

# Stephanie Wehner

## Curriculum Vitae

QuTech, Lorentzweg 1  
2628 CJ Delft

✉ [steph@locc.la](mailto:steph@locc.la)

Born: 8 May 1977

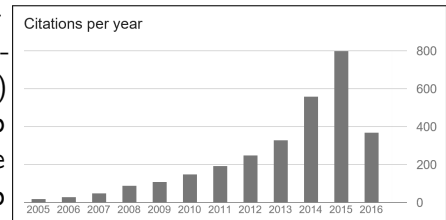
Nationality: German

Languages: German, Dutch, English



## Highlights

- Science** Over 60 publications (> 2900 citations of which > 790 in 2015, hindex 30, i10-index 54, Google Scholar May 2016) in Science (1x), Nature (1x), Nature Communications (5x), PNAS (1x), IEEE Transactions on Information Theory (7x), CRYPTO (2x), Physical Review Letters (9x, 2x Editor's suggestion) and others. Works selected for Science's "Top 10 Breakthroughs of 2015", Nature's "Science Events that shaped 2015", and voted in Top 10 of 2014 in physics news at [phys.org](http://phys.org).
- Press** Popular science coverage in New York Times (Front Page), The Economist, TIME, The Times, Huffington Post, New Scientist, Wired, Vice, and others.
- Outreach** Talks at TEDx, New Scientist Live, as well as the Dutch KNAW and others. Perspective article in Science in 2016.
- Funding** ERC Starting Grant 2015 (1.5M EUR), NWO VIDI Grant 2015 (800k EUR). Previous grants in Singapore (resigned) total  $\approx$  11.4 M EUR (personal share  $\approx$  1.4M EUR).
- Education** 9 distinct classes, of which one has received a perfect score on teaching evaluation. edX MOOC Quantum cryptography in fall 2016.
- Leadership** Co-Founder QCRYPT, now the largest annual international conference on quantum cryptography.



## Experience

### Academic appointments

- 2014-now **Associate Professor**, QuTECH, TU DELFT, Delft, Netherlands.  
Roadmap leader, QuTech Management Team
- 2013-2014 **Associate Professor**, SCHOOL OF COMPUTING, NATIONAL UNIVERSITY OF SINGAPORE (NUS), Singapore.
- 2010-2013 **Assistant Professor**, SCHOOL OF COMPUTING, NATIONAL UNIVERSITY OF SINGAPORE, Singapore.
- 2010-now **Principal Investigator**, CENTRE FOR QUANTUM TECHNOLOGIES (CQT), Singapore.

2008-2010 **Postdoctoral Scholar**, CALIFORNIA INSTITUTE OF TECHNOLOGY, Pasadena, USA.

#### Industry appointments

1999-2002 **Hacker**, ITSX BV, Amsterdam, Netherlands.

Security analysis and penetration testing. Full time and part time (0.4 fte)

1997-1999 **Network administrator**, XS4ALL INTERNET BV, Amsterdam, Netherlands.

Custom solutions (some still in use today).

#### Education

2004-2008 **PhD**, *University of Amsterdam*, Netherlands.

Science, specialization computer science. Supervised by Prof. R. de Wolf and H. Buhrman

2002-2004 **MSc (Doctorandus)**, *University of Amsterdam*, Netherlands.

Supervised by Prof. R. de Wolf

1999-2002 **BSc (Kandidaat)**, *University of Amsterdam*, Netherlands.

Exchange to University of New South Wales, Sydney, Australia in 2003

#### Awards

2016 Paul Ehrenfest award, international award for quantum foundations

2015 ERC Starting Grant

2015 NWO VIDI Grant

2014 Dean's Chair, National University of Singapore

2004 KHMW Jong Talent Afstudeerprijs (Prize given by Royal Dutch Society to best master's student graduating in NL in computer science in 2004)

2003 STUNT Grant for Exchange to UNSW, Sydney

#### Leadership

Co-Founder QCRYPT, Now largest annual conference on quantum cryptography in both theory and experiment

Steering Committee QCRYPT 2011-2016

Steering Committee QIP 2013-2019, Largest annual event in theoretical quantum computer science

Steering Committee QCMC 2014-2017, International conference on quantum computing, measurement and communication

Board FP7 QUTE Virtual Institute on Theoretical Quantum Information

---

## Service

### Service to the academic community

- Editorial Board, New Journal of Physics, 2016-
- Program Committees
  - Chair, MP1209 COST Quantum Thermodynamics, Valetta, Malta, February 2015
  - AQIS Asian Conference Quantum Information Science 2010, 2011, 2012, 2013, 2014
  - QIP Quantum Information Processing 2010, 2012
  - ICITS International Conference on Information Theoretic Security 2012, 2013
  - Hacking at Random 2009, What the Hack 2005, Hackers at Large 2001 (Computer security festivals, ca 3000 participants, mentioned on BBC News and others) (Program team)
- Initial member EU COST Action MP1209 "Thermodynamics in the quantum regime"
- Journal referee: Nature (free subscriptions in 2012-2015 in recognition of numerous referee reports), Science, Nature Communications, Communications in Mathematical Physics, Physical Review Letters, and others
- Conference referee: CRYPTO, QIP, ITCS, STOC, FOCS, and others

### Conference Organization

- QIP 2018 (main organizer)
- IMS workshop on inverse moment problems (2013, organizer topical week)
- IMS workshop on quantum thermodynamics (2013, main organizer)
- QCRYPT 2012 (main organizer)
- QIP 2011 (Rump session organizer)
- Workshop on Cryptography from Storage Imperfections, Caltech, March 2010 (main organizer)

### University service

- QuTech Academy, TU Delft, 2015- (Established new education series spanning three departments: Physics, EE and CS)
- QuTech Management Team 2015-
- NUS PhD Program Revision Team 2013
- NUS 2013-2014 Welfare officer CQT (counseling)
- NUS 2011-2014 Chair IT/Media Committee at CQT, NUS 2010-2013

---

## Funding

- EU ○ Quantum Communication Networks, 2016-2021, ERC Starting Grant, EUR 1.5M, Personal Grant.
- Large quantum networks from small quantum devices, 2015-2020, EUR 800.000, NWO VIDI, Personal Grant.

- Singapore
- Space-based QKD, 2014-2019, S\$6.3 million ( $\approx$  3.9M EUR), National Research Foundation Singapore, CRP Grant, joint with Alex Ling, Resigned due to move to Europe.
  - Quantum information as a tool, 2014-2016, S\$1.26 M ( $\approx$  743k EUR), Ministry of Education, Singapore/Centre for Quantum Technologies, Resigned due to move.
  - Random numbers from quantum processes, 2013-2018, S\$ 10M ( $\approx$  6.2 M EUR), Ministry of Education, Academic Research Fund Tier 3 Grant, 13 Investigators, personal share S\$1.03 million. Primary grant writer joint with Valerio Scarani. Lead PI Cluster “Random numbers from complex systems” (7 PIs at 2 universities in Singapore), Resigned due to move to Europe.
  - Resources for cryptography, 2011-2013, S\$1 million ( $\approx$  590k EUR), Ministry of Education, Singapore/Centre for Quantum Technologies, sole Principal Investigator.

## Teaching

### Classes

- 2016/2017 MOOC edX “Quantum Cryptography”
- 2015/2016 Fundamentals of Quantum Information, TU Delft (joint with Leo DiCarlo)  
Quantum communication and cryptography, TU Delft
- 2014/2015 Quantum computation and Computation, TU Delft
- 2013/2014 Introduction to Information Theory, NUS  
Mathematical Horizons of Quantum Physics, NUS (Project class “Information-theoretic approaches to thermodynamics”)
- 2012/2013 Introduction to Information Theory, NUS
- 2011/2012 Topics in Cryptography, NUS, Perfect score in student teaching evaluation: 5/5  
Selected (randomly) for teaching evaluation by faculty: 5/5  
Quote from anonymous student evaluation: “Q9 What are the teacher’s strengths? I didn’t want this course to end because it was so exciting. She motivated me towards this area so much, that I will keep learning this.”  
Seminar Class in Quantum Information, NUS
- 2010/2011 Computer Security, NUS  
Discovering Science, NUS
- 2005 T.A., Quantum Computing, University of Amsterdam
- 2002- Feb.2003 Student mentor, U. of Amsterdam (Counseling first years)

### Student supervision

- PhD Jed Kaniewski, 2011-2015, National University of Singapore (now Postdoc Copenhagen)
- Tanvirul Islam, 2011-2015, National University of Singapore (now Postdoc Singapore)
- Corsin Pfister, 2012-Jul 2016 (expected), National University of Singapore
- Nelly Ng, 2012-Fall 2016 (expected), National University of Singapore and TU Delft

Filip Rozpedek, 2015-, TU Delft

Jérémy Ribeiro, 2015-, TU Delft

Jonas Helsen, 2015-, TU Delft

Other Co-supervision PhD 3, Master students 7, Bachelor and undergraduate researchers 25 (Singapore follows the American system in which research students typically do not do a master's degree). Students have won 3 prizes as a result of this work in Singapore.

## Selected Research Visits and Collaborations

2016 University of Sydney

2015 University of Sydney

2014 ETH Zurich, University of Sydney, Stanford, MIT

2013 ETH Zurich, University of Sydney, UCL, MPQ

2012 Los Alamos National Labs, University of Sydney, ETH Zurich

2011 Caltech, University of Sydney, ETH Zurich, FU Berlin, Perimeter Institute

2010 Mittag Leffler Institute, Sweden (1 month), University of Sydney, Perimeter Institute, ETH Zurich

2009 Kavli Institute for Theoretical Physics, UCSB (1.5 months), ETH Zurich, Imperial College

Prior Long IBM Watson, Yorktown, USA (1 month, 2007), University of Queensland, Australia term visits (1 month, 2005), University of Cambridge (2 months, 2004)

## Publications

Each research result is listed **only once**, even if it first appeared at a conference and later as a much longer journal version under a potentially different title.

Due to the interdisciplinary nature of quantum information my publications are both in journals (more important in physics) and in conferences (more important in theoretical computer science).

Following my mathematical background author ordering of my papers (especially prior to supervising my own students) is generally alphabetical, with only two exceptions during my PhD (when I collaborated with physicists). When working with my physics students, however, I consider it appropriate to adopt the physics convention of non-alphabetical author ordering, typically making the student the first and myself as the supervisor the last author.

66. (Nearly) optimal P-values of all Bell experiments, D. Elkouss and S. Wehner, To appear in Nature Partner Journal Quantum Information (2016).
65. Relative thermalization, L. del Rio, A. Hutter, R. Renner and S. Wehner, To appear in Physical Review E (2016).
64. Assessing the performance of quantum repeaters for all phase-insensitive Gaussian bosonic channels, K. Goodenough, D. Elkouss, and S. Wehner, *New Journal of Physics*, 18 (2016).
63. Device-independent two-party cryptography secure against sequential attacks, J. Kaniewski and

- S. Wehner, *New Journal of Physics*, 18 (2016).
62. Sifting attacks in finite-size quantum key distribution, C. Pfister, N. Lütkenhaus, S. Wehner and P. J. Coles, *New Journal of Physics*, 18 (2016).
  61. Asynchronous reference frame agreement in a quantum network, T. Islam and S. Wehner, *New Journal of Physics*, 18 (2016).
  60. To see the world in a grain of spins, S. Wehner, *Science*, Perspective Article, 11 Mar 2016.
  59. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres, B. Hensen, H. Bernien, A. Dréau, A. Reiserer, N. Kalb, M. Blok, J. Ruitenberg, R. Vermeulen, R. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. Mitchell, M. Markham, D. Twitchen, D. Elkouss, S. Wehner, T. Taminiau, R. Hanson, ***Nature***, 526 (7575), 682-686 (2015). Science's "Top 10 Breakthroughs of 2015", Nature's "Science Events that shaped 2015". Cover New York Times, TIME, The Economist, Huffington Post, New Scientist, and others.
  58. Limits to catalysis in quantum thermodynamics, N. Ng, C. Cirstoiu, J. Eisert, and S. Wehner, *New Journal of Physics* 17 (8), 085004 (2015). Perspective article in NJP 17, 075004 (2015).
  57. Practical relativistic bit commitment, T. Lunghi, J. Kaniewski, F. Bussi eres, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden, *Physical Review Letters*, 115 (3), 030502 (2015).
  56. The second laws of quantum thermodynamics, F. Brand ao, M. Horodecki, N. Ng, J. Oppenheim, S. Wehner, ***Proceedings of the National Academy of Sciences***, 112 (11), 3275-3279 (2015).
  55. Entanglement-assisted guessing of complementary measurement outcomes, M. Berta, P. Coles, and S. Wehner, *Physical Review A*, 90 (6), 062127 (2014).
  54. Equivalence of wave particle duality to entropic uncertainty, P. Coles, J. Kaniewski, and S. Wehner, ***Nature Communications***, 5 (2014). Voted top 10 of physics results on phys.org in 2014. Huffington Post, Vice, and others.
  53. An experimental implementation of oblivious transfer in the noisy-storage model, C. Erven, N. Ng, N. Giggov, R. LaFlamme, S. Wehner and G. Weihs, ***Nature Communications***, 5, 3418 (2014), Also appeared as a talk at QCRYPT 2013.
  52. Spatial reference frame agreement in quantum networks, T. Islam, L. Magnin, B. Sorg and S. Wehner, *New Journal of Physics*, 16, 063040 (2014), Also appeared as a talk at QCRYPT 2013.
  51. Entropic uncertainty from effective anticommutators, J. Kaniewski, M. Tomamichel and S. Wehner, *Physical Review A*, 90, 012332 (2014), Also appeared as a talk at QCRYPT 2014.
  50. Finite blocklength converse bounds for quantum channels, W. Matthews and S. Wehner, *IEEE Transactions on Information Theory*, 60 (11), 7317-7329 (2015). Also appeared as a talk at QIP 2013.
  49. A unified view on Hardy's paradox and the CHSH inequality, L. Mancinska and S. Wehner, Invited contribution to the special issue celebrating the 50th anniversary of Bell's theorem, *Journal of Physics A: Mathematical and Theoretical*, 47 (42), 424027 (2014).

48. Bell Nonlocality, N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani and S. Wehner, *Reviews of Modern Physics*, 86, 419 (2014).
47. Experimental bit commitment based on quantum communication and special relativity, T. Lunghi, J. Kaniewski, F. Bussieres, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner and H. Zbinden, *Physical Review Letters*, 111, 180504, (2013), Editor's suggestion, Also appeared as a talk at QCRYPT 2013.
46. Achieving the limits of the noisy-storage model using entanglement sampling, F. Dupuis, O. Fawzi and S. Wehner, *Proceedings of Advances in Cryptology – CRYPTO 2013*. Long version under the title "Entanglement sampling and applications" in *IEEE Transactions on Information Theory*, 61(2), 1093-1112 (2014). Also appeared as a talk at QCRYPT 2013 and QIP 2014.
45. Entanglement cost of quantum channels, M. Berta, F. Brandao, M. Christandl and S. Wehner, *Proceedings of IEEE ISIT*, Long version in *IEEE Transactions on Information Theory*, 59(10), 6779-6795 (2013).
44. Strong parallel repetition of a monogamy of entanglement game, M. Tomamichel, S. Fehr, J. Kaniewski and S. Wehner, *Proceedings of Advances in Cryptology – EUROCRYPT 2013*. Long version in *New Journal of Physics*, 15, 103002 (2013).
43. If no information gain implies no disturbance, then any discrete theory is classical, C. Pfister and S. Wehner, *Nature Communications*, 4, 1851 (2013). Also appeared as a contributed talk at Quantum physics and logic (QPL) 2012.
42. Secure bit commitment from relativistic constraints, J. Kaniewski, M. Tomamichel, E. Haenggi and S. Wehner, *IEEE Transactions on Information Theory*, 59, 7, 4687-4699 (2013). Also appeared as a talk at QCRYPT 2012.
41. A violation of the uncertainty principle implies a violation of the second law of thermodynamics, E. Haenggi and S. Wehner, *Nature Communications* 4, 1670 (2013). Covered in popular press in *New Scientist*, Issue 2870, June 2012.
40. Dependence of a quantum mechanical system on its own initial state and the initial state of the environment it interacts with, A. Hutter and S. Wehner, *Physical Review A*, 87, 012121 (2013).
39. Experimental implementation of bit commitment in the noisy storage model, N. Ng, S. Joshi, C. Chia, C. Kurtsiefer and S. Wehner, *Nature Communications*, 3, 1326 (2012). Also appeared as a talk at QCMC 2012.
38. Quantum to classical randomness extractors, M. Berta, O. Fawzi and S. Wehner, *Proceedings of Advances in Cryptology – CRYPTO, 2012*. Long version in *IEEE Transactions of Information Theory*, 60(2): 1168-1192 (2014) Also appeared as a talk at ICITS 2012, and QCRYPT 2012.
37. A min-entropy uncertainty relation for finite size cryptography, N. Ng, M. Berta and S. Wehner, *Physical Review A*, 86, 042315 (2012).
36. Are all non-local correlations physical?, T. Islam and S. Wehner, *Physical Review A*, 86, 042109 (2012).
35. Multipartite entanglement verification resistant against dishonest parties, A. Pappa, A. Chailloux, S. Wehner, E. Diamanti and I. Kerenidis, *Physical Review Letters*, 108, 260502 (2012).

34. Almost all quantum states have low entropy rates for any coupling to the environment, A. Hutter and S. Wehner, *Physical Review Letters*, 108, 070501 (2012), Editor's suggestion.
33. Long distance two-party quantum cryptography made simple, I. Kerenidis and S. Wehner, *Quantum Information and Computation*, 12, 0448-0406 (2012).
32. Unconditional security from noisy-quantum storage, R. Koenig, S. Wehner and J. Wullschleger, *IEEE Transactions on Information Theory*, 58, 1962-1984 (2012). Also appeared as a talk at QIP 2010.
31. A time-dependent Tsirelson's bound from limits on the rate of information gain in quantum systems, A. Doherty and S. Wehner, *New Journal of Physics*, 13, 073033 (2011).
30. Does ignorance of the whole imply ignorance of the parts?, T. Vidick and S. Wehner, *Physical Review Letters*, 107, 030402 (2011).
29. Achieving the physical limits of the bounded-storage model, P. Mandayam and S. Wehner, *Physical Review A*, 83, 022329 (2011).
28. More non-locality with less entanglement, T. Vidick and S. Wehner, *Physical Review A*, 83, 052310 (2011).
27. The uncertainty principle determines the non-locality of quantum mechanics, J. Oppenheim and S. Wehner, *Science*, 330, 6007, 1072-1074 (2010). Also appeared as a talk at QIP 2011. Media coverage in New Scientist (3 articles), Wired, Cosmos, and others.
26. A transform of complementary aspects with applications to entropic uncertainty relations, P. Mandayam, N. Balachandran and S. Wehner, *Journal of Mathematical Physics*, 51, 082201 (2010).
25. Using post-measurement information in state discrimination, D. Gopal and S. Wehner, *Physical Review A*, 82, 022326 (2010).
24. Implementation of two-party cryptographic protocols in the noisy-storage model, S. Wehner, M. Curty, C. Schaffner and H. Lo, *Physical Review A*, 81, 052336 (2010).
23. Local quantum measurement and relativity imply quantum correlations, H. Barnum, S. Beigi, S. Boixo, M. Elliot and S. Wehner, *Physical Review Letters*, 104, 140401 (2010).
22. Entropy in general physical theories, A. J. Short and S. Wehner, *New Journal of Physics*, 12, 033023 (2010).
21. Entropic uncertainty relations - A survey, S. Wehner and A. Winter, *New Journal of Physics - Special Issue on Quantum Information and Many-Body Theory*, 12, 025009 (2010).
20. A strong converse for classical channel coding using entangled inputs, R. Koenig and S. Wehner, *Physical Review Letters*, 103, 070504 (2009).
19. Relaxed uncertainty relations and information processing, G. Ver Steeg and S. Wehner, *Quantum Information and Computation*, 9 (9&10), 0801-0832 (2009).



18. Distinguishability of quantum states under restricted families of measurements with an application to quantum data hiding, W. Matthews, S. Wehner and A. Winter, *Communications in Mathematical Physics*, 813, 3 (2009).
17. Lower bound on the dimension of a quantum system given measured data, S. Wehner, M. Christandl and A. C. Doherty, *Physical Review A*, 78, 062112 (2008).
16. Robust Cryptography in the Noisy-Quantum-Storage Model, C. Schaffner, B. Terhal and S. Wehner, *Quantum Information and Computation*, 9 (11&12), 0963-0996 (2009).
15. The quantum moment problem and bounds on entangled multi-prover games, A. C. Doherty, Y.C. Liang, B. Toner and S. Wehner, *Proceedings of IEEE Conference on Computational Complexity*, 2008.
14. Cryptography from noisy storage, S. Wehner, C. Schaffner and B. Terhal, *Physical Review Letters*, 100, 220502 (2008). (Chosen by the EU Integrated Project Qubit Applications as the research highlight of the month, July 2008).
13. Higher entropic uncertainty relations for anti-commuting observables, S. Wehner and A. Winter, *Journal of Mathematical Physics*, 49, 062105 (2008). Also accepted as a talk at QIP 2008.
12. Composable security in the bounded-quantum-storage model, S. Wehner and J. Wullschlegel, *Proceedings of ICALP*, 2008.
11. Possibility, Impossibility and Cheat-Sensitivity of Quantum Bit String Commitments, H. Buhrman, M. Christandl, P. Hayden, H. Lo and S. Wehner, *Physical Review A*, 78, 022316 (2008).
10. A simple family of nonadditive quantum codes, J. A. Smolin, G. Smith and S. Wehner, *Physical Review Letters*, 99, 130505 (2007).
9. Analyzing worms and network traffic using compression, S. Wehner, *Journal of Computer Security*, Vol 15, Number 3, 303-320 (2007). Covered in Heise Security (c't Magazine, 2004).
8. State Discrimination with Post-Measurement Information, M. Ballester, S. Wehner and A. Winter, *IEEE Transactions on Information Theory*, 54 (9), 4183-4198 (2008). Also accepted as a talk at QIP 2007.
7. Entropic uncertainty relations and locking: tight bounds for mutually unbiased bases, M. Ballester and S. Wehner, *Physical Review A*, 75, 022319 (2007). Also accepted as a talk at QIP 2007.
6. Security of Quantum Bit String Commitment depends on the information measure, H. Buhrman, M. Christandl, P. Hayden, H. Lo and S. Wehner, *Physical Review Letters*, 97, 250501 (2006). Also accepted as a talk at QIP 2005.
5. Tsirelson bounds for generalized CHSH inequalities, S. Wehner, *Physical Review A*, 73, 022110 (2006).
4. Entanglement in Interactive Proof Systems with Binary Answers, S. Wehner, *Proceedings of STACS 2006*. Also accepted as a talk at QIP 2006.
3. Implications of Superstrong Nonlocality for Cryptography, H. Buhrman, M. Christandl, F. Unger, S. Wehner and A. Winter, *Proceedings of the Royal Society A*, vol. 462 (2006), 1919-1932 (2006).

2. Quantum Anonymous Transmissions, M. Christandl and S. Wehner, *Proceedings of ASIACRYPT*, 2005.
1. Improved Lower Bounds for Locally Decodable Codes and Private Information Retrieval, S. Wehner and R. de Wolf, *Proceedings of ICALP*, 2005.

## Preprints

10. Entropic Uncertainty Relations and their Applications, P. J. Coles, M. Berta, M. Tomamichel, S. Wehner, Review Article commissioned by Reviews of Modern Physics, arXiv:1511.00267.
9. Entropic uncertainty and measurement reversibility, M. Berta, S. Wehner, M. M. Wilde, arXiv:1509.09123.
8. Continuous-Variable Protocols in the Noisy-Storage Model, F. Furrer, C. Schaffner, and S. Wehner, currently being implemented, arXiv:1509.09123.
7. Work and reversibility in quantum thermodynamics, S. Wehner, M. M. Wilde, M. P. Woods, arXiv:1506.08145.
6. The maximum efficiency of nano heat engines depends on more than temperature, M. P. Woods, N. Ng, and S. Wehner, arXiv:1506.02322.
5. Loophole-free Bell test using electron spins in diamond: second experiment and additional analysis, B. Hensen, N. Kalb, M.S. Blok, A. Dréau, A. Reiserer, R.F.L. Vermeulen, R.N. Schouten, M. Markham, D.J. Twitchen, K. Goodenough, D. Elkouss, S. Wehner, T.H. Taminiau, R. Hanson, arXiv:1603.05705.
4. Contextuality without nonlocality in a superconducting quantum system, M. Jerger, Y. Reshitnyk, M. Oppliger, A. Potocnik, M. Mondal, A. Wallraff, K. Goodenough, S. Wehner, K. Juliusson, N. K. Langford, and A. Fedorov, arXiv:1602.00440.
3. Understanding nature from experimental observations: a theory independent test for gravitational decoherence, C. Pfister, J. Kaniewski, M. Tomamichel, A. Mantri, R. Schmucker, N. McMahon, G. Milburn and S. Wehner, arXiv:1503.00577.
2. Entanglement improves classical control, D. Nguyen, M. McKague and S. Wehner, arXiv:1307.1569.
1. Convergence of SDP hierarchies for polynomial optimization on the hypersphere, A.C. Doherty and S. Wehner, arXiv:1210.5048 (still under review at Mathematical Programming).

## Selected Software Contributions

- PHP Scripting language for Web Servers, former Committer, creator YP/NIS module (1999) (PHP was deployed on 244 million web sites in 2012)
- IP Layer encryption ports SKIP (BSD/OS kernel) and IPSec (FreeBSD kernel) (1997) This software enabled encrypted communication of e.g. B92 Radio Station in Belgrade with the outside world.

## Invited Talks

More than 50 invited talks at workshops, conferences or university colloquia, not counting invited seminar talks (> 40).

- 2016
- Quantum Programming Languages and Logic, Glasgow, UK (June)
  - COST Conference on Quantum Thermodynamics, Erice, Italy (May)
  - Colloquium, Physics Department, Eindhoven, Netherlands (March)
  - APS March Meeting, Baltimore, USA (March)
  - FOM Veldhoven, Focus Session on the physics of quantum information, Veldhoven, Netherlands (January)
- 2015
- Colloquium, Physics Department, University of Ulm, Germany (December)
  - Colloquium, Physics Department, St. Andrews University, UK (December)
  - Workshop on Quantum Cryptography and Quantum Information Semantic Security and Indistinguishability in the Quantum World, Aarhus, Denmark (October)
  - QUICC Summer School, Imperial CDTL, Warwick, UK (September)
  - QIPC, Leeds, UK (September)
  - ICMP International Congress of Mathematical Physics, Santiago de Chile, Chile (August) (primary event in mathematical physics held only every three years)
  - Trustworthy Quantum Cryptography, Michigan, USA (July)
  - Google Sci Foo Conference, Mountain View, USA (June)
  - Quantum systems and technology, Monte Verita, Switzerland (June)
  - Randomness in quantum physics, May, ICFO, Barcelona, Spain (May)
  - APS March Meeting, San Antonio, Texas, USA (March)
  - Coogee Workshop on Quantum Information, Sydney, Australia (January)
- 2014
- QCMC Quantum Computation, Measurement and Communication, Hefei, China (November)
  - Algorithmic spectral graph theory: Semidefinite optimization, approximation and applications, Simon's Institute, Berkeley, USA (September)
  - The greatest inspiration surely is non-locality (GISIN '14), Riederalp, Switzerland (September)
  - New frontiers of quantum information theory, Ascoli Piceno, Italy (July)
  - Seefeld Workshop on Quantum Information, Seefeld, Austria (July)
  - New perspectives on thermalization  $\dot{U}$  Interdisciplinary Physics, Aspen Center for Theoretical Physics, Aspen, USA (March)
  - ICERM Semidefinite Programming and Graph Algorithms, Providence, USA (February)

- 2013
  - University Colloquium, University of Wuerzburg, Germany (December)
  - Symposium in Theoretical Physics, Freie Universitaet Berlin, Germany (October)
  - IEEE Summer Topicals on Quantum Communication and Photonics, Hawaii, USA (July)
  - Thematic Program on Quantum Foundations and Cryptography, Madrid, Spain (July)
  - QSTART Inauguration Conference for the Quantum Information Science Center, Hebrew University, Jerusalem, Israel (June)
  - Conference on the Theory of Quantum Computing, Communication and Cryptography (TQC), Guelph, Canada (May)
  - 4th SDP Days Workshop, Amsterdam, Netherlands (March)
  - Symposium on Quantum Information Theory, Vienna, Austria (March)
  
- 2012
  - CIFAR Quantum Information Processing, Ottawa, Canada (November)
  - Symposium on Quantum Foundations, Baltimore, USA (October)
  - Q+ Hangouts, online talk series (September)
  - Japan-Singapore Workshop on Multi-user Qu. Networks, Singapore (Sept)
  - Quantum Physics of Information, Shanghai, China (August)
  - Quantum information workshop, Seefeld, Austria (July), Plenary
  - University colloquium, IST Austria, Vienna (June)
  - SQUINT (Southwest Quant, Inf. and Technology), Albuquerque, USA (April)
  
- 2011
  - Conceptual Foundations for Quantum Information Processing, Waterloo, Canada (May)
  - Central European Conference on Quantum Information Processing (CEQIP), Znojmo, Czech Republic (June)
  - Scottish Universities Summer School in Physics (SSUSP67) (August)
  - Quantum information and foundations of thermodynamics, Zurich (August)
  
- 2010
  - IPAM Workshop on Convex Optimization and Algebraic Geometry, Los Angeles, USA (September)
  - DOE Roundtable on Cybersecurity, San Jose, USA (March)
  - APS March Meeting, Portland, USA (March)
  - Caltech Lunch Bunch (colloquium), Pasadena, USA (February)
  
- 2009
  - 4th TQC (Conf. on theory of computation, communication and cryptography), Waterloo, Canada (May)
  - Operator Structures in Quantum Information, Fields Institute, Toronto, Canada (July) 2008
  - Workshop on Quantum Algorithms and Complexity, Singapore (Nov)
  - CIFAR Quantum Information Processing, Kelowna, Canada (Nov)
  - Workshop on information primitives and laws of nature, Zurich (May)

- 2007
  - China Theory Week, Beijing, China (September)
  - Bellairs Cryptography Workshop, McGill University Research Center, Barbados (March)
  
- 2006
  - IPAM Securing Cyberspace, UCLA, Los Angeles, USA (September)
  - 7th European workshop on quantum information processing and communication, Royal Society, London, UK

## Recent Outreach and Press

- Popular science coverage in New York Times (Front Page), The Economist, TIME, The Times, as well as on several occasions in Huffington Post, New Scientist, Wired, Vice, and others.
- KNAW Talk “De ultieme privacy van de natuur”, Amsterdam (January 2016)
- NWA Eureka Festival, Amsterdam (November 2015)
- New Scientist Live, London (2x, February and November 2015)
- TEDxDelft “Hacking nature”, Delft (March 2015)
- Student symposium DESDA Quantum Information, Nijmegen, Netherlands (June 2015)
- I have featured in a documentary “The Mechanics” about quantum information, and was featured in the Dutch National newspaper Volkskrant on my arrival in the Netherlands in October 2014.

## References

Professor Ignacio Cirac (ignacio.cirac@mpq.mpg.de)  
Director Theory Division  
Max Planck Institute for Quantum Optics, Germany

Professor John Preskill (preskill@theory.caltech.edu)  
Richard P. Feynman Professor of Theoretical Physics  
California Institute of Technology, USA

Professor Artur Ekert (artur.ekert@qubit.org)  
Director, Centre for Quantum Technologies  
Lee Kong Chian Centennial Professor  
National University of Singapore  
and  
Professor of Physics, University of Oxford, UK

Professor Patrick Hayden (phayden@stanford.edu)  
Stanford, USA