QUROPE Winter School, Obergurgl, Austria, February 18–24, 2007
- Quantum information theory without independence assumptions (invited talk), Southwest Quantum Information and Technology Workshop (SQuInT), Pasadena, USA, February 17, 2007.
- Security proof of quantum cryptography based on information-theoretic arguments, Seminar at the Max Planck Institute für Informatik, Germany, November 28, 2006.
- How secure is quantum key distribution? (invited talk), Quantum Cryptography and Computing Workshop, Fields Institute, Canada, October 3, 2006.
- An information-theoretic view on quantum cryptography, Swiss Federal Institute of Technology, Switzerland, September 11, 2006.

- Symmetry implies independence, National University of Singapore, Singapore, August 3, 2006.
- Security of quantum key distribution, GI Dissertationspreis-Kolloquium, Dagstuhl, Germany, May 23, 2006.
- Quantum information theory (invited talk), Gordon Research Conference on Quantum Information Science, Il Ciocco, Italy, May 10, 2006.
- A de Finetti representation theorem for finite symmetric quantum states, Seminar at Royal Holloway, University of London, United Kingdom, January 26, 2006.
- An exponential de Finetti theorem and its applications to quantum cryptography (invited talk), Workshop on Quantum Information Processing (QIP), Paris, France, January 18, 2006.
- Quantum key distribution and composability (invited talk), Workshop on Classical and Quantum Information Security, California Institute of Technology, Pasadena, USA, December 17, 2005.
- A quantum de Finetti theorem, Seminar at the University of Bristol, United Kingdom, November 9, 2005.
- Tutorial in information-theoretic and quantum cryptography (invited tutorial), ECRYPT Autumn School, Bertinoro, Italy, October 16–21, 2005.
- Security of quantum key distribution (invited lecture series), SECOQC-QIT Meeting, Erlangen, Germany, from October 10 to October 14, 2005.
- De Finetti representation for symmetric quantum states (invited talk), Being Bayesian in a Quantum World (Workshop), Konstanz, Germany, August 2, 2005.
- Tutorial in quantum cryptography (invited lecture series), Workshop on Information Measures in Quantum Cryptography, Bellairs Research Institute, Barbados, from March 7 to March 12, 2005.
- Universally composable privacy amplification against quantum adversaries, Theory of Cryptography Conference (TCC), Cambridge, Massachusetts, USA, February 12, 2005.
- A new security proof for QKD protocols, Université de Montréal, Montreal, Canada, February 7, 2005.
- A de Finetti representation theorem and applications to QKD, University of Waterloo, Waterloo, Canada, January 7, 2005.
- Privacy amplification against quantum adversaries, Quantum Cryptography Workshop, University of Cambridge, United Kingdom, September 6, 2004.
- Smooth Rényi entropy and applications, IEEE International Symposium on Information Theory (ISIT), Chicago, Illinois, USA, June 29, 2004.
- Privacy amplification secure against an enemy with selectable knowledge, IEEE International Symposium on Information Theory (ISIT), Chicago, Illinois, USA, June 28, 2004.
- The exact price for unconditionally secure asymmetric cryptography, EUROCRYPT 2004, Interlaken, Switzerland, May 3, 2004.
- Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology, Theory of Cryptography Conference (TCC), Cambridge, Massachusetts, USA, February 19, 2004.
- On the power of quantum memory (invited talk), Quantum Information Workshop, Barcelona, Spain, January 8, 2004.

- Relating quantum entanglement and classical correlation, Seminar at the University of Cambridge, United Kingdom, May 27, 2003.
- New bounds in secret-key agreement: the gap between formation and secrecy extraction, EUROCRYPT 2003, Warsaw, Poland, May 8, 2003.
- Towards characterizing the non-locality of entangled quantum states, Université de Montréal, Montreal, Canada, February 24, 2003.
- New bounds in secret-key agreement, bound entanglement, and bound information, McGill University, Montreal, Canada, February 20, 2003.
- About the mutual (conditional) information, IEEE International Symposium on Information Theory (ISIT), Lausanne, Switzerland, July 4, 2002.
- Generalized indistinguishability, IEEE International Symposium on Information Theory (ISIT), Lausanne, Switzerland, July 4, 2002.
- Linking secret key agreement and quantum distillation, Quantum Computing Workshop, Geneva, Switzerland, May 3, 2002.
- Kryptographie und andere Paradoxa, Tag der Schweizer Informatikolympiade, ETH Zurich, Switzerland, April 18, 2002.
- Secret-key agreement and the link to quantum information theory, Université de Montréal, Montreal, Canada, January 25, 2002.

Additional Professional Activities

- Head of the Strategy Committee of the Department of Physics of ETH Zurich; since 2018.
- Head of the Institute for Theoretical Physics; 2013 – 2015.
- Member of the ETH Aufnahmeprüfungskommission; since 2008.
- Member of selection committees (Wahlvorbereitungskommissionen) in the Departments ITET, Mathematics, and Physics.
- Organiser of the joint Zurich Theory Colloquium of the University and ETH Zurich; 2012 – 2018.
- Organisation of several workshops at ETH Zurich (see below).
- Expert for matura exams at the Kantonsschule Schaffhausen; 2007 – 2010.
- Member of the Schulkommission Kantonsschule Büelrain, Winterthur; 2010 – 2019.

Organisation of Conferences and Workshops

- Coordinator of the Program "Quantum Physics of Information" at the Kavli Institute for Theoretical Physics, Santa Barbara, USA, from September to December 2017.
- Co-organiser of the Special Session on Quantum Information of the *QMath13 Conference*, Atlanta, United States, October 2016.
- Co-organiser of the *Workshop on the Foundations of Randomness*, Stellenbosch Institute for Advanced Study, South Africa, October 2015.
- Co-organiser of the *Workshop Beyond I.I.D. in Information Theory*, Banff International Research Station, Canada, July 2015.
- Co-organiser of the *ITS Workshop on the Foundations of Quantum Mechanics*, ETH Zurich, October 2014.
- Co-organiser of the *First Workshop on Quantum Information and Foundations of Thermodynamics*, ETH Zurich, August 2011.
- Co-organiser of the *Workshop on Fundamentals of Physics and Information*, ETH Zurich, June 2010.
- Main Organiser of the *13th Conference on Quantum Information Processing (QIP 2010)*, ETH Zurich, January 2010.
- Co-organiser of the *8th Symposium of Topological Quantum Computing*, ETH Zurich, August 2009.
- Co-organiser of the *Workshop on Information Primitives and Laws of Nature*, ETH Zurich, May 2008.

Membership of Scientific Committees

- Various technical program committees for workshops and conferences, including the *IEEE International Symposium on Information Theory (ISIT) 2008 and 2015*, the *International Conference on Information Theoretic Security (ICITS) 2008* and *2009*, *CRYPTO 2008, 2009,* and *2012*, *EUROCRYPT 2011*, the *Workshop on Theory of Quantum Computation, Communication, and Cryptography (TQC) 2009* and *2012*, the *Conference on Quantum Information Processing (QIP) 2012* and *2016*, and the *Conference for Quantum Information Processing and Communication (QIPC) 2011*.
- Program Chair of the *5th Conference on Quantum Cryptography (QCRYPT 2015)*.
- Program Chair of the *Seventeenth Conference on Quantum Information Processing (QIP 2014)*.
- Vice Chair of the European COST Action *Thermodynamics in the Quantum Regime* (MP1209); from 2013 to 2017.
- Steering Committee of the *Conference on Quantum Cryptography (QCRYPT)*; from 2010 to 2012.
- Steering Committee of the *Conference on Quantum Information Processing (QIP)*; from 2008 until 2011, and since 2016.
- C18 Commission on "Mathematical Physics" of the *International Union of Pure and Applied Physics (IUPAP)*; from 2008 to 2014.

Publications

151. Mirjam Weilenmann, Lea Krämer, Philippe Faist, and Renato Renner, Smooth entropy in axiomatic thermodynamics, in "Thermodynamics in the Quantum Regime," Springer, April 2019.

150. Ernest Y.-Z. Tan, Charles C.-W. Lim, and Renato Renner, Advantage distillation for device-independent quantum key distribution, arXiv:1903.10535, March 2019.

149. Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, Simple and tight device-independent security proofs, *SIAM Journal on Computing*, vol. 48, pp. 181–225, February 2019.

148. David Sutter and Renato Renner, Necessary criterion for approximate recoverability, *Annales Henri Poincaré*, vol. 19, pp. 3007–3029, October 2018.

147. Marius Junge, Renato Renner, David Sutter, Mark M. Wilde, and Andreas Winter, Universal recovery maps and approximate sufficiency of quantum relative entropy, *Annales Henri Poincaré*, vol. 19, pp. 2955–2978, October 2018.

146. Daniela Frauchiger and Renato Renner, Quantum theory cannot consistently describe the use of itself, *Nature Communications*, vol. 9, 3711, September 2018.

145. Jinzhao Wang, Volkher B. Scholz, and Renato Renner, Confidence polytopes in quantum state tomography, arXiv:1808.09988, August 2018.

144. Raban Iten, Tony Metger, Henrik Wilming, Lidia del Rio, and Renato Renner, Discovering physical concepts with neural networks, arXiv:1807.10300, July 2018.

143. Sandra Stupar, Christian Klumpp, Renato Renner, and Nicolas Gisin, Performance of stochastic clocks in the Alternate Ticks Game, arXiv:1806.08812, June 2018.

142. Mischa P. Woods, Ralph Silva, Gilles Pütz, Sandra Stupar, and Renato Renner, Quantum clocks are more accurate than classical ones, arXiv:1806.00491, June 2018.

141. Christian Matt, Ueli Maurer, Christopher Portmann, Renato Renner, and Björn Tackmann, Toward an algebraic theory of systems, *Theoretical Computer Science*, vol. 747, 1–25, June 2018.

140. Siddarth Koduru Joshi *et al.*, Space QUEST mission proposal: experimentally testing decoherence due to gravity, *New Journal of Physics*, vol. 20, 063016, June 2018.

139. Philippe Faist and Renato Renner, Fundamental work cost of quantum processes, *Physical Review X*, vol. 8, 021011, April 2018.

138. Philipp Kammerlander and Renato Renner, The zeroth law of thermodynamics is redundant, arXiv:1804.09726, April 2018.

137. Shima Bab Hadiashar, Ashwin Nayak, and Renato Renner, Communication complexity of one-shot remote state preparation, *IEEE Transactions on Information Theory*, vol. 64, pp. 4709–4728, March 2018.

136. Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick, Practical device-independent quantum cryptography via entropy accumulation, *Nature Communications*, vol. 9, 459, January 2018.

135. Elisa Bäumer, Martí Perarnau-Llobet, Philipp Kammerlander, and Renato Renner, Partial thermalizations allow for optimal thermodynamic processes, arXiv:1712.07128, December 2017.

134. David Sutter, Volkher B. Scholz, and Renato Renner, Approximate degradable quantum channels, *IEEE Transactions on Information Theory*, vol. 63, pp. 7832–7844, December 2017.

133. Daniela Frauchiger and Renato Renner, A non-probabilistic substitute for the Born rule, arXiv:1710.05033, October 2017.

132. Christopher Portmann, Christian Matt, Ueli Maurer, Renato Renner, and Björn Tackmann, Causal Boxes: Quantum information-processing systems closed under composition, *IEEE Transactions on Information Theory*, vol. 63, pp. 3277–3305, May 2017.

131. Christian Majenz, Mario Berta, Frédéric Dupuis, Renato Renner, and Matthias Christandl, Catalytic decoupling of quantum information, *Physical Review Letters*, vol. 118, 080503, February 2017.

130. Roger Colbeck and Renato Renner, A system's wave function is uniquely determined by its underlying physical state, *New Journal of Physics*, vol. 19, 013016, January 2017.

129. Mirjam Weilenmann, Lea Krämer, Philippe Faist, Renato Renner, Axiomatic relation between thermodynamic and information-theoretic entropies, *Physical Review Letters*, vol. 117, 260601, December 2016.

128. Ueli Maurer and Renato Renner, From indifferentiability to constructive cryptography (and back), Proceedings of the Fourteenth IACR Theory of Cryptography Conference, *Lecture Notes in Computer Science*, Springer, vol. 9985, pp. 3–24, November 2016.

127. Lidia del Rio, Adrian Hutter, Renato Renner, and Stephanie Wehner, Relative thermalization, *Physical Review E*, vol. 94, 022104, August 2016.

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

125. Frédéric Dupuis, Omar Fawzi, and Renato Renner, Entropy accumulation, arXiv:1607.01796, July 2016.

124. Philippe Faist and Renato Renner, Practical and reliable error bars in quantum tomography, *Physical Review Letters*, vol. 117, 010404, July 2016.

123. Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick, Non-signalling parallel repetition using de Finetti reductions, *IEEE Transactions on Information Theory*, vol. 62, pp. 1440–1457, March 2016.

122. David Sutter, Omar Fawzi, and Renato Renner, Universal recovery map for approximate Markov chains, *Proceedings of the Royal Society A*, vol. 472, 20150623, February 2016.

121. David Sutter, Tobias Sutter, Peyman M. Esfahani, and Renato Renner, Efficient approximation of quantum channel capacities, *IEEE Transactions on Information Theory*, vol. 62, pp. 578–598, January 2016.

120. Roger Colbeck and Renato Renner, The completeness of quantum theory for predicting measurement outcomes, in "Quantum Theory: Informational Foundations and Foils," *Fundamental Theories of Physics*, Springer, vol. 181, pp. 497–528, December 2015.

119. Omar Fawzi and Renato Renner, Quantum conditional mutual information and approximate Markov chains, *Communications in Mathematical Physics*, vol. 340, pp. 575-611, December 2015.

118. Lidia del Rio, Lea Kraemer, Renato Renner, Resource theories of knowledge, arXiv:1511.08818, November 2015.

117. Philippe Faist, Frédéric Dupuis, Jonathan Oppenheim, and Renato Renner, The minimal work cost of information processing, *Nature Communications*, vol. 6, 7669, July 2015.

116. Dario Egloff, Oscar Dahlsten, Renato Renner, and Vlatko Vedral, A measure of majorization emerging from single-shot statistical mechanics, *New Journal of Physics*, vol. 17, 073001, July 2015.

115. Sandra Ranković, Yeong-Cherng Liang, and Renato Renner, Quantum clocks and their synchronisation — the Alternate Ticks Game, arXiv:1506.01373, June 2015.

114. Rotem Arnon-Friedman and Renato Renner, de Finetti reductions for correlations, *Journal of Mathematical Physics*, vol. 56, 052203, May 2015.

113. Philippe Faist, Jonathan Oppenheim, and Renato Renner, Gibbs-preserving maps outperform thermal operations in the quantum regime, *New Journal of Physics*, vol. 17, 043003, April 2015.

112. Roger Colbeck and Renato Renner, On the sufficiency of the wavefunction, in "The Message of Quantum Science," *Lecture Notes in Physics*, Springer, vol. 899, pp. 65–93, January 2015.

111. Romain Alléaume, Cyril Branciard, Jan Bouda, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, Philippe Grangier, Thomas Länger, Norbert Lütkenhaus, Christian Monyk, Philippe Painchault, Momtchil Peev, Andreas Poppe, Thomas Pornin, John Rarity, Renato Renner, Gregoire Ribordy, Michel Riguidel, Louis Salvail, Andrew Shields, Harald Weinfurter, and Anton Zeilinger, Using quantum key distribution for cryptographic purposes: A survey, *Theoretical Computer Science*, vol. 560, 62–81, December 2014.

110. Vedran Dunjko, Joseph F. Fitzsimons, Christopher Portmann, and Renato Renner, Composable security of delegated quantum computation, in "Advances in Cryptology — ASIACRYPT 2014," *Lecture Notes in Computer Science*, Springer, vol. 8874, pp. 406–425, December 2014.

109. Christopher Portmann and Renato Renner, Cryptographic security of quantum key distribution, arXiv:1409.3525, September 2014.

108. Lluís Masanes, Renato Renner, Matthias Christandl, Andreas Winter, and Jonathan Barrett, Full security of quantum key distribution from no-signaling constraints, *IEEE Transactions on Information Theory*, vol. 60, pp. 4973–4986, August 2014.

107. Felipe Lacerda, Joseph M. Renes, and Renato Renner, Classical leakage resilience from fault-tolerant quantum computation, arXiv:1404.7516, April 2014.

106. Frédéric Dupuis, Mario Berta, Jürg Wullschleger, and Renato Renner, One-shot decoupling, *Communications in Mathematical Physics*, vol. 328, pp. 251–284, March 2014.

105. Artur Ekert and Renato Renner, The ultimate physical limits of privacy, *Nature*, vol. 507, pp. 443–447, March 2014.

104. Nikola Ciganović, Normand J. Beaudry, and Renato Renner, Smooth max-information as one-shot generalization for mutual information, *IEEE Transactions on Information Theory*, vol. 60, pp. 1573–1581, March 2014.

103. Nilanjana Datta, Joseph M. Renes, Renato Renner, and Mark M. Wilde, One-shot lossy quantum data compression, *IEEE Transactions on Information Theory*, vol. 59, pp. 8057–8076, December 2013.

102. David Sutter, Joseph M. Renes, and Renato Renner, Efficient one-way secret-key agreement and private channel coding via polarization, in "Advances in Cryptology — ASIACRYPT 2013," *Lecture Notes in Computer Science*, Springer, vol. 8269, pp. 194–213, December 2013.

101. Normand J. Beaudry, Marco Lucamarini, Stefano Mancini, Renato Renner, Security of two-way quantum key distribution, *Physical Review A*, vol. 88, 062302, December 2013.

100. Daniela Frauchiger, Renato Renner, and Matthias Troyer, True randomness from realistic quantum devices, arXiv:1311.4547, November 2013.

99. Renato Renner, Quantum information: From bits to solids, *Nature Physics (News & Views)*, vol. 9, pp. 697–698, November 2013.

98. Daniela Frauchiger and Renato Renner, Truly random number generation: an example, in "Proceedings of SPIE, Emerging Technologies in Security and Defence," vol. 8899, October 2013.

97. Charles Ci Wen Lim, Christopher Portmann, Marco Tomamichel, Renato Renner, and Nicolas Gisin, Device-independent quantum key distribution with local Bell test, *Physical Review X*, vol. 3, 031006, July 2013.

96. David Sutter, Joseph M. Renes, Frédéric Dupuis, and Renato Renner, Efficient quantum channel coding scheme requiring no preshared entanglement, in "Proceedings of the 2013 International Symposium on Information Theory," IEEE, pp. 354–358, July 2013.

95. Alexander Vitanov, Frédéric Dupuis, Marco Tomamichel, and Renato Renner, Chain rules for smooth min- and max-entropies, *IEEE Transactions on Information Theory*, vol. 59, pp. 2603–2612, May 2013.

94. Renato Renner and Stefan Wolf, Towards characterizing the non-locality of entangled quantum states, *Theoretical Computer Science*, vol. 486, pp. 50–60, May 2013.

93. Esther Hänggi, Renato Renner, and Stefan Wolf, The impossibility of non-signaling privacy amplification, *Theoretical Computer Science*, vol. 486, pp. 27–42, May 2013.

92. Oleg Szehr, Frédéric Dupuis, Marco Tomamichel, and Renato Renner, Decoupling with unitary approximate two-designs, *New Journal of Physics*, vol. 15, 053022, May 2013.

91. Stefan Hengl, Johan Åberg, and Renato Renner, Directed quantum communication, *New Journal of Physics*, vol. 15, 033025, March 2013.

90. Roger Colbeck and Renato Renner, A short note on the concept of free choice, arXiv:1302.4446, February 2013.

89. Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J. Cerf, Security of continuous-variable quantum key distribution against general attacks, *Physical Review Letters*, vol. 110, 030502, January 2013.

88. Frédéric Dupuis, Lea Kraemer, Philippe Faist, Joseph M. Renes, and Renato Renner, Generalized entropies, *Proceedings of the XVIIth International Congress on Mathematical Physics*, pp. 134-153, November 2012.

87. Renato Renner, Reply to recent scepticism about the foundations of quantum cryptography, arXiv: 1209.2423, September 2012.

86. Matthias Christandl and Renato Renner, Reliable quantum state tomography, *Physical Review Letters*, vol. 109, 120403, September 2012.

85. Anindya De, Christopher Portmann, Thomas Vidick, Renato Renner, Trevisan's extractor in the presence of quantum side information, *SIAM Journal on Computing*, vol. 41, pp. 915–940, August 2012.

84. Joseph M. Renes, Frédéric Dupuis, and Renato Renner, Efficient polar coding of quantum information, *Physical Review Letters*, vol. 109, 050504, August 2012.

83. David Sutter, Joseph M. Renes, Frédéric Dupuis, and Renato Renner, Achieving the capacity of any DMC using only Polar Codes, in "Proceedings of the 2012 IEEE Information Theory Workshop," IEEE, pp. 114–118, August 2012.

82. Terence E. Stuart, Joshua A. Slater, Roger Colbeck, Renato Renner, and Wolfgang Tittel, Experimental bound on the maximum predictive power of physical theories, *Physical Review Letters*, vol. 109, 020402, July 2012.

81. Renato Renner and Stefan Wolf, Ernst Specker and the hidden variables, *Elemente der Mathematik*, vol. 67, pp. 1–12, July 2012.

80. Oscar Dahlsten, Daniel Lercher, and Renato Renner, Tsirelson's bound from a generalised data processing inequality, *New Journal of Physics*, vol. 14, 063024, June 2012.

79. Roger Colbeck and Renato Renner, Free randomness can be amplified, *Nature Physics*, vol. 8, pp. 450–454, May 2012.

78. Ligong Wang and Renato Renner, One-shot classical-quantum capacity and hypothesis testing, *Physical Review Letters*, vol. 108, 200501, May 2012.

77. Normand Beaudry and Renato Renner, An intuitive proof of the data processing inequality, *Quantum Information and Computation*, vol. 12, pp. 432–441, May 2012.

76. Roger Colbeck and Renato Renner, Is a system's wave function in one-to-one correspondence with its elements of reality?, *Physical Review Letters*, vol. 108, 150402, April 2012.

75. Joseph M. Renes and Renato Renner, One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys, *IEEE Transactions on Information Theory*, vol. 58, pp. 1985–1991, March 2012.

74. Renato Renner, The fridge gate, *Nature (News & Views)*, vol. 482, pp. 164–165, February 2012.

73. Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner, Tight finite-key analysis for quantum cryptography, *Nature Communications*, vol. 3, 634, January 2012.

72. Renato Renner, Information security in a quantum world, "Mathematical and Engineering Methods in Computer Science — MEMICS 2011," *Lecture Notes on Computer Science*, Springer, vol. 7119, pp. 57–62, January 2012.

71. Joseph M. Renes and Renato Renner, Noisy channel coding via privacy amplification and information reconciliation, *IEEE Transactions on Information Theory*, vol. 57, pp. 7377–7385, November 2011.

70. Roger Colbeck and Renato Renner, No extension of quantum theory can have improved predictive power, *Nature Communications*, vol. 2, 411, August 2011.

69. Severin Winkler, Marco Tomamichel, Stefan Hengl, and Renato Renner, Impossibility of growing quantum bit commitments, *Physical Review Letters*, vol. 107, 090502, August 2011.

68. Mario Berta, Matthias Christandl, and Renato Renner, The Quantum Reverse Shannon Theorem based on one-shot information theory, *Communications in Mathematical Physics*, vol. 306, pp. 579–615, August 2011.

67. Marco Tomamichel, Christian Schaffner, Adam Smith, and Renato Renner, Leftover hashing against quantum side information, *IEEE Transactions on Information Theory*, vol. 57, pp. 5524–5535, August 2011.

66. Cyril Stark, Lode Pollet, Atac Imamoglu, and Renato Renner, Localization of toric code defects, *Physical Review Letters*, vol. 107, 030504, July 2011.

65. Robert König and Renato Renner, Sampling of min-entropy relative to quantum knowledge, *IEEE Transactions on Information Theory*, vol. 57, pp. 4760–4787, July 2011.

64. Lidia del Rio, Johan Aberg, Renato Renner, Oscar Dahlsten, and Vlatko Vedral, The thermodynamic meaning of negative entropy, *Nature*, vol. 474, pp. 61–63, June 2011.

63. Fabian Furrer, Johan Aberg, and Renato Renner, Min- and max-entropy in infinite dimensions, *Communications in Mathematical Physics*, vol. 306, pp. 165-186, June 2011.

62. Oscar Dahlsten, Renato Renner, Elisabeth Rieper, and Vlatko Vedral, Inadequacy of von Neumann entropy for characterising extractable work, *New Journal of Physics*, vol. 13, 053015, May 2011.

61. Renato Renner, Quantum-resilient randomness extraction, in "Information Theoretic Security," *Lecture Notes in Computer Science*, Springer, vol. 6673, pp. 52–57, May 2011.

60. Thomas Holenstein and Renato Renner, On the randomness of independent experiments, *IEEE Transactions on Information Theory*, vol. 57, No. 4, pp. 1865–1871, April 2011.

59. Marco Tomamichel and Renato Renner, Uncertainty relation for smooth entropies, *Physical Review Letters*, vol. 106, 110506, March 2011.

58. Ueli Maurer and Renato Renner, Abstract cryptography, in "Innovations in Computers Science — ICS 2011, Proceedings," pp. 1–21, Tsinghua University Press, January 2011.

57. Esther Hänggi and Renato Renner, Device-independent quantum key distribution with commuting measurements, arXiv:1009.1833, September 2010.

56. Marco Tomamichel, Roger Colbeck, and Renato Renner, Duality between smooth min- and max-entropies, *IEEE Transactions on Information Theory*, vol. 56, pp. 4674–4681, August 2010.

55. Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner, The uncertainty principle in the presence of quantum memory, *Nature Physics*, vol. 6, pp. 659–662, July 2010.

54. Esther Hänggi, Renato Renner, and Stefan Wolf, Efficient device-independent quantum key distribution, in "Advances in Cryptology — EUROCRYPT 2010," *Lecture Notes in Computer Science*, Springer, vol. 6110, pp. 216–234, May 2010.

53. Renato Renner, Simplifying information-theoretic arguments by post-selection, in "Proceedings of the NATO Advanced Research Workshop Quantum Cryptography and Computing: Theory and Implementation," vol. 26, pp. 66–75, February 2010.

52. Marco Tomamichel, Roger Colbeck, and Renato Renner, A fully quantum asymptotic equipartition property, *IEEE Transactions on Information Theory*, vol. 55, pp. 5840–5847, December 2009.

51. Renato Renner, Optimal decoupling, in "Proceedings of the XVI International Congress on Mathematical Physics," pp. 541–545, October 2009.

50. Robert König, Renato Renner, and Christian Schaffner, The operational meaning of min- and max-entropy, *IEEE Transactions on Information Theory*, vol. 55, pp. 4337–4347, September 2009.

49. Jörn Müller-Quade and Renato Renner, Composability in quantum cryptography, *New Journal of Physics*, vol. 11, 085006, August 2009.

48. Roger Colbeck and Renato Renner, Defining the local part of a hidden variable model: a comment, arXiv:0907:4967, July 2009.

47. Renato Renner, Stefan Wolf, and Jürg Wullschleger, Trade-offs in information-theoretic multiparty one-way key agreement, in "Information Theoretic Security," *Lecture Notes in Computer Science*, Springer, vol. 4883, pp. 65–75, August 2009.

46. Nilanjana Datta and Renato Renner, Smooth entropies and the quantum information spectrum, *IEEE Transactions on Information Theory*, vol. 55, pp. 2807–2815, June 2009.

45. Ligong Wang, Roger Colbeck, and Renato Renner, Simple channel coding bounds, in "Proceedings of the 2009 International Symposium on Information Theory," IEEE, pp. 1804–1808, June 2009.

44. Rupert Ursin, Thomas Jennewein, Johannes Kofler, Josep M. Perdigues, Luigi Cacciapuoti, Clovis J. de Matos, Markus Aspelmeyer, Alejandra Valencia, Thomas Scheidl, Alessandro Fedrizzi, Antonio Acin, Cesare Barbieri, Giuseppe Bianco, Caslav Brukner, Jose Capmany, Sergio Cova, Dirk Giggenbach, Walter Leeb, Robert H. Hadfield, Raymond Laflamme, Norbert Lutkenhaus, Gerard Milburn, Momtchil Peev, Timothy Ralph, John Rarity, Renato Renner, Etienne Samain, Nikolaos Solomos, Wolfgang Tittel, Juan P. Torres, Morio Toyoshima, Arturo Ortigosa-Blanch, Valerio Pruneri, Paolo Villoresi, Ian Walmsley, Gregor Weihs, Harald Weinfurter, Marek Zukowski, and Anton Zeilinger, Space-QUEST: Experiments with quantum entanglement in space, *Europhysics News*, vol. 40, pp. 26–29, May 2009.

43. Renato Renner and J. Ignacio Cirac, De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography, *Physical Review Letters*, vol. 102, 110504, March 2009.

42. Matthias Christandl, Robert König, and Renato Renner, Post-selection technique for quantum channels with applications to quantum cryptography, *Physical Review Letters*, vol. 102, 020504, January 2009.

41. Valerio Scarani and Renato Renner, Security bounds for quantum cryptography with finite resources, in "Proceedings of the 3rd Workshop on Theory of Quantum Computation, Communication, and Cryptography, TQC 2008," *Lecture Notes in Computer Science*, Springer, vol. 5106, pp. 83–95, November 2008.

40. Roger Colbeck and Renato Renner, Hidden variable models for quantum theory cannot have any local part, *Physical Review Letters*, vol. 101, 050403, August 2008.

39. Renato Renner, Quantum key distribution, *in* Encyclopedia of Algorithms, Springer, pp. 708–711, June 2008.

38. Valerio Scarani and Renato Renner, Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post-processing, *Physical Review Letters*, vol. 100, 200501, May 2008.

37. Renato Renner, Extracting classical randomness in a quantum world, Proceedings of the IEEE Information Theory Workshop 2008, pp. 360–363, May 2008.

36. Ueli Maurer, Renato Renner, and Stefan Wolf, Unbreakable keys from random noise, *in* Security with Noisy Data, Springer, pp. 21–44, November 2007.

35. Ivan Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner, A tight high-order entropic quantum uncertainty relation with applications, in "Advances in Cryptology — CRYPTO 2007," *Lecture Notes in Computer Science*, Springer, vol. 4622, pp. 360–378, August 2007.

34. Ueli Maurer, Krzysztof Pietrzak, and Renato Renner, Indistinguishability amplification, in "Advances in Cryptology — CRYPTO 2007," *Lecture Notes in Computer Science*, Springer, vol. 4622, pp. 130–149, August 2007.

33. Renato Renner, Symmetry of large physical systems implies independence of subsystems, *Nature Physics*, vol. 3, pp. 645–649, July 2007.

32. Robert König, Renato Renner, Andor Bariska, and Ueli Maurer, Small accessible quantum information does not imply security, *Physical Review Letters*, vol. 98, 140502, April 2007.

31. Matthias Christandl, Robert König, Graeme Mitchison, and Renato Renner, One-and-a-half quantum de Finetti theorems, *Communications in Mathematical Physics*, vol. 273, pp. 473–498, March 2007.

30. Renato Renner, Beweisbare Sicherheit durch Quantenkryptografie, it - Information Technology, Oldenbourg-Wissenschaftsverlag, March 2007.

29. Matthias Christandl, Artur Ekert, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Renato Renner, Unifying classical and quantum key distillation, in "Proceedings of the Theory of Cryptography Conference, TCC 2007," *Lecture Notes in Computer Science*, Springer, vol. 4392, pp. 456–478, February 2007.

28. Barbara Kraus, Cyril Branciard, and Renato Renner, Security of quantum key distribution protocols using two-way classical communication or weak coherent pulses, *Physical Review A*, vol. 75, 012316, January 2007.

27. Yevgeniy Dodis and Renato Renner, On the impossibility of extracting classical randomness using a quantum computer, in "Proceedings of the 33rd International Colloquium on Automata, Languages and Programming," *Lecture Notes in Computer Science*, Springer, vol. 4051, pp. 204–215, July 2006.

26. Renato Renner, Stefan Wolf, and Jürg Wullschleger, The single-serving channel capacity, in "Proceedings of the 2006 IEEE International Symposium on Information Theory," IEEE, pp. 1424–1427, July 2006.

25. Robert König and Renato Renner, A de Finetti representation for finite symmetric quantum states, *Journal of Mathematical Physics*, vol. 46, 122108, December 2005.

24. Renato Renner and Stefan Wolf, Simple and tight bounds for information reconciliation and privacy amplification, in "Advances in Cryptology — ASIACRYPT 2005," *Lecture Notes in Computer Science*, Springer, vol. 3788, pp. 199–216, December 2005.

23. Renato Renner, Security of Quantum Key Distribution, PhD thesis, Diss. ETH No. 16242, available at arXiv:quant-ph/0512258, September 2005. (Appeared in the *International Journal of Quantum Information*, vol. 6, pp. 1–127, February 2008.)

22. Renato Renner, On the variational distance of independently repeated experiments, arXiv:cs.IT/0509013, September 2005.

21. Barbara Kraus, Nicolas Gisin, and Renato Renner, Lower and upper bounds on the secret-key rate for QKD protocols using one-way classical communication, *Physical Review Letters*, vol. 95, 080501, August 2005.

20. Thomas Holenstein and Renato Renner, One-way secret-key agreement and applications to circuit polarization and immunization of public-key encryption, in "Advances in Cryptology — CRYPTO 2005," *Lecture Notes in Computer Science*, Springer, vol. 3621, pp. 478–493, August 2005.

19. Renato Renner, Nicolas Gisin, and Barbara Kraus, Information-theoretic security proof for quantum key distribution protocols, *Physical Review A*, vol. 72, 012332, July 2005.

18. Robert König, Ueli Maurer, and Renato Renner, On the power of quantum memory, *IEEE Transactions on Information Theory*, vol. 51, no. 7, pp. 2391–2401, July 2005.

17. Renato Renner and Robert König, Universally composable privacy amplification against quantum adversaries, in "Proceedings of the Second Theory of Cryptography Conference, TCC 2005," *Lecture Notes in Computer Science*, Springer, vol. 3378, pp. 407–425, February 2005.

16. Renato Renner and Stefan Wolf, Smooth Rényi entropy and applications, in "Proceedings of the 2004 IEEE International Symposium on Information Theory," IEEE, p. 233, June 2004.

15. Matthias Christandl and Renato Renner, On intrinsic information, in "Proceedings of the 2004 IEEE International Symposium on Information Theory," IEEE, p. 135, June 2004.

14. Robert König, Ueli Maurer, and Renato Renner, Privacy amplification secure against an adversary with selectable knowledge, in "Proceedings of the 2004 IEEE International Symposium on Information Theory," IEEE, p. 231, June 2004.

13. Renato Renner and Stefan Wolf, Quantum pseudo-telepathy and the Kochen-Specker theorem, in "Proceedings of the 2004 IEEE International Symposium on Information Theory," IEEE, p. 322, June 2004.

12. Renato Renner and Stefan Wolf, The exact price for unconditionally secure asymmetric cryptography, in "Advances in Cryptology — EUROCRYPT 2004," *Lecture Notes in Computer Science*, Springer, vol. 3027, pp. 109–125, May 2004.

11. Matthias Christandl, Renato Renner, and Artur Ekert, A generic security proof for quantum key distribution, arXiv:quant-ph/0402131, March 2004.

10. Ueli Maurer, Renato Renner, and Clemens Holenstein, Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology, in "Proceedings of the First Theory of Cryptography Conference, TCC 2004," *Lecture Notes in Computer Science*, Springer, vol. 2951, pp. 21–39, February 2004.

9. Renato Renner and Stefan Wolf, Unconditional authenticity and privacy from an arbitrarily weak secret, in "Advances in Cryptology — CRYPTO 2003," *Lecture Notes in Computer Science*, Springer, vol. 2729, pp. 78–95, August 2003.

8. Matthias Christandl, Renato Renner, and Stefan Wolf, A property of the intrinsic mutual information, in "Proceedings of the 2003 IEEE International Symposium on Information Theory," IEEE, p. 258, June 2003.

7. Renato Renner, Juraj Skripsky, and Stefan Wolf, A new measure for conditional mutual information and its properties, in "Proceedings of the 2003 IEEE International Symposium on Information Theory," IEEE, p. 259, June 2003.

6. Renato Renner and Stefan Wolf, New bounds in secret-key agreement: the gap between formation and secrecy extraction, in "Advances in Cryptology — EUROCRYPT 2003," *Lecture Notes in Computer Science*, Springer, vol. 2656, pp. 562–577, May 2003.

5. Nicolas Gisin, Renato Renner, and Stefan Wolf, Linking classical and quantum key agreement: is there a classical analog to bound entanglement?, *Algorithmica*, Springer, vol. 34, no. 4, pp. 389–412, November 2002.

4. Renato Renner and Stefan Wolf, Towards proving the existence of "bound" information, in "Proceedings of the 2002 IEEE International Symposium on Information Theory," IEEE, p. 103, June 2002.

3. Renato Renner and Ueli Maurer, About the mutual (conditional) information, in "Proceedings of the 2002 IEEE International Symposium on Information Theory," IEEE, p. 364, June 2002.

2. Ueli Maurer and Renato Renner, Generalized indistinguishability, in "Proceedings of the 2002 IEEE International Symposium on Information Theory," IEEE, p. 295, June 2002.

1. Nicolas Gisin, Renato Renner, and Stefan Wolf, Bound information: the classical analog to bound quantum entanglement, in "Proceedings of 3ecm, Progress in Mathematics," Birkhäuser Verlag, vol. 202, pp. 439–447, July 2000.

Co-edited books

2. Renato Renner and Sandra Stupar (eds.), Time in Physics, *Tutorials, Schools, and Workshops in the Mathematical Sciences*, Birkhäuser, 2017.

1. Tal Mor and Renato Renner (eds.), Theoretical Aspects of Quantum Cryptography — Celebrating 30 Years of BB84, *Theoretical Computer Science*, vol. 560, Elsevier, 2014.