Curriculum Vitae of Christian Schaffner

July 28, 2021

Personal Information

Christian Schaffner
Born in Chur, Switzerland
Citizen of Switzerland
Married, 2 children

Contact Information

Institute for Logic, Language and Computation (ILLC)
University of Amsterdam
P.O. Box 94242
1090 GE Amsterdam

phone: +31 20 525 6061
email: c.schaffner@uva.nl
web: https://staff.fnwi.uva.nl/c.schaffner

Research Interests

Quantum Cryptography, Cryptographic Protocols, and (Quantum) Information Theory.

Jobs

Chairman of Quantum.Amsterdam **08/2020 –**
Innovation Hub for quantum software, technology and applications

Invited Researcher at The Quantum Wave in Computing **01/2020 – 06/2020**
Simons Institute, Berkeley, California, USA

Associate Professor (Universitair Hoofddocent) in Quantum Informatica **07/2018 –**
Institute for Logic, Language and Computation (ILLC)
University of Amsterdam, The Netherlands

Member of QuSoft, Research Center for Quantum Software **12/2015 –**
Centrum Wiskunde & Informatica, Amsterdam, The Netherlands

Assistant Professor (Universitair Docent) in Theoretical CS **07/2013 – 06/2018**
Institute for Logic, Language and Computation (ILLC)
University of Amsterdam, The Netherlands

Post-Doc (VENI grant) **04/2011 – 06/2013**
Institute for Logic, Language and Computation (ILLC)
University of Amsterdam, The Netherlands

Post-Doc in Computer Science **06/2007 – 03/2011**
Centrum Wiskunde & Informatica (CWI), Amsterdam, The Netherlands
in the group of Harry Buhrman

Education

PhD in Computer Science **04/2004 – 06/2007**
BRICS International PhD School, University of Aarhus, University of Aarhus, Denmark
PhD advisors: Louis Salvail, Ivan Damgård
PhD Thesis: *Cryptography in the Bounded-Quantum-Storage Model.*

Research visit **06/2005 - 12/2005**
McGill University, Montréal, QC, Canada

Diploma Studies in Mathematics **1998 – 2003**
ETH Zürich, Switzerland
Final grade: 5.8 (of 6)
Specialisations: Stochastics, Theoretical Computer Science

Diploma Thesis advisors: Ueli M. Maurer, Renato Renner
Diploma Thesis: *Secret-Key Agreement Information-Theoretically Secure Against Active Adversaries.*

Exchange Semester **02/2001 – 07/2001**
Université Paris-Sud, Orsay (Paris XI), France

Languages

German (mother tongue)
English, Dutch (fluent written and spoken)
French, Danish (good knowledge)

Awards, Scholarships, Grants

- 4-year PhD position from an internal call of the Quantum Software Consortium (QSC), funded by a (NWO) Zwaartekracht project, 2018.
- €10,000: Blended-learning grant from FNWI, University of Amsterdam, 2018.
- €800,000: VIDI Innovational Research Incentives Scheme from the Netherlands Organisation for Scientific Research (NWO), 2015
- Interview Round of ERC Starting Grant, 2013
- €250,000: VENI Innovational Research Incentives Scheme from the Netherlands Organisation for Scientific Research (NWO), 2010
- Diploma with distinction from ETH Zürich, 2003
- Châtelain-Fond of ETH Zürich scholarship, 2001 – 2003
- Foundation Moriz and Elsa von Kuffner scholarship, 2000 – 2003

Presentations, Research Visits

I have given invited talks at numerous workshops and conferences. I have contributed more than 10 talks to conferences such as FOCS, CRYPTO, ASIACRYPT and TCC.

Since 2005, I have given more than 30 seminar talks and visited various research groups including Simons Institute at UC Berkeley, IQI Caltech, QuICS (Maryland), IQC Waterloo, ETH Zurich, McGill University Montréal, Université de Montréal, Laboratoire de Recherche en Informatique LRI (Paris), Télécom Paristech, Centre for Quantum Computing (Cambridge), ICMAT (Madrid).

Steering Committee

From 2014 to 2018, I was on the steering committee of QCRYPT, the annual conference on quantum cryptography. From Oct 2016 to Oct 2017, I have been chairing the steering committee, being responsible to co-organize the 2017 edition of QCrypt held in Cambridge, UK.

Program Committees

TCC 21, ITC 20, EUROCRYPT 19, AQIS 18, PKC 18, CRYPTO 17, TQC 16, TQC 15, EUROCRYPT 15, QCRYPT 14, SCN 14, QCRYPT 13, CRYPTO 13, ICITS 12, QIP 12, QCRYPT 11, ICITS 11, WISSec 10, Cryptography track of RSA 09.

Editorial board

Since March 2018, I am on the editorial board of the Quantum Science and Technology journal, published by IOP.

Refereeing

Referee for various conferences including STOC, FOCS, EUROCRYPT, CRYPTO, TCC, QIP, ICALP, RANDOM, ISIT, STACS, AFRICACRYPT, PQCrypto.

Nature, Nature Communications, Physical Review X, Quantum Information & Computation, Proceedings of the Royal Society A, Journal of Physics A, Foundations of Physics, Quantum Information Processing, Physica Scripta, European Physics Journal D.

SIAM Journal on Computing, ACM Journal of Computing, Theory of Computing, Journal of Cryptology, IEEE Transactions on Information Theory, Entropy, Design Codes and Cryptography, IET Information Security.

Scientific project reviewer for QuantERA 2021, NWO VIDI 2021, NWO RUBICON 2018, CHIST-ERA, Digiteo.

Member of Jury Radboud Honours Academy 2012.

Organization

- Co-organizer of QCrypt 2020 and 2021 held online (with Serge Fehr)
- Submitted bids for the organisation of QCRYPT 2014, 2017 in Amsterdam.
- Co-organizer of the Workshop on Cryptography from Storage Imperfections
  (with John Preskill and Stephanie Wehner)
  Institute for Quantum Information, Caltech, USA, March 20–22, 2010
- Organizing committee member of EUROCRYPT 2005
  Aarhus, Denmark, May 22–26, 2005

Committee/Institute Work

- since Fall 2020: chairman of Quantum.Amsterdam, the innovation hub for quantum software, technology and applications
- since Fall 2020: member of exam committee of Master of Logic
- since Fall 2020: member of opleidingscommissie (OC) of mathematics
- since Fall 2017: chairman of Talent & Outreach Committee of the Quantum Software

Consortium

- Jan 2016 to Nov 2019: chairman of opleidingscommissie (OC) of Master of Logic
- 2015 and 2016: member of the PhD Programm eValuation Committee (PVC) of the ILLC
- since 2014 to Jan 2016: member of opleidingscommissie (OC) of Master of Logic
- since 2014: co-organizer of the ILLC colloquium
- since 2013: academic mentor of numerous MoL students

Scientific Committees

Opposed in PhD defenses of:

- Thomas Van Himbeeck, Université libre de Bruxelles, 2019
- Jort Bergfeld, University of Amsterdam, 2019
- Malvin Gattinger, University of Amsterdam, 2018
- Tommaso Gagliardoni, TU Darmstadt, 2017
- Florian Speelman, University of Amsterdam, 2016
- Teresa Piovesan, University of Amsterdam, 2016
- Normand Beaudry, ETH Zürich, 2014
- David García Soriano, University of Amsterdam, 2012
- Jop Briët, University of Amsterdam, 2011
- Stephanie Wehner, University of Amsterdam, 2009

Opposed in many MSc defenses for the Master of Logic.

Public Outreach

I have given public-outreach presentations at various big and small events. Among others at 32C3 in 2015, a large hacker congress with an audience of 3000+ listeners, at the Landing Festival 2019 in Berlin, or at the open days of Science Park Amsterdam. I have been invited panelist at the BetaBreak debate about information security in October 2013. I have spoken to Dutch high school students at Leve de Wiskunde 2017. I have given radio and podcast interviews on Dutch NPR radio on the topic of quantum computation and its impact on cryptocurrencies.

Since Fall 2017, I am chairman of the Talent & Outreach committee of the Quantum Software Consortium (QSC), a 10-year NWO gravitation grant between Amsterdam, Delft and Leiden. In this role, I am structuring and coordinating the portfolio of QSC educational programs and outreach activities.

I am actively involved in the outreach activities of Quantum.Amsterdam and QuSoft. We have developped several exhibition experiments (about polarization of light, quantum random number generator, exponential growth etc.) which we regularly use for site visits by industry or university representatives, or general public.

Teaching

2014: Basiskwalificatie Onderwijs (BKO)
Since 2017, I am teaching all my courses in fully-flipped classroom style.

at University of Amsterdam

- Fall 2021, Fall 2020, Fall 2019, Fall 2018, Fall 2017: Moderne Cryptographie, for the

Bachelor Computer Science
- Fall 2020, Fall 2019, Fall 2018, Fall 2017, Fall 2016, Fall 2015, Fall 2014, Spring 2014: Information Theory, for the Master of Logic
- June 2018, June 2017: Quantum Cryptography for the Master of Logic
- Spring 2016, Spring 2015: Information & Communication, for the Bachelor of Computer Science
- Fall 2016: Basic Probability: Theory and Programming, for the Master of Logic
- Fall 2015: Basic Probability, Computing and Statistics, for the Master of Logic
- Fall 2014, Fall 2012, Fall 2011: Introduction to Modern Cryptography, for the Master of Logic

Student Supervision

PhD Students

- Jana Sotáková
  QuSoft and University of Amsterdam, from September 2019
- Jan Czajkowski
  QuSoft and University of Amsterdam
  from November 2016, submitted thesis in April 2021
- Yfke Dulek
  QuSoft and University of Amsterdam
  from June 2016, defended in January 2021

Bachelor and Master Theses

- Sebastian Zur: *The Compressed Oracle and its Applications to Quantum Query Complexity*, Master Mathematics, University of Amsterdam, 2019
- Lynn Engelberts: *Implementing Quantum-Cryptographic Protocols using SimulaQron*, Capstone bachelor thesis, Amsterdam University College. Winner of distinction, 2019
- Thijs Blom: *Dirichlet L-series and transforming generators of principal ideals in lattice-based cryptography*, Bachelor Thesis Mathematics and Computer Science, 2018
- Jelle Don: *Quantum Random Oracle Model*, Master of Logic, University of Amsterdam, 2018
- Jeroen van Wier: *Quantum Plaintext Non-Malleability*, Master of Logic, University of Amsterdam, 2018
- Merel Schalkers: *A review of the bomb testing attack copying Wiesner's private-key quantum money*, AUC capstone project (bachelor thesis), 2018
- Charlotte Rugers: *Risk Management and the Quantum Threat*, Master of Science, Cyber Security Academy, 2018
- Esteban Landerreche: *Leaning on Impossible-To-Prallelize Work for Immutability Guarantees in the Blockchain*, (joint supervision with Marc Stevens, CWI)
  Master of Logic, University of Amsterdam, 2017
- Brecht Boskaljon: *The Perfect Bib-File* BSc Artificial Intelligence, University of Amsterdam, 2017
- Tim Coopmans: *Robust Self-Testing*, (joint supervision with Jed Kaniewski, Copenhagen)
  Master of Logic, University of Amsterdam, 2017
- Yfke Dulek; *Quantum Homomorphic Encryption for Polynomial-Sized Circuits*
  Master of Logic, University of Amsterdam, 2016
- Filippos Vogiatzian; *Secure Identification in the Isolated Qubit Model*
  Master of Grid Computing University of Amsterdam, 2015
- Casper Thuis: *Visualisation of Sport-Rating Systems*,
  BSc Artificial Intelligence, University of Amsterdam, 2015

- Max Fillinger: *Reconstructing the Cryptanalytic Attack Behind the Flame Malware*, Master of Logic, University of Amsterdam, 2013
- Maria Velema: *Post-Quantum Cryptography*, Master of Logic, University of Amsterdam, 2013
- Florian Speelman: *Position-Based Quantum Cryptography and the Garden-Hose Game*, Master in Computer Science, University of Amsterdam, 2011
- Søren Fries Skovsen: *Visual Secret Sharing*, Master in Cryptology, University of Aarhus, 2005

Student Projects

- Feb 2018 - March 2018: Research Project in MSc KI: Privately Training CNNs using Two-Party SPDZ, by Ruben Seggers and Koen van der Veen.
- Oct 2016 - January 2017: Research Project in Master of Logic: A Zero-Error Source Coding Solution to the Russian Cards Problem. By Esteban Landerreche.
- July - August 2016: Bachelor project: Introduction to modern cryptography. By Sebastian Zur
- May - June 2016: Project for HvA students: Programming a Score-Keeping App for Sport Tournaments: see project page for outcomes.
- January 2016: MoL research programming project: Bibtex parser. By Mathijs Mul.
- September 2015 - Jan 2016: Honours Project in BSc Artificial Intelligence: Programming a Score-Keeping App for Sport Tournaments. By Max Wong and Alex Khawalid.
- February - July 2015: 2-jaars Bachelor Project in BSc Wiskunde: Quantum Cryptography. By Sander Bet and Sebastian Zur.
- February - June 2014: 2-jaars Bachelor Project in BSc Wiskunde: Position-Based Cryptography. By Joost Helbing & Joost Kuipers
- September 2013 - February 2014: Honours Project in BSc Artificial Intelligence: Sport Ratings. By Joost Hoppenbrouwer & Marysia Winkels
- August 2012: Research Project in MoL: Lattice-Based Cryptography and Fully Homomorphic Encryption. By Max Fillinger

Publications (available from homepage)

In computer science, publications in conference proceedings are more important than journals, due to their faster turnaround time. In cryptography, the best papers typically appear at the two international IACR conferences CRYPTO and EUROCRYPT, which usually receive more than 200 submissions and acceptance rates are lower than with most journals (around 15%). Strong theory-oriented papers on cryptography may also appear at TCC, and very good papers that are of broader interest at STOC and FOCS. QIP is the largest annual workshop in the area of quantum-information processing where all major work is submitted and peer-reviewed. About 20% of the submissions are accepted as contributed talks of which a few get upgraded to *plenary talks*. In theoretical computer science, names of authors are almost always ordered alphabetically. Number of citations and h-index can be checked on my Google Scholar profile.

Preprints

1. Christian Majenz, Christian Schaffner, Mehrdad Tahmasbi
   Limitations on Uncloneable Encryption and Simultaneous One-Way-to-Hiding
   https://arxiv.org/abs/2103.14510
2. Jelle Don, Serge Fehr, Christian Majenz, Christian Schaffner

Online-Extractability in the Quantum Random-Oracle Model
https://arxiv.org/abs/2103.03085

3. Gorjan Alagic, Zvika Brakerski, Yfke Dulek, Christian Schaffner
Impossibility of quantum virtual black-box obfuscation of classical circuits
https://arxiv.org/abs/2005.06432
presented at QCrypt 2020, and QIP 2021
4. Christian Majenz, Christian Schaffner, Jeroen van Wier
Non-malleability for quantum public-key encryption
https://arxiv.org/abs/1905.05490
presented at QCrypt 2019
5. Jan Czajkowski, Christian Majenz, Christian Schaffner, Sebastian Zur
Quantum Lazy Sampling and Game-Playing Proofs for Quantum Indifferentiability
https://arxiv.org/abs/1904.11477
presented at QCrypt 2019

Conference Articles

6. Yfke Dulek, Alex Bredariol Grilo, Stacey Jeffery, Christian Majenz, Christian Schaffner
Secure Multi-party Quantum Computation with a Dishonest Majority
In EUROCRYPT 2020, pp 729-758, 2020
7. Esteban Landerreche, Marc Stevens, Christian Schaffner
Non-interactive Cryptographic Timestamping based on Verifiable Delay Functions
In Financial Crypto 2020, pp 541-558, 2020
8. Jelle Don, Serge Fehr, Christian Majenz, Christian Schaffner
Security of the Fiat-Shamir Transformation in the Quantum Random-Oracle Model
In CRYPTO 2019, pp 356-383, 2019
presented at QCrypt 2019
9. Jan Czajkowski, Andreas Hülsing, Christian Schaffner
Quantum Indistinguishability of Random Sponges
In CRYPTO 2019, pp 296-325, 2019
10. Eike Kiltz, Vadim Lyubashevsky, Christian Schaffner
A Concrete Treatment of Fiat-Shamir Signatures in the Quantum Random-Oracle Model
In EUROCRYPT 2018, Proceedings of Advances in Cryptology, pages 552-586, 2018
11. Jan Czajkowski, Leon Groot Bruinderink, Andreas Hülsing, Christian Schaffner, and Dominique Unruh
Post-quantum security of the sponge construction
In PQCrypto 2018, Proceedings of Post-Quantum Cryptography pp 185-204, 2018
12. Gorjan Alagic, Yfke Dulek, Christian Schaffner, Florian Speelman
Quantum Fully Homomorphic Encryption With Verification
In ASIACRYPT 2017, Proceedings of Advances in Cryptology, pages 438-467, 2017
13. Gorjan Alagic, Anne Broadbent, Bill Fefferman, Tommaso Gagliardoni, Christian Schaffner, Michael St. Jules
Computational Security of Quantum Encryption
In ICITS 2016, Proceedings of Information Theoretic Security, LNCS 10015, pages 47-71, 2016.

14. Yfke Dulek, Christian Schaffner, Florian Speelman
Quantum homomorphic encryption for polynomial-sized circuits
In CRYPTO 2016, Proceedings of Advances in Cryptology, LNCS 9816, pages 3-32, 2016.
presented at QCRYPT 2016 and plenary talk at QIP 2017 (best student paper award)

15. Tommaso Gagliardoni, Andreas Hülsing, Christian Schaffner
Semantic Security and Indistinguishability in the Quantum World
In CRYPTO 2016, Proceedings of Advances in Cryptology, LNCS 9816, pages 60-89, 2016
presented at QCRYPT 2016

16. Harry Buhrman, Serge Fehr, Christian Schaffner
On the Parallel Repetition of Multi-Player Games: The No-Signaling Case
In Proceedings of 9th Conference on the Theory of Quantum Computation, Communication and Cryptography –TQC 2014, pages 24-35, 2014

17. Harry Buhrman, Serge Fehr, Christian Schaffner, Florian Speelman
The Garden-Hose Game and Application to Position-Based Quantum Cryptography
In Proceedings of the 4th conference on Innovations in Theoretical Computer Science – ITCS 2013, pages 145-158, 2013
contributed talks at QIP 2012 and at QCRYPT 2011

18. Niek J. Bouman, Serge Fehr, Carlos Gonzalez-Guillen, Christian Schaffner
An All-But-One Entropic Uncertainty Relation, and Application to Password-based Identification
In Proceedings of Theory of Quantum Compuation, Communication, and Cryptography – TQC 2012, LNCS 7582, pages 29-44, 2012
contributed talk at QCRYPT 2011

19. Dan Boneh, Özgür Dagdalen, Marc Fischlin, Anja Lehmann, Christian Schaffner, Mark Zhandry
Random Oracles in a Quantum World
In Advances in Cryptology – ASIACRYPT 2011, pages 41–69, 2011

20. Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, Christian Schaffner
Position-Based Quantum Cryptography: Impossibility and Constructions
In Advances in Cryptology – CRYPTO 2011, pages 429–446, 2011
plenary talk at QIP 2011

21. Louis Salvail, Christian Schaffner, Miroslava Sotáková
On the Power of Two-Party Quantum Cryptography
In Theory and Application of Cryptology and Information Security – ASIACRYPT 2009, pages 70-87, 2009

22. Ivan Damgård, Serge Fehr, Carolin Lunemann, Louis Salvail, Christian Schaffner
Improving the Security of Quantum Protocols via Commit-and-Open
In Advances in Cryptology – CRYPTO 2009, pages 408–427, 2009
contributed talk at QIP 2010

23. Serge Fehr, Christian Schaffner
Composing Quantum Protocols in a Classical Environment, In Theory of Cryptography – TCC 2009, pages 350–367, 2009

24. Serge Fehr, Christian Schaffner
Randomness Extraction via δ-Biased Masking in the Presence of a Quantum Attacker, In Theory of Cryptography – TCC 2008, pages 465–481, 2008

25. Ivan Damgård, Serge Fehr, Louis Salvail, Christian Schaffner
Secure Identification and QKD in the Bounded-Quantum-Storage Model, In Advances in Cryptology – CRYPTO 2007, pages 342–359, 2007
contributed talk at QIP 2008

26. Ivan Damgård, Serge Fehr, Renato Renner, Louis Salvail, Christian Schaffner
A Tight High-Order Entropic Uncertainty Relation With Applications, In Advances in Cryptology – CRYPTO 2007, pages 360–378, 2007
contributed talk at QIP 2008

27. Ivan Damgård, Serge Fehr, Louis Salvail, Christian Schaffner
Oblivious Transfer and Linear Functions
In Advances in Cryptology – CRYPTO 2006, pages 427–444, 2006

28. Claude Crépeau, George Savvides, Christian Schaffner, Jürg Wullschleger
Information-Theoretic Conditions for Two-Party Secure Function Evaluation
In Advances in Cryptology – EUROCRYPT 2006, pages 538–554, 2006

29. Ivan Damgård, Serge Fehr, Louis Salvail, Christian Schaffner
Cryptography in the Bounded-Quantum-Storage Model
In 46th Symposium on Foundations of Computer Science (FOCS), pages 449–458, 2005
invited talk at QIP 2006

Journal Articles

30. Tim Coopmans, Jędrzej Kaniewski, Christian Schaffner
Robust self-testing of two-qubit states
In Physical Review A, Volume 99, Issue 5, 052123 (2019).

31. Yfke Dulek and Christian Schaffner and Florian Speelman
Quantum homomorphic encryption for polynomial-size circuits
In Theory of Computing, volume 14, article 7, pages 1-45, 2018.

32. Fabian Furrer, Tobias Gehring, Christian Schaffner, Christoph Pacher, Roman Schnabel, Stephanie Wehner
Continuous-Variable Protocol for Oblivious Transfer in the Noisy-Storage Model
In Nature Communications, volume 9, article number: 1450, 2018.

33. Thomas Santoli and Christian Schaffner
Using Simon's Algorithm to Attack Symmetric-Key Cryptographic Primitives
In Quantum Information & Computation, volume 17, number 1&2, pages 65-78, 2017.

34. Anne Broadbent and Christian Schaffner
Quantum Cryptography Beyond Quantum Key Distribution In Designs, Codes and Cryptography, Volume 78, Issue 1, pp 351-382, January 2016.

35. Teresa Piovesan, Giannicola Scarpa, and Christian Schaffner
Multi-party zero-error classical channel coding with entanglement
In IEEE Transactions of Information Theory, vol.61, no.2, pp.1113,1123, Feb. 2015

36. Ivan Damgård, Serge Fehr, Louis Salvail, Christian Schaffner
Secure Identification and QKD in the Bounded-Quantum-Storage Model
In Theoretical Computer Science 560, 12-26, 2014 (invited in 2010).

37. Louis Salvail, Christian Schaffner and Miroslava Sotakova
Quantifying the leakage of quantum protocols for classical two-party cryptography
In Int. J. Quantum Inform. 12, 1450041, 2014

38. Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, Christian Schaffner
Position-Based Quantum Cryptography: Impossibility and Constructions
In SIAM Journal on Computing, 43 (1), pages 150–178, 2014.

39. Harry Buhrman, Peter T. S. van der Gulik, Gunnar W. Klau, Christian Schaffner, Dave Speijer, Leen Stougie
A Realistic Model Under Which the Genetic Code is Optimal
In Journal of Molecular Evolution, July 2013

40. Serge Fehr, Ran Gelles, Christian Schaffner
Security and Composability of Randomness Expansion from Bell Inequalities
In Physical Review A, Volume 87, Issue 1, 012335, 2013

41. Harry Buhrman, Matthias Christandl, Christian Schaffner
Complete Insecurity of Quantum Protocols for Classical Two-Party Computation
In Physical Review Letters (PRL), Volume 109, Issue 16, 160501, 2012

42. Marco Tomamichel, Christian Schaffner, Adam Smith, Renato Renner
Leftover Hashing Against Quantum Side Information
In IEEE Transactions on Information Theory, volume 57, issue 8, pages 5524–5535, 2011

43. Christian Schaffner
Simple Protocols for Oblivious Transfer and Secure Identification in the Noisy-Quantum-Storage Model
In Physical Review A 82, pages 032308, 2010

44. Stephanie Wehner, Marcos Curty, Christian Schaffner, Hoi-Kwong Lo
How to implement two-party protocols in the noisy-storage model
In Physical Review A 81, pages 052336, 2010

45. Christian Schaffner, Barbara Terhal, Stephanie Wehner
Robust Cryptography in the Noisy-Quantum-Storage Model
In Quantum Information & Computation (QIC), volume 11&12, pages 963–996, 2009
contributed talk at QIP 2009

46. Robert König, Renato Renner, Christian Schaffner
The Operational Meaning of Min- and Max-Entropy
In IEEE Transactions on Information Theory, volume 55, number 9, pages 4337–4347, 2009

47. Stephanie Wehner, Christian Schaffner, Barbara Terhal
Practical Cryptography from Noisy Storage
In Physical Review Letters (PRL), volume 100, 220502, 2008

48. Ivan Damgård, Serge Fehr, Louis Salvail, Christian Schaffner
Cryptography in the Bounded-Quantum-Storage Model
In SIAM Journal of Computing, volume 37, number 6, pages 1865–1890, 2008

Theses

49. Christian Schaffner
Cryptography in the Bounded-Quantum-Storage Model
PhD Thesis, BRICS, University of Aarhus, 2007

50. Christian Schaffner
Secret-Key Agreement Information-Theoretically Secure Against Active Adversaries
Diploma Thesis, ETH Zürich, 2003

References

1. Harry Buhrman, Professor, University of Amsterdam, group leader at CWI Amsterdam, director of QuSoft
Email: buhrman@cwi.nl

2. Kareljan Schoutens, Professor, University of Amsterdam, The Netherlands
Email: C.J.M.Schoutens@uva.nl

3. Serge Fehr, Professor, University of Leiden, Scientific Staff Member of the CWI Cryptology Group, CWI Amsterdam, The Netherlands
Email: fehr@cwi.nl

4. Louis Salvail, Associate Professor, Université de Montréal, QC, Canada
Email: salvail@iro.umontreal.ca