

Renato Renner

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

Personal Information

Born December 11, 1974, in Lucerne, Switzerland.
Swiss citizen.
Married, two children.
Languages: German, English, French.

Education

- | | |
|-----------|---|
| 2001–2005 | PhD (Dr. sc. nat.), Department of Computer Science, ETH Zurich (Swiss Federal Institute of Technology), Switzerland; Thesis: <i>Security of Quantum Key Distribution</i> (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 (École Polytechnique Fédérale de Lausanne), Switzerland. |
| 1990–1994 | Matura Typus C, Obergymnasium, Kantonsschule Lucerne, Switzerland. |

Employment History

- | | |
|-----------------|---|
| since Oct. 2007 | Assistant professor (tenure track) at the Institute for Theoretical Physics, ETH Zurich, Switzerland. |
| 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

Award for the best dissertation by the German Chapter of the ACM; ETH Medal for my PhD thesis; ETH Medal for my diploma thesis; third prize of the European Union Contest for Young Scientists; Matura-Preis (university entrance exam, award for best results); award for best project at the Young Scientists Contest Switzerland (SJF).

Professional Contributions and Activities

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

- 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, UK, 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, UK, 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 in 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 2008, 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 (invited talk), Bristol, UK, 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, Workshop on Operational Probabilistic Theories as Foils to Quantum Theory, Cambridge, UK, 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, 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) 2007, Dagstuhl, Germany, April 3, 2007.
- Tutorial in quantum cryptography (invited tutorial), Theory of Cryptography Conference (TCC) 2007, 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, Max Planck Institute für Informatik, Germany, November 28, 2006.
- How secure is quantum key distribution?, 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, Royal Holloway, University of London, UK, January 26, 2006.
- An exponential de Finetti theorem and its applications to quantum cryptography (invited talk), Workshop on Quantum Information Processing (QIP) 2006, 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, University of Bristol, UK, November 9, 2005.
- Tutorial in information-theoretic and quantum cryptography, ECRYPT Autumn School, Bertinoro, Italy, October 16–21, 2005.
- Security of quantum key distribution (invited lecture series), SECOQC-QIT Meeting, Erlangen, Germany, October 10–14, 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, Workshop on Information Measures in Quantum Cryptography, Bellairs Research Institute, Barbados, March 7–12, 2005.
- Universally composable privacy amplification against quantum adversaries, Theory of Cryptography Conference (TCC) 2005, 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, UK, September 6, 2004.
- Smooth Rényi entropy and applications, 2004 IEEE International Symposium on Information Theory (ISIT), Chicago, Illinois, USA, June 29, 2004.
- Privacy amplification secure against an enemy with selectable knowledge, 2004 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) 2004, 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, University of Cambridge, UK, 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, 2002 IEEE International Symposium on Information Theory (ISIT), Lausanne, Switzerland, July 4, 2002.
- Generalized indistinguishability, 2002 IEEE International Symposium on Information Theory (ISIT), Lausanne, Switzerland, July 4, 2002.
- Linking secret key agreement and quantum distillation, Quantum Computing Workshop, Université de Genève, 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.

Other Professional Activities

I served as a member of the technical program committees for various workshops and conferences, including the IEEE International Symposium on Information Theory (ISIT) 2008, the International Conference on Information Theoretic Security (ICITS) 2008 and 2009, CRYPTO 2008 and 2009, and the Workshop on Theory of Quantum Computation, Communication, and Cryptography (TQC) 2009. I am also a member of the C18 commission on "Mathematical Physics" of the International Union of Pure and Applied Physics (IUPAP).

I have been co-organizer of several scientific meetings, among them the workshop on *Information Primitives and Laws of Nature*, which has been held in May 2008 at ETH Zurich. In addition, I have been the main organizer of the *13th Workshop on Quantum Information Processing, QIP 2010*, which is the major theory meeting in the area of quantum information and quantum computation. I am currently the chair of the Steering Committee of QIP.

Supervision of Students

- Normand Beaudry, PhD project, ETH Zurich (ongoing).
- Lidia del Rio, PhD project, ETH Zurich (ongoing).
- Cyril Stark, PhD project, ETH Zurich (ongoing).
- Stefan Hengl, PhD project, ETH Zurich (ongoing).

- Marco Tomamichel, PhD project, ETH Zurich (ongoing).
- Dejan Dukaric, PhD project (co-supervised by Stefan Wolf), ETH Zurich (ongoing).
- Daniel Lercher, master project, ETH Zurich (ongoing).
- Oliver Marty, master project, ETH Zurich (ongoing).
- Pascal Neupert, Securely Sharing Any Pure Quantum State, master project, ETH Zurich, 2009.
- Fabian Furrer, Min- and Max-Entropies as Generalized Entropy Measures in Infinite-Dimensional Quantum Systems, master project, ETH Zurich, 2009.
- Fabio Pedrocchi, An Infinite Dimensional Quantum de Finetti Theorem: Tests of Robustness, master project, ETH Zurich, 2009.
- Junji Shimagaki, Numerical Analysis of the Stability of Toric Codes Against Errors, master project, ETH Zurich, 2009
- Dino Burger, Typical Multipartite Correlations, diploma project, ETH Zurich, 2008.
- Mario Berta, Single-Shot Quantum State Merging, diploma project, ETH Zurich, 2008.
- David Gablinger, The Role of Entanglement in Thermodynamics, diploma project, ETH Zurich, 2008.
- Andor Bariska, On the Security of Quantum Keys, diploma project, ETH Zurich, 2005.
- Andreas Streich, Secret-Sharing from Correlated Information, semester project, ETH Zurich, 2005.
- Stefano Tessaro, Information-Theoretically Secure Coin Flipping Through Shared Information, semester project, ETH Zurich, 2004.
- Andreas Meier and Simon Heimlicher, Key Agreement from Arbitrarily Correlated Information, semester project, ETH Zurich, 2004.
- Emil Müller, Security in the Context of Public Adversaries, diploma project, ETH Zurich, 2004.
- Christian Schaffner, Secret-Key Agreement Secure Against Active Adversaries, diploma project, ETH Zurich, 2003.
- Robert König, On the Capacity of Quantum Memory, diploma project, ETH Zurich, 2003.
- Juraj Skripsky, The Gap Between Intrinsic Information and the Secret-Key Rate, diploma project, ETH Zurich, 2002.
- Regina Bischoff, Information-Theoretically Secure Secret-Key Agreement, semester project, ETH Zurich, 2002.
- Matthias Christandl, The Quantum Analog to Intrinsic Information, diploma project, ETH Zurich, 2002.
- Fabian Kuhn, Optimal Information-Theoretically Secure Secret-Key Agreement, diploma project, ETH Zurich, 2001.
- Lukas Peter, On the Intrinsic Information, diploma project, ETH Zurich, 2001.

Publications (five most important marked with ►)

- Anindya De, Christopher Portmann, Thomas Vidick, Renato Renner, Trevisan's extractor in the presence of quantum side information, arXiv:0912.5514, December 2009.
- 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.
- Mario Berta, Matthias Christandl, Renato Renner, A conceptually simple proof of the Quantum Reverse Shannon Theorem, arXiv:0912.3805, December 2009.
- Esther Hnggi, Renato Renner, Stefan Wolf, Quantum cryptography based solely on Bell's theorem, arXiv:0911.4171, November 2009.
- Stefan Hengl, Johan Åberg, and Renato Renner, Directed quantum communication, arXiv:0910.1745, October 2009.
- Renato Renner, Optimal decoupling, to appear in the Proceedings of the XVI International Congress on Mathematical Physics, October 2009.
Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, Renato Renner, An entropic uncertainty relation with quantum side information, arXiv:0909.0950, September 2009.
- 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.
- Jörn Müller-Quade and Renato Renner, Composability in quantum cryptography, New Journal of Physics, vol. 11, 085006, August 2009.
- Oscar Dahlsten, Renato Renner, Elisabeth Rieper, Vlatko Vedral, The work value of information, arXiv:0908.0424, August 2009.
- Marco Tomamichel, Roger Colbeck, and Renato Renner, Duality between smooth min- and max-entropies, arXiv:0907.5238, July 2009.
- Roger Colbeck and Renato Renner, Defining the local part of a hidden variable model: a comment, arXiv:0907.4967, July 2009.
- Nilanjana Datta and Renato Renner, Smooth entropies and the quantum information spectrum, IEEE Transactions on Information Theory, vol. 55, pp. 2807–2815, June 2009.
- Ligong Wang, Roger Colbeck, and Renato Renner, Simple channel coding bounds, Proceedings of the 2009 International Symposium on Information Theory, IEEE, pp. 1804–1808, June 2009.
- Esther Hänggi, Renato Renner, and Stefan Wolf, The impossibility of non-signaling privacy amplification, arXiv:0906.4760, June 2009 (to appear in Theoretical Computer Science, Elsevier).
- Ursin *et al.*, Space-QUEST: Experiments with quantum entanglement in space, Europhysics News, vol. 40, pp. 26–29, May 2009.
- Renato Renner and J. Ignacio Cirac, De Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography, Phys. Rev. Lett., vol. 102, 110504, March 2009.
- Matthias Christandl, Robert König, and Renato Renner, Post-selection technique for quantum channels with applications to quantum cryptography, Phys. Rev. Lett., vol. 102, 020504, January 2009.

- 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.
- ▶ Roger Colbeck and Renato Renner, Hidden variable models for quantum theory cannot have any local part, *Phys. Rev. Lett.*, vol. 101, 050403, August 2008.
- Renato Renner, Quantum key distribution, *in* *Encyclopedia of Algorithms*, Springer-Verlag, pp. 708–711, June 2008.
- Valerio Scarani and Renato Renner, Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post-processing, *Phys. Rev. Lett.*, vol. 100, 200501, May 2008.
- Valerio Scarani and Renato Renner, Security bounds for quantum cryptography with finite resources, *Proceedings of the 3rd Workshop on Theory of Quantum Computation, Communication, and Cryptography, TQC 2008, Lecture Notes in Computer Science*, Springer-Verlag, vol. 5106, pp. 83–95, November 2008.
- Robert König and Renato Renner, Sampling of min-entropy relative to quantum knowledge, *arXiv:0712.4291*, December 2007.
- Ueli Maurer, Renato Renner, and Stefan Wolf, Unbreakable keys from random noise, *in* *Security with Noisy Data*, Springer-Verlag, pp. 21–44, November 2007.
- Ivan Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner, A tight high-order entropic quantum uncertainty relation with applications, *Advances in Cryptology — CRYPTO 2007, Lecture Notes in Computer Science*, Springer-Verlag, vol. 4622, pp. 360–378, August 2007.
- Ueli Maurer, Krzysztof Pietrzak, and Renato Renner, Indistinguishability amplification, *Advances in Cryptology — CRYPTO 2007, Lecture Notes in Computer Science*, Springer-Verlag, vol. 4622, pp. 130–149, August 2007.
- ▶ Renato Renner, Symmetry of large physical systems implies independence of subsystems, *Nature Physics*, vol. 3, pp. 645–649, July 2007.
- Robert König, Renato Renner, Andor Bariska, and Ueli Maurer, Small accessible quantum information does not imply security, *Phys. Rev. Lett.*, vol. 98, 140502, April 2007.
- 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.
- Renato Renner, Beweisbare Sicherheit durch Quantenkryptografie, *it - Information Technology*, Oldenbourg-Wissenschaftsverlag, March 2007.
- Matthias Christandl, Artur Ekert, Michal Horodecki, Pawel Horodecki, Jonathan Oppenheim, and Renato Renner, Unifying classical and quantum key distillation, *Proceedings of the Theory of Cryptography Conference, TCC 2007, Lecture Notes in Computer Science*, Springer-Verlag, vol. 4392, pp. 456–478, February 2007.
- Romain Alléaume *et al.*, SECOQC White paper on quantum key distribution and cryptography, *arXiv:quant-ph/0701168*, January 2007.
- Barbara Kraus, Cyril Branciard, and Renato Renner, Security of quantum key distribution protocols using two-way classical communication or weak coherent pulses, *Phys. Rev. A*, vol. 75, 012316, January 2007.

- Thomas Holenstein and Renato Renner, On the randomness of independent experiments, arXiv:cs.IT/0608007, August 2006.
- Yevgeniy Dodis and Renato Renner, On the impossibility of extracting classical randomness using a quantum computer, Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, Springer-Verlag, pp. 204–215, July 2006.
- Renato Renner, Stefan Wolf, and Jürg Wullschlegler, The single-serving channel capacity, Proceedings of the 2006 IEEE International Symposium on Information Theory, IEEE, pp. 1424–1427, July 2006.
- Robert König and Renato Renner, A de Finetti representation for finite symmetric quantum states, Journal of Mathematical Physics, vol. 46, 122108, December 2005.
- Renato Renner and Stefan Wolf, Simple and tight bounds for information reconciliation and privacy amplification, Advances in Cryptology — ASIACRYPT 2005, Lecture Notes in Computer Science, Springer-Verlag, vol. 3788, pp. 199–216, December 2005.
- Renato Renner, On the variational distance of independently repeated experiments, arXiv:cs.IT/0509013, September 2005.
- ▶ Renato Renner, Security of Quantum Key Distribution, PhD thesis, Diss. ETH No. 16242, arXiv:quant-ph/0512258, September 2005. (Appeared in the International Journal of Quantum Information, vol. 6, pp. 1–127, February 2008).
- Barbara Kraus, Nicolas Gisin, and Renato Renner, Lower and upper bounds on the secret-key rate for QKD protocols using one-way classical communication, Phys. Rev. Lett., vol. 95, 080501, August 2005.
- Thomas Holenstein and Renato Renner, One-way secret-key agreement and applications to circuit polarization and immunization of public-key encryption, Advances in Cryptology — CRYPTO 2005, Lecture Notes in Computer Science, Springer-Verlag, vol. 3621, pp. 478–493, August 2005.
- Renato Renner, Nicolas Gisin, and Barbara Kraus, Information-theoretic security proof for quantum key distribution protocols, Phys. Rev. A, vol. 72, 012332, July 2005.
- 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.
- Renato Renner and Robert König, Universally composable privacy amplification against quantum adversaries, Proceedings of the Second Theory of Cryptography Conference, TCC 2005, Lecture Notes in Computer Science, Springer-Verlag, vol. 3378, pp. 407–425, February 2005.
- Renato Renner and Stefan Wolf, Smooth Rényi entropy and applications, Proceedings of the 2004 IEEE International Symposium on Information Theory, IEEE, p. 233, June 2004.
- Matthias Christandl and Renato Renner, On intrinsic information, Proceedings of the 2004 IEEE International Symposium on Information Theory, IEEE, p. 135, June 2004.
- Robert König, Ueli Maurer, and Renato Renner, Privacy amplification secure against an adversary with selectable knowledge, Proceedings of the 2004 IEEE International Symposium on Information Theory, IEEE, p. 231, June 2004.
- Renato Renner and Stefan Wolf, Quantum pseudo-telepathy and the Kochen-Specker theorem, Proceedings of the 2004 IEEE International Symposium on Information Theory, IEEE, p. 322, June 2004.

- Renato Renner and Stefan Wolf, The exact price for unconditionally secure asymmetric cryptography, *Advances in Cryptology — EUROCRYPT 2004*, Lecture Notes in Computer Science, Springer-Verlag, vol. 3027, pp. 109–125, May 2004.
- Matthias Christandl, Renato Renner, and Artur Ekert, A generic security proof for quantum key distribution, *arXiv:quant-ph/0402131*, March 2004.
- Ueli Maurer, Renato Renner, and Clemens Holenstein, Indifferentiability, impossibility results on reductions, and applications to the random oracle methodology, *Proceedings of the First Theory of Cryptography Conference, TCC 2004*, Lecture Notes in Computer Science, Springer-Verlag, vol. 2951, pp. 21–39, February 2004.
- Renato Renner and Stefan Wolf, Unconditional authenticity and privacy from an arbitrarily weak secret, *Advances in Cryptology — CRYPTO 2003*, Lecture Notes in Computer Science, Springer-Verlag, vol. 2729, pp. 78–95, August 2003.
- Matthias Christandl, Renato Renner, and Stefan Wolf, A property of the intrinsic mutual information, *Proceedings of the 2003 IEEE International Symposium on Information Theory*, IEEE, p. 258, June 2003.
- Renato Renner and Stefan Wolf, Towards characterizing the non-locality of entangled quantum states, *Proceedings of the 2003 IEEE International Symposium on Information Theory*, IEEE, p. 428, June 2003. (An extended version is available at *arXiv:quant-ph/0211019*.)
- Renato Renner, Juraj Skripsky, and Stefan Wolf, A new measure for conditional mutual information and its properties, *Proceedings of the 2003 IEEE International Symposium on Information Theory*, IEEE, p. 259, June 2003.
- Renato Renner and Stefan Wolf, New bounds in secret-key agreement: the gap between formation and secrecy extraction, *Advances in Cryptology — EUROCRYPT 2003*, Lecture Notes in Computer Science, Springer-Verlag, vol. 2656, pp. 562–577, May 2003.
- Nicolas Gisin, Renato Renner, and Stefan Wolf, Linking classical and quantum key agreement: is there a classical analog to bound entanglement?, *Algorithmica*, Springer-Verlag, vol. 34, no. 4, pp. 389–412, November 2002.
- Renato Renner and Stefan Wolf, Towards proving the existence of “bound” information, *Proceedings of the 2002 IEEE International Symposium on Information Theory*, IEEE, p. 103, June 2002.
- Renato Renner and Ueli Maurer, About the mutual (conditional) information, *Proceedings of the 2002 IEEE International Symposium on Information Theory*, IEEE, p. 364, June 2002.
- Ueli Maurer and Renato Renner, Generalized indistinguishability, *Proceedings of the 2002 IEEE International Symposium on Information Theory*, IEEE, p. 295, June 2002.
- Nicolas Gisin, Renato Renner, and Stefan Wolf, Bound information: the classical analog to bound quantum entanglement, *Proceedings of 3ecm*, Progress in Mathematics, Birkhäuser Verlag, vol. 202, pp. 439–447, July 2000.