Joseph M. Renes *Curriculum Vitae*

Institute for Theoretical Physics
ETH Zürich
Wolfgang-Pauli-Str. 27
8093 Zürich, Switzerland

renes@phys.ethz.ch
http://www.phys.ethz.ch/~renes
+41 44 633 70 62

Personal Details

Born 4 July 1977 in Moscow, Idaho, USA. US Citizen. Married, 2 children.

Language abilities: English (native) and German (fluent).

Research Interests

Quantum error-correction & coding, classical & quantum information theory, signal processing & optimization, and uncertainty relations & complementarity.

Education

Habilitation, Theoretical Physics, Technische Universität Darmstadt, 2011.
Thesis: *The Physics of Quantum Information: Complementarity, Uncertainty, and Entanglement.*

PhD, Physics, University of New Mexico, 2004.
Thesis: *Frames, Designs, and Codes in Quantum Information Theory.*
Advisor: Carlton M. Caves.

MS, Physics, University of New Mexico, 2002.

BS with Honor, Physics, California Institute of Technology, 1999.

Academic Employment

2018–present	Senior Scientist (permanent position), ETH Zürich
2012–2017	Senior Assistent Group of Renato Renner, ETH Zürich
2006–2011	Postdoctoral Scholar Group of Gernot Alber, Technische Universität Darmstadt
2005–2006	Postdoctoral Scholar Group of Norbert Lütkenhaus, Universität Erlangen-Nürnberg
2004	Postdoctoral Scholar Group of Thomas Beth, Universität Karlsruhe

Teaching Experience

Quantum Information Theory (Master), ETH Zürich (2022, 2020, 2018, 2017, 2014, 2013)

Quantum Error Correction (Master), ETH Zürich (2022, 2020, 2014)

Quantum Information Theory (Master), TU Darmstadt (2012, 2009)

Electrodynamics (Teacher Candidates – Bachelor; in German), TU Darmstadt (2011).

Student Supervision

ongoing	PhD	Christophe Piveteau
2021	MS	Christian Bertoni, *Information theory and renormalization in statistical mechanics*
2020	MS	Paula Belzig (joint with D. Gross, Cologne), *Studying Stabilizer de Finetti Theorems - Applications in Quantum Information Processing*
2019	MS	Dina Abdelhadi, *Bounds for Quantum Protocols using Partially Smoothed Entropies*
2019	MS	Sami Boulebnane (joint with M. P. Woods), *Quantum clocks and non-demolition measurement*
2018	PhD	David Sutter (joint with R. Renner), *Approximate quantum Markov chains*
2018	MS	Luca Petrović, *Efficiency of Rectangular Shapes of Surface Codes*
2016	MS	Álvaro Piedrafita, *Channel Adapted Decoding Strategies Based on Complementarity*
2016	MS	Raban Iten (joint with D. Sutter), *Relations between different quantum Renyi divergences*
2016	MS	Axel Dahlberg, *Quantum error-correcting codes*
2015	PhD	Felipe Lacerda (visiting student from U. Brasília), *Classical Leakage Resilience from Fault-Tolerant Quantum Computation*
2015	MS	Stefan Huber (joint with V. B. Scholz), *Operationally Motivated Uncertainty Relations for Position and Momentum*
2014	MS	Dominik Waldburger (joint with D. Sutter), *Quantum Polar Codes*
2012	MS	David Sutter (joint with F. Dupuis), *Achieving the Capacity of any DMC using only Polar Codes*

Professional Activities

Member of the steering and admission committees for the Master of Quantum Engineering degree program.

Program committee member, Quantum Information Processing (QIP). 2018, 2019, 2022.

Program committee member, International Symposium on Information Theory (ISIT). 2021.

Editor for Quantum, the open journal for quantum science, 2016-2021.

Referee for the Physical Review, IEEE Transactions on Information Theory, Quantum Information & Computation, Communications in Mathematical Physics, and New Journal of Physics.

Member of the American Physical Society (APS), Deutsche Physikalische Gesellschaft (DPG), and the Institute of Electrical and Electronics Engineers (IEEE).

Co-organizer of the Third International Conference on Quantum Error Correction
www.qec14.ethz.ch

Awards & Honors

Alexander von Humboldt Postdoctoral Fellowship, 2005–2007.

UNM Physics & Astronomy Department Chairman's Award for Best Dissertation, 2005.

Caltech Haren Lee Fisher Memorial Prize in Junior Physics, 1998.

Research Funding

2020–2023 Co-PI *(QuantEOM) Quantum-coherent electro-optic microwave-to-optical conversion with GaP and BaTiO3*, Sinergia grant of the Swiss National Science Foundation.

Books

[1] Joseph M. Renes, *Quantum Information Theory: Concepts and Methods* (De Gruyter Oldenbourg, Berlin, 2022).

Preprints

[4] Philippe Faist, Mischa P. Woods, Victor V. Albert, Joseph M. Renes, Jens Eisert, and John Preskill, "Time-energy uncertainty relation for noisy quantum metrology", 2022, arXiv:2207.13707 [quant-ph].

[3] Joseph M. Renes, "Achievable error exponents of data compression with quantum side information and communication over symmetric classical-quantum channels", 2022, arXiv:2207.08899 [quant-ph].

[2] Joseph M. Renes, "Consistency in the description of quantum measurement: Quantum theory can consistently describe the use of itself", 2021, arXiv:2107.02193 [quant-ph].

[1] Joseph M. Renes and Renato Renner, "Are quantum cryptographic security claims vacuous?", 2020, arXiv:2010.11961 [quant-ph].

Refereed Journal Publications

[53] Christian Bertoni and Joseph M. Renes, "Minimizing couplings in renormalization by preserving short-range mutual information", Journal of Physics A: Mathematical and Theoretical **55**, 375004 (2022), arXiv:2107.00990 [cond-mat.stat-mech].

[52] Christophe Piveteau and Joseph M. Renes, "Quantum message-passing algorithm for optimal and efficient decoding", Quantum **6**, 784 (2022), arXiv:2109.08170 [quant-ph].

[51] Yuxiang Yang, Yin Mo, Joseph M. Renes, Giulio Chiribella, and Mischa P. Woods, "Optimal universal quantum error correction via bounded reference frames", Physical Review Research **4**, 023107 (2022), arXiv:2007.09154 [quant-ph].

[50] Sami Boulebnane, Mischa P. Woods, and Joseph M. Renes, "Waveform Estimation from Approximate Quantum Nondemolition Measurements", Physical Review Letters **127**, 010502 (2021), arXiv:1909.05265 [quant-ph].

[49] Armin Tavakoli, Ingemar Bengtsson, Nicolas Gisin, and Joseph M. Renes, "Compounds of symmetric informationally complete measurements and their application in quantum key distribution", Physical Review Research **2**, 043122 (2020), arXiv:2007.01007 [quant-ph].

[48] Dina Abdelhadi and Joseph M. Renes, "On the Second-Order Asymptotics of the Partially Smoothed Conditional Min-Entropy & Application to Quantum Compression", IEEE Journal on Selected Areas in Information Theory **1**, 416–423 (2020), arXiv:1905.08268 [quant-ph].

[47] Arkin Tikku, Mario Berta, and Joseph M. Renes, "Non-Additivity in Classical-Quantum Wiretap Channels", IEEE Journal on Selected Areas in Information Theory **1**, 526–535 (2020), arXiv:2002.06580 [quant-ph].

[46] Christian Bertoni, Yuxiang Yang, and Joseph M. Renes, "Entropic time–energy uncertainty relations: an algebraic approach", New Journal of Physics **22**, 083010 (2020), arXiv:2001.00799 [quant-ph].

[45] Felipe G. Lacerda, Joseph M. Renes, and Renato Renner, "Classical Leakage Resilience from Fault-Tolerant Quantum Computation", Journal of Cryptology **32**, 1071–1094 (2019), arXiv:1404.7516 [quant-ph].

[44] Joseph M. Renes, "On Privacy Amplification, Lossy Compression, and Their Duality to Channel Coding", IEEE Transactions on Information Theory **64**, 7792–7801 (2018), arXiv:1708.05685 [quant-ph].

[43] Rajai Nasser and Joseph M. Renes, "Polar Codes for Arbitrary Classical-Quantum Channels and Arbitrary cq-MACs", IEEE Transactions on Information Theory **64**, 7424–7442 (2018), arXiv:1701.03397 [quant-ph].

[42] Joseph M. Renes, "Duality of Channels and Codes", IEEE Transactions on Information Theory **64**, 577–592 (2018), arXiv:1701.05583 [quant-ph].

[41] Álvaro Piedrafita and Joseph M. Renes, "Reliable Channel-Adapted Error Correction: Bacon-Shor Code Recovery from Amplitude Damping", Physical Review Letters **119**, 250501 (2017), arXiv:1704.05857 [quant-ph].

[40] Joseph M. Renes, "Better bounds on optimal measurement and entanglement recovery, with applications to uncertainty and monogamy relations", Physical Review A **96**, 042328 (2017), arXiv:1707.01114 [quant-ph].

[39] Joseph M. Renes, "Belief propagation decoding of quantum channels by passing quantum messages", New Journal of Physics **19**, 072001 (2017), arXiv:1607.04833 [quant-ph].

[38] Joseph M. Renes, Volkher B. Scholz, and Stefan Huber, "Uncertainty relations: An operational approach to the error-disturbance tradeoff", Quantum **1**, 20 (2017), arXiv:1612.02051 [quant-ph].

[37] Felipe Lacerda, Joseph M. Renes, and Volkher B. Scholz, "Coherent-state constellations and polar codes for thermal Gaussian channels", Physical Review A **95**, 062343 (2017), arXiv:1603.05970 [quant-ph].

[36] Raban Iten, Joseph M. Renes, and David Sutter, "Pretty good measures in quantum information theory", IEEE Transactions on Information Theory **63**, 1270–1279 (2017), arXiv:1608.08229 [quant-ph].

[35] Joseph M. Renes, "Relative submajorization and its use in quantum resource theories", Journal of Mathematical Physics **57**, 122202 (2016), arXiv:1510.03695 [quant-ph].

[34] Joseph M. Renes, "Uncertainty relations and approximate quantum error correction", Physical Review A **94**, 032314 (2016), arXiv:1605.01420 [quant-ph].

[33] Marco Tomamichel, Mario Berta, and Joseph M. Renes, "Quantum coding with finite resources", Nature Communications **7**, 11419 (2016), arXiv:1504.04617 [quant-ph].

[32] Mark M. Wilde, Joseph M. Renes, and Saikat Guha, "Second-order coding rates for pure-loss bosonic channels", Quantum Information Processing **15**, 1289–1308 (2016), arXiv:1408.5328 [quant-ph].

[31] Joseph M. Renes, David Sutter, and S. Hamed Hassani, "Alignment of Polarized Sets", IEEE Journal on Selected Areas in Communications **34**, 224–238 (2016), arXiv:1411.7925 [quant-ph].

[30] Nicole Yunger Halpern and Joseph M. Renes, "Beyond heat baths: Generalized resource theories for small-scale thermodynamics", Physical Review E **93**, 022126 (2016), arXiv:1409.3998 [quant-ph].

[29] Joseph M. Renes, David Sutter, Frederic Dupuis, and Renato Renner, "Efficient Quantum Polar Codes Requiring No Preshared Entanglement", IEEE Transactions on Information Theory **61**, 6395–6414 (2015), arXiv:1307.1136 [quant-ph].

[28] Mario Berta, Joseph M. Renes, and Mark M. Wilde, "Identifying the Information Gain of a Quantum Measurement", IEEE Transactions on Information Theory **60**, 7987–8006 (2014), arXiv:1301.1594 [quant-ph].

[27] Michael Walter and Joseph M. Renes, "Lower Bounds for Quantum Parameter Estimation", IEEE Transactions on Information Theory **60**, 8007–8023 (2014), arXiv:1310.2155 [quant-ph].

[26] Joseph M. Renes, "Work cost of thermal operations in quantum thermodynamics", The European Physical Journal Plus **129**, 153 (2014), arXiv:1402.3496 [math-ph].

[25] Joseph M. Renes and Mark M. Wilde, "Polar Codes for Private and Quantum Communication Over Arbitrary Channels", IEEE Transactions on Information Theory **60**, 3090–3103 (2014), arXiv:1212.2537 [quant-ph].

[24] Joseph M. Renes, "The Physics of Quantum Information: Complementarity, Uncertainty, and Entanglement", International Journal of Quantum Information **11**, 1330002 (2014), arXiv:1212.2379 [quant-ph].

[23] N. Datta, J.M. Renes, R. Renner, and M.M. Wilde, "One-Shot Lossy Quantum Data Compression", IEEE Transactions on Information Theory **59**, 8057–8076 (2013), arXiv:1304.2336 [quant-ph].

[22] Fernando G. S. L. Brandão, Michał Horodecki, Jonathan Oppenheim, Joseph M. Renes, and Robert W. Spekkens, "Resource Theory of Quantum States Out of Thermal Equilibrium", Physical Review Letters **111**, 250404 (2013), arXiv:1111.3882 [quant-ph].

[21] Joseph M. Renes, Akimasa Miyake, Gavin K. Brennen, and Stephen D. Bartlett, "Holonomic quantum computing in symmetry-protected ground states of spin chains", New Journal of Physics **15**, 025020 (2013), arXiv:1103.5076 [quant-ph].

[20] Joseph M. Renes, Frédéric Dupuis, and Renato Renner, "Efficient Polar Coding of Quantum Information", Physical Review Letters **109**, 050504 (2012), arXiv:1109.3195 [quant-ph].

[19] 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 **58**, 1985–1991 (2012), arXiv:1008.0452 [quant-ph].

[18] Joseph M. Renes and Renato Renner, "Noisy Channel Coding via Privacy Amplification and Information Reconciliation", IEEE Transactions on Information Theory **57**, 7377–7385 (2011), arXiv:1012.4814 [quant-ph].

[17] Joseph M. Renes, "Duality of privacy amplification against quantum adversaries and data compression with quantum side information", Proceedings of the Royal Society A **467**, 1604–1623 (2011), arXiv:1003.0703 [quant-ph].

[16] Stephen D. Bartlett, Gavin K. Brennen, Akimasa Miyake, and Joseph M. Renes, "Quantum Computational Renormalization in the Haldane Phase", Physical Review Letters **105**, 110502 (2010), arXiv:1004.4906 [quant-ph].

[15] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner, "The uncertainty principle in the presence of quantum memory", Nature Physics **6**, 659–662 (2010), arXiv:0909.0950 [quant-ph].

[14] Joseph M. Renes and Jean-Christian Boileau, "Conjectured Strong Complementary Information Tradeoff", Physical Review Letters **103**, 020402 (2009), arXiv:0806.3984 [quant-ph].

[13] Geir Ove Myhr, Joseph M. Renes, Andrew C. Doherty, and Norbert Lütkenhaus, "Symmetric extension in two-way quantum key distribution", Physical Review A **79**, 042329–10 (2009), arXiv:0812.3607 [quant-ph].

[12] Joseph M. Renes and Jean-Christian Boileau, "Physical underpinnings of privacy", Physical Review A **78**, 032335–12 (2008), arXiv:0803.3096 [quant-ph].

[11] Oliver Kern and Joseph M. Renes, "Improved one-way rates for BB84 and 6-state protocols", Quantum Information and Computation **8**, 756–772 (2008), arXiv:0712.1494 [quant-ph].

[10] Graeme Smith, Joseph M. Renes, and John A. Smolin, "Structured Codes Improve the Bennett-Brassard-84 Quantum Key Rate", Physical Review Letters **100**, 170502–4 (2008), arXiv:quant-ph/0607018.

[9] Joseph M. Renes, "Equiangular tight frames from Paley tournaments", Linear Algebra and its Applications **426**, 497–501 (2007), arXiv:math/0408287.

[8] Joseph M. Renes and Graeme Smith, "Noisy Processing and Distillation of Private Quantum States", Physical Review Letters **98**, 020502 (2007), arXiv:quant-ph/0603262.

[7] Joseph M. Renes and Markus Grassl, "Generalized decoding, effective channels, and simplified security proofs in quantum key distribution", Physical Review A **74**, 022317–9 (2006), arXiv:quant-ph/0505061.

[6] Jean-Christian Boileau, Kiyoshi Tamaki, Jamie Batuwantudawe, Raymond Laflamme, and Joseph M. Renes, "Unconditional Security of a Three State Quantum Key Distribution Protocol", Physical Review Letters **94**, 040503–4 (2005), arXiv:quant-ph/0408085.

[5] Joseph M. Renes, "Equiangular spherical codes in quantum cryptography", Quantum Information and Computation **5**, 081–092 (2005), arXiv:quant-ph/0409043.

[4] Joseph M. Renes, "Spherical-code key-distribution protocols for qubits", Physical Review A **70**, 052314 (2004), arXiv:quant-ph/0402135.

[3] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves, "Symmetric informationally complete quantum measurements", Journal of Mathematical Physics **45**, 2171–2180 (2004), arXiv:quant-ph/0310075.

[2] Carlton M. Caves, Christopher A. Fuchs, Kiran K. Manne, and Joseph M. Renes, "Gleason-Type Derivations of the Quantum Probability Rule for Generalized Measurements", Foundations of Physics **34**, 193–209 (2004), arXiv:quant-ph/0306179.

[1] Andrew M. Childs, John Preskill, and Joseph Renes, "Quantum information and precision measurement", Journal of Modern Optics **47**, 155–176 (2000), arXiv:quant-ph/9904021.

Refereed Conference Publications

[21] Christophe Piveteau and Joseph M. Renes, "Quantum message-passing algorithm for optimal and efficient decoding", 2022 IEEE International Symposium on Information Theory (ISIT) (2022), pp. 2225–2230, arXiv:2109.08170 [quant-ph].

[20] July X. Li, Joseph M. Renes, and Pascal O. Vontobel, "Pseudocodeword-based Decoding of Quantum Color Codes", 2021 IEEE International Symposium on Information Theory (ISIT) (2021), pp. 1558–1563, arXiv:2010.10845 [quant-ph].

[19] Dina Abdelhadi and Joseph M. Renes, "Second-order asymptotics of quantum data compression from partially-smoothed conditional entropy", 2020 IEEE International Symposium on Information Theory (ISIT) (2020), pp. 1846–1851, arXiv:1905.08268 [quant-ph].

[18] Arkin Tikku, Joseph M. Renes, and Mario Berta, "Additivity in Classical-Quantum Wiretap Channels", 2020 IEEE International Symposium on Information Theory (ISIT) (2020), pp. 1996–2001, arXiv:2002.06580 [quant-ph].

[17] Joseph M. Renes, "Privacy Amplification, Lossy Compression, and their Duality to Channel Coding", 2019 IEEE International Symposium on Information Theory (ISIT) (2019), pp. 2144–2148, arXiv:1708.05685 [quant-ph].

[16] Raban Iten, Joseph M. Renes, and David Sutter, "Pretty good measures in quantum information theory", 2017 IEEE International Symposium on Information Theory (ISIT) (2017), pp. 3195–3199, arXiv:1608.08229 [quant-ph].

[15] Rajai Nasser and Joseph M. Renes, "Polar codes for arbitrary classical-quantum channels and arbitrary cq-MACs", 2017 IEEE International Symposium on Information Theory (ISIT) (2017), pp. 281–285, arXiv:1701.03397 [quant-ph].

[14] Joseph M. Renes, "Belief propagation decoding of quantum channels by passing quantum messages", 2017 IEEE International Symposium on Information Theory (ISIT) (2017), pp. 1723–1727, arXiv:1607.04833 [quant-ph].

[13] Joseph M. Renes, "Duality of channels and codes", 2017 IEEE International Symposium on Information Theory (ISIT) (2017), pp. 299–306, arXiv:1701.05583 [quant-ph].

[12] Felipe Lacerda, Joseph M. Renes, and Volkher B. Scholz, "Coherent state constellations for Bosonic Gaussian channels", 2016 IEEE International Symposium on Information Theory (ISIT) (2016), pp. 2499–2503, arXiv:1603.05970 [quant-ph].

[11] Joseph M. Renes, David Sutter, and S. Hamed Hassaniy, "Alignment of polarized sets", 2015 IEEE International Symposium on Information Theory (ISIT) (2015), pp. 2446–2450, arXiv:1411.7925 [quant-ph].

[10] Mario Berta, Joseph M. Renes, and Mark M. Wilde, "Identifying the information gain of a quantum measurement", 2014 IEEE International Symposium on Information Theory (ISIT) (2014), pp. 331–335, arXiv:1301.1594 [quant-ph].

[9] David Sutter and Joseph M. Renes, "Universal polar codes for more capable and less noisy channels and sources", 2014 IEEE International Symposium on Information Theory (ISIT) (2014), pp. 1461–1465, arXiv:1312.5990 [cs.IT].

[8] Michael Walter and Joseph M. Renes, "A Heisenberg limit for quantum region estimation", 2014 IEEE International Symposium on Information Theory (ISIT) (2014), pp. 1126–1130, arXiv:1310.2155 [quant-ph].

[7] Joseph M. Renes, Renato Renner, and David Sutter, "Efficient One-Way Secret-Key Agreement and Private Channel Coding via Polarization", Advances in Cryptology - ASIACRYPT 2013, edited by Kazue Sako and Palash Sarkar, Lecture Notes in Computer Science 8269 (2013), pp. 194–213, arXiv:1304.3658 [cs.IT].

[6] David Sutter, Joseph M. Renes, Frederic Dupuis, and Renato Renner, "Efficient quantum channel coding scheme requiring no preshared entanglement", 2013 IEEE International Symposium on Information Theory Proceedings (ISIT) (2013), pp. 354–358, arXiv:1307.1136 [quant-ph].

[5] F. Dupuis, L. Krämer, P. Faist, J. M. Renes, and R. Renner, "Generalized Entropies", *XVIIth International Congress on Mathematical Physics* (World Scientific, 2013), pp. 134–153, arXiv:1211.3141 [quant-ph].

[4] Mark M. Wilde and Joseph M. Renes, "Polar codes for private classical communication", 2012 International Symposium on Information Theory and its Applications (ISITA) (2012), pp. 745–749, arXiv:1203.5794 [quant-ph].

[3] David Sutter, Joseph M. Renes, Frederic Dupuis, and Renato Renner, "Achieving the capacity of any DMC using only polar codes", 2012 IEEE Information Theory Workshop (ITW) (2012), pp. 114–118, arXiv:1205.3756 [cs.IT].

[2] Mark M. Wilde and Joseph M. Renes, "Quantum polar codes for arbitrary channels", 2012 IEEE International Symposium on Information Theory Proceedings (ISIT) (2012), pp. 334–338, arXiv:1201.2906 [quant-ph].

[1] Jean-Christian Boileau and Joseph M. Renes, "Optimal State Merging Without Decoupling", Fourth Workshop on Theory of Quantum Computation, Communication, and Cryptography, Vol. 5906, edited by Andrew M. Childs and Michele Mosca, Lecture Notes in Computer Science (2009), p. 76, arXiv:0905.1324 [quant-ph].

Patents

Quantum Key Distribution (using equiangular spherical codes), US Patent 7,653,199.

Invited Conference Presentations

- *Belief propagation decoding by passing quantum messages*, Quantum Measurement Theory: Foundations and Applications, Bad Honnef, Germany (online), 2022.
- *Tutorial: Quantum Information Theory*, 9th NCCR QSIT Winter School, Arosa, Switzerland, 2020.
- *Quantum communication and networks*, ICTP Advanced School on Ubiquitous Quantum Physics: The New Quantum Revolution, Trieste, Italy, 2019.
- *Operational uncertainty relations and their use*, FQXi Workshop: Quantum Incompatibility, Kloster Maria Laach, Germany, 2017.
- *Duality of channels and codes: Operational relations between coding and secrecy from quantum mechanics*, ZiF Workshop on Secure Communication via Quantum Channels, Bielefeld, Germany, 2017.
- *Tutorial: Quantum Information Theory*, 6th NCCR QSIT Winter School, Arosa, Switzerland, 2017.

- *Quantum polar codes: The uses of complementarity in decoding*, Fourth Beyond I.I.D. in Information Theory Workshop, Barcelona, Spain, 2016.
- *Dual Channels and Dual Codes- Using Heisenberg uncertainty to achieve Shannon capacity*, ICERM Workshop on Algorithmic Coding Theory, Providence, USA, 2016.
- *New Heisenberg uncertainty relations and classical uses of complementarity*, Quantum Uncertainty Days, York, England, 2015.
- *New Heisenberg uncertainty relations and classical uses of complementarity*, National Quantum Information Center Symposium on Quantum Information, Gdansk, Poland, 2015.
- *Classical uses of quantum complementarity: Leakage resilient computation and semantically-secure communication*, 8th International Conference on Information-Theoretic Security, Lugano, Switzerland, 2015.
- *What is Quantum Information?*, Second Beyond I.I.D. in Information Theory Workshop, Singapore, 2014.
- *Quantum Polar Coding*, Last Frontiers of Quantum Information Workshop, Denali, USA, 2013.
- *A Theory of Information (?)*, Beyond i.i.d. in Information Theory, University of Cambridge, 2013.
- *Efficient Quantum Polar Coding*, Japan-Singapore Workshop on Multi-user Quantum Networks, Singapore, 2012.
- *Better Quantum Gates through Renormalization*, International Conference on Quantum Systems and Technology, Ascona, Switzerland, 2012.
- *Efficient Quantum Polar Codes*, 9th Central European Quantum Information Processing Workshop (CEQIP), Smolenice, Slovakia, 2012.
- *Quantum information processing as classical processing of complementary information...and quantum polar codes, too.* Centre de Recherches Mathématiques Workshop on Quantum Information: Codes, Geometry and Random Structures, Montreal, Canada, 2011.
- *Quantum Phases for Quantum Computation*, Sydney Quantum Information Theory Workshop, Coogee, Australia, 2011.
- *Quantum Phases for Quantum Computation: Renomalization & Symmetry-Protected Topological Order*, Workshop on Collective Quantum Operations for Information Technologies, Leibniz University, Hannover, Germany, 2010.
- *Dissecting Quantum Information: Classical conditions for quantum error-correction*, Workshop on Cryptography from Storage Imperfections, Caltech, Pasadena, USA, 2010.
- *Quantum Information as Complementary Classical Information*, A2 Workshop, TU Braunschweig, Germany, 2009.
- *Private States in Quantum Key Distribution*, Workshop on the Theory and Realisation of Practical Quantum Key Distribution, Waterloo, Canada, 2007.
- *Tutorial: Quantum Communication and Cryptography*, Fifth Informal Quantum Information Gathering, Innsbruck, Austria, 2007.

Contributed Conference Presentations

- *Quantum message-passing algorithm for optimal and efficient decoding*, International Symposium on Information Theory, Helsinki, Finland, 2022.
- *On the Second-Order Asymptotics of the Partially Smoothed Conditional Min-Entropy & Application to Quantum Compression*, 1. DPG-Herbsttagung: Quantum Science and Information Technologies, Freiburg, Germany, 2019.

- *Approximate quantum non-demolition measurements*, 1. DPG-Herbsttagung: Quantum Science and Information Technologies, Freiburg, Germany, 2019.
- *Privacy amplification, lossy compression, and their duality to channel coding*, International Symposium on Information Theory, Paris, 2019.
- *On privacy amplification, lossy compression, and their duality to channel coding*, Sixth Beyond I.I.D. in Information Theory Workshop, Cambridge, England, 2018.
- *Duality of channels and codes*, 21st Annual Conference on Quantum Information Processing (QIP), Delft, Holland, 2018.
- *Belief propagation decoding of quantum channels by passing quantum messages*, International Symposium on Information Theory, Aachen, Germany, 2017.
- *Duality of channels and codes*, International Symposium on Information Theory, Aachen, Germany, 2017.
- *Belief propagation decoding of quantum channels by passing quantum messages*, 20th Annual Conference on Quantum Information Processing, Seattle, USA, 2017.
- *Operationally-Motivated Uncertainty Relations for Joint Measurability and the Error-Disturbance Tradeoff*, Spring Meeting of the German Physical Society, Berlin, Germany, 2014.
- *Thermodynamics as a (Quantum) Resource Theory*, Workshop on Thermodynamics in the Quantum Regime, Potsdam, Germany, 2014.
- *Thermodynamics as a (Quantum) Resource Theory*, 2nd Workshop on Noise Information and Complexity at Quantum Scale, Erice, Italy, 2013.
- *Efficient Quantum Polar Codes*, 15th Annual Conference on Quantum Information Processing (QIP), Montreal, Canada, 2011.
- *The Uncertainty Principle in the Presence of Quantum Memory*, March Meeting of the American Physical Society, Portland, USA, 2010.
- *Optimal State Merging Without Decoupling*, Fourth Workshop on the Theory of Quantum Computation, Communication, and Cryptography (TQC), Waterloo, Canada, 2009.
- *Measurement-Based Quantum Computation in Realistic Spin-1 Chains*, Spring Meeting of German Physical Society, Hamburg, Germany, 2009.
- *Measurement-Based Quantum Computation in Realistic Spin-1 Chains*, 11th Annual Workshop of the Southwest Quantum Information and Technology Network (SQuInT), Seattle, USA, 2009.
- *Complementarity and Privacy: From Private State Distillation to Quantum Channel Coding*, Fifth Central European Quantum Information Processing Workshop (CEQIP), Telč, Czech Republic, 2008.
- *Complementarity, Privacy, and Entanglement*, Spring Meeting of the German Physical Society, Darmstadt, Germany, 2008.
- *Private States, Privacy Amplification, and the Uncertainty Principle*, Spring Meeting of the German Physical Society, Düsseldorf, Germany, 2007.
- *Effective Channels in Quantum Key Distribution*, Spring Meeting of the German Physical Society, Frankfurt, Germany, 2006.
- *Effective Channels in Quantum Key Distribution*, Fourth Informal Quantum Information Gathering, Paris, France, 2005.
- *Two Protocols for Spherical Codes in Quantum Cryptography*, Seventh International Conference on Quantum Communication, Measurement and Computing (QCMC), Glasgow, Scotland, 2004.
- *Equiangular Spherical Codes in Quantum Cryptography*, Sixth Annual Workshop of the Southwest Quantum Information and Technology Network (SQuInT), La Jolla, USA, 2004.

- *Towards a Quantum de Finetti Theorem*, Sixth Biennial Conference of the International Quantum Structures Association (IQSA), Vienna, Austria, 2002.
- *Frame Functions for qubits*, Quantum Theory: Reconsideration of Foundations, Växjö, Sweden, 2001.

Seminars & Colloquia

- *Belief propagation decoding by passing quantum messages*, Laboratoire d'Informatique de Grenoble Seminar, Grenoble, 2021.
- *Belief propagation decoding by passing quantum messages*, QuSoft Seminar, Amsterdam (online), 2021.
- *Complementarity in quantum information processing*, IBM Zurich Research Seminar, Zürich, Switzerland, 2019.
- *Feasible Device-Independent Quantum Cryptography*, Workshop Zur Quantenzufallserzeugung, Bundesamt Für Sicherheit in Der Informationstechnologie, Bonn, Germany, 2018.
- *Feasible device-independent quantum cryptography*, AFOSR Cyber Security Program Review, Arlington, VA, 2018.
- *Duality of channels and codes: Relations between coding and secrecy from quantum mechanics*, Seminar Lehrstuhl Für Theoretische Informationstechnik, TUM, Munich, Germany, 2017.
- *From Heisenberg to Shannon: Dual channels via the uncertainty principle, and a route to capacity*, EPFL Information Processing Seminar, Lausanne, Switzerland, 2016.
- *From Classical to Quantum Information Processing via Uncertainty*, Quantum Information Seminar, Vienna, Austria, 2014.
- *Quanteninformation und Physik: Von hochpräzisen Messungen bis zu neuen (Quanten-) Zuständen der Materie. (Quantum Information and Physics: From High-Precision Measurement to New Quantum Phases of Matter)*, TU Darmstadt Inaugural Habilitation Lecture, Darmstadt, Germany, 2012.
- *Gravitational Waves and Their Detection*, TU Darmstadt Habilitation Lecture, Darmstadt, Germany, 2011.
- *The Physics of (Quantum) Information: Uncertainty, Complementarity, and Quantum Information Theory*, TU Darmstadt Physics Colloquium, Darmstadt, Germany, 2011.
- *Measurement-Based Quantum Computation in Realistic Spin-1 Chains*, Institute for Quantum Information Seminar, Caltech, Pasadena, USA, 2009.
- *Quantum Information as Complementary Classical Information*, Quantumlah Seminar, CQT, Singapore, 2009.
- *Quantum Info as Complementary Classical Info: Secret Key and Entanglement Distillation via Processing Complementary Information*, QIT Seminar, ETH Zürich, Switzerland, 2009.
- *Measurement-Based Quantum Computation in Realistic Spin-1 Chains*, Condensed Matter Seminar, Max Planck Institute for the Physics of Complex Systems, Dresden, Germany, 2009.
- *Entanglement and Secret-Key Distillation from a Complementary Information Tradeoff*, Perimeter Institute Quantum Discussions, Waterloo, Canada, 2008.
- *Quantum key distribution for the lazy and careless: Noisy preprocessing and twisted states*, CAS Seminar, University of New Mexico, Albuquerque, New Mexico, 2006.
- *Quantum key distribution for the lazy, faulty, and careless: Noisy preprocessing, twisted states, and degenerate codes*, IQC Colloquium, University of Waterloo, Waterloo, Canada, 2006.
- *Quantum Perspectives on Classical Problems: Quantum Information Theory and Quantum Key Distribution*, TU Darmstadt Theoretical Physics Colloquium, Darmstadt, Germany, 2006.

- *Encoding Quantum Information in Transverse Modes of Light*, Max Planck Research Group, Institute of Optics, Information, and Photonics, Erlangen, Germany, 2005.
- *Spherical Codes and Designs in Quantum Cryptography*, Quantum Institute Visitor Symposium "Quantum Lunch", Los Alamos, USA, 2004.
- *Spherical Codes and Designs in Quantum Key Distribution*, Seminar at the University of Erlangen, Germany, 2004.
- *Spherical Codes and Designs in Quantum Cryptography*, Seminar at the University of Potsdam, Germany, 2004.
- *Use of Spherical Codes in Quantum Cryptography*, Seminar at the University of Hannover, Germany, 2004.
- *Quantum Cryptography with Spherical Codes*, Seminar at the University of Karlsruhe, Germany, 2003.