Curriculum Vitæ

Gilles Brassard FRS, O.C., O.Q.

http://www.iro.umontreal.ca/~brassard/en

December 2025

Education

- Ph.D., Theoretical computer science, Cornell University, 1979.
- M.Sc., Computer science, Université de Montréal, 1975.
- B.Sc., Computer science, Université de Montréal, 1972.

Professional Experience

- Canada Research Chair in Quantum Information Science, 2001–2021.
- Senior Fellow, Institute for Theoretical Studies, ETH Zürich, 2014, 2019 and 2024.
- Professor, Université de Montréal, since June 1988.
- Visiting Professorial Fellow, University of Wollongong, Australia, 1995.
- Directeur de recherche associé du CNRS, École Normale Supérieure, Paris, 1994.
- Invited Professor, École Polytechnique Fédérale de Lausanne, May 1988.
- Invited Researcher, Philips Research Laboratory, Brussels, Spring of 1988.
- Invited Researcher, CWI, Amsterdam, summer and fall of 1987.
- Visiting Associate Professor, University of California, Berkeley, 1984 – 1985.
- Associate Professor, Université de Montréal, 1983 – 1988.
- Assistant Professor, Université de Montréal, 1979 – 1983.

Prizes and Distinctions

- Doctor Honoris Causa: ETH Zürich (Eidgenössische Technische Hochschule), 2010; University of Ottawa, 2014; Università della Svizzera italiana, Lugano, 2015.
- Inauguration of "Laboratoire Gilles Brassard de cryptographie quantique" in Transinne, Belgium, 7 February 2025.
- Technology Award, Eduard Rhein Foundation, 2023.
- Breakthrough Prize in Fundamental Physics, 2023.
- NEC C&C Prize, 2022.
- International Member, National Academy of Sciences, United States, elected in 2021.
- Inaugural Turing Chair, QuSoft, CWI, Amsterdam, The Netherlands, December 2020.
- BBVA Foundation Frontiers of Knowledge Award in Basic Sciences, 2019.
- Micius Quantum Prize, 2019.
- Inaugural Chaire du Québec, Académie royale de Belgique, February 2019.
- Wolf Prize in Physics, 2018.
- Officer of the Ordre national du Québec, appointed in 2017.
- Lifetime Achievement Award in Computer Science, CS-Can/Info-Can, 2016.
- Officer of the Order of Canada, appointed in 2013.
- Fellow of the Royal Society of London, elected in 2013.
- Prix d'excellence, FRQNT, 2013.
- Creation of NSERC Gilles Brassard Doctoral Prize for Interdisciplinary Research, 2012.
- Thomson Reuters Citation Laureate (their "picks" for the Nobel Prize), 2012.
- Foreign Member, Academia Europaea, 2011.
- Killam Prize in Natural Sciences, Canada Council, 2011.
- Gerhard Herzberg Canada Gold Medal for Science and Engineering, NSERC, 2009.
- Distinguished Lecturer, International Association for Cryptologic Research, 2008.
- Personality of the year 2007 in information technology (OCTAS), Réseau Action TI, 2008.
- Award of Excellence, NSERC, 2006.
- Fellow, International Association for Cryptologic Research, 2006.
- Rank Prize in Opto-Electronics (United Kingdom), 2006.
- Senior Fellow, Canadian Institute for Advanced Research (CIFAR), 2002–2019.
- Prix Marie–Victorin (highest scientific recognition by Government of Québec), 2000.
- Foreign Member, Latvian Academy of Sciences, 1998.
- Killam Research Fellow, Canada Council, 1997.
- Fellow, Royal Society of Canada, Academy of Science, elected in 1996.
- Scientist of the Year, *La Presse*, 1995.
- Steacie Prize, National Research Council of Canada, 1994.
- Université de Montréal Teaching Prize, 1993.
- "Grand Débrouillard", *Les Débrouillards* (science magazine for children), May 1993.
- Prix Urgel–Archambault, ACFAS, 1992.
- E.W.R. Steacie Memorial Fellowship, NSERC, 1992.

Scientific Board Memberships

- ◇ Member of Advisory Board, QIS program, CIFAR, 2019–2025.
- ◇ Founder and Scientific Director, Institut transdisciplinaire d'information quantique (INTRIQ).
- ◇ Member of Scientific Advisory Committee, QuSoft, Amsterdam, since 2017.
- ◇ Membre du Conseil scientifique, Université Interdisciplinaire de Paris, since 2006.
- ◇ Member of Scientific Advisory Board, Centre for Applied Cryptographic Research (CACR), University of Waterloo.
- ◇ Membre du Bureau de direction, Centre de recherches mathématiques (CRM), 1998–2003.
- ◇ Membre du Conseil d'administration, Association francophone pour le savoir (ACFAS), 1998–2000.
- ◇ Director, International Association for Cryptologic Research (IACR), 1997–1999.

Editorial Duties

- ◇ Editor-in-Chief of the *Journal of Cryptology*, 1991 – 1998; editor, 1999 – 2001.
- ◇ Editorial Board Member of *Communications of the ACM* (2008 – 2017), *Natural Computing* and *Theoretical Computer Science*.
- ◇ Advisory Board Member, *Handbook of Natural Computing*, Springer–Verlag.
- ◇ Advisory Board Member of a book series on Natural Computing, Springer–Verlag.

Program Committees

- ◇ Sixth International Conference on the Theory and Practice of Natural Computing (TPNC), Prague, Czech Republic, 2017.
- ◇ Eleventh Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC), Berlin, 2016.
- ◇ Thirteenth Asian Conference on Quantum Information Science (AQIS), **Program Co-Chair**, Chennai, India, August 2013.
- ◇ Sixteenth Workshop on Quantum Information Processing (QIP), Beijing, January 2013.
- ◇ Twelft AQIS, Suzhou, China, August 2012.
- ◇ Fifth International Conference on Risks and Security of Internet and Systems (CRiSIS), Montréal, October 2010.
- ◇ Third International Workshop on Post-Quantum Cryptography, Darmstadt, May 2010.
- ◇ Fourth CRiSIS, Toulouse, October 2009.
- ◇ Second International Conference on Quantum, Nano, and Micro Technologies, Sainte-Luce, Martinique, February 2008.
- ◇ International Conference on Information Theoretic Security, Madrid, May 2007.
- ◇ IASTED International Conference on Communication, Network and Information Security, MIT, October 2006.
- ◇ Ninth QIP, Paris, January 2006.
- ◇ Eighth Workshop on Algorithms and Data Structures, Waterloo, August 2005.
- ◇ Fifth International Conference on Quantum Communication, Measurement & Computing, Capri, Italy, July 2000.
- ◇ Third QIP, **Program Co-Chair** and Co-Organizer, Montréal, December 1999.
- ◇ Second Workshop on Algorithms in Quantum Information Processing (AQIP), Chicago, January 1999.
- ◇ First NASA International Conference in Quantum Computing and Quantum Communications, Palm Springs, February 1998.
- ◇ First AQIP, Aarhus, Denmark, January 1998.
- ◇ Crypto '97, Santa Barbara, August 1997.
- ◇ In charge of a mini-symposium on cryptology at the Winter Meeting of the Canadian Mathematical Society, Montréal, December 1992.
- ◇ Seventh Annual IEEE Structure in Complexity Theory Conference, Boston, June 1992.
- ◇ Crypto '89, **Program Chair**, Santa Barbara, August 1989.
- ◇ Crypto '88, Santa Barbara, August 1988.

Other Services to the Community / Public Exposure

- ◇ Member of Weyl Prize Selection Committee, 2020.
- ◇ Co-organizer of 9th Annual *QCrypt* Conference, Montréal, 2019.
- ◇ Grand ambassadeur, *Créer l'étincelle*, Conseil du loisir scientifique de Montréal.
- ◇ Member of IACR Fellow Selection Committee, 2014-2018; Chair in 2016.
- ◇ Member of Selection Committee, Vanier Canada Graduate Scholarships Program.
- ◇ Member of Selection Committee, John Stuart Bell Prize for Research on Fundamental Issues in Quantum Mechanics and their Applications, 2009.
- ◇ Founding Director, Institut transdisciplinaire d'informatique quantique (INTRIQ).
- ◇ Theme Leader for quantum cryptography, Quantum*Works*, 2006–2011.
- ◇ Member of Synge Committee, Royal Society of Canada, 2006–2008.
- ◇ Member of panel to draft a *Roadmap* for Quantum Cryptography, Advanced Research and Development Activity (ARDA), 2004.
- ◇ Member of Canada Research Chairs College of Reviewers.
- ◇ Organizer of three Workshops on Quantum Foundations in the Light of Quantum Information, Montréal, 2000, 2002 and 2011.
- ◇ Jury member for Super Expo-Sciences Bell, Montréal, 2001.
- ◇ Jury member for Prix Urgel–Archambault (ACFAS) in 1999; Chair in 2000.
- ◇ Member of selection committee panel for the Canadian Networks of Centres of Excellence, 2000.
- ◇ Co-organizer of international Workshops in Schloß Dagstuhl, Germany (1993 and 1998) and in Monte Verita, Switzerland (1998).
- ◇ Member of NSERC selection panel for the E.W.R. Steacie Memorial Fellowship, 1997.
- ◇ Organizer of a workshop on "What are the pros and cons of cryptography?", International Conference on Privacy, Montréal, September 1997.
- ◇ Organizer of several workshops on quantum information processing in Montréal, 1992, 1993, 1997, 1999.
- ◇ Local arrangement chair, *26th Annual ACM Symposium on Theory of Computing*, Montréal, May 1994.
- ◇ Member of *ad hoc* NSERC committee for redrafting the mission statement for strategic grants on information systems, 1991.
- ◇ Treasurer, *9th Annual ACM Symposium on Principles of Distributed Computing*, Québec, August 1990.
- ◇ Member of NSERC grant selection panel for strategic grants, information systems and manufacturing systems, 1989 – 1992.
- ◇ Cryptology columnist for *Sigact News*, 1989 – 1997.
- ◇ Opponent on a thesis submitted at the University of Leiden (Netherlands) and external examiner on theses submitted at the University of Waterloo (Canada), Orsay (France, twice), Århus (Denmark), the University of Wollongong (Australia), Masaryk University (Czech Republic, twice) and the Technion (Israel).
- ◇ External consultant for a modification of the computer science program, Université du Québec à Montréal.
- ◇ Featured on television in *Découverte*, Radio-Canada, 11 December 1994; *C'est mathématique!*, Z-Channel, 2 March 2000; *Changer le monde* (Prix du Québec), Télé-Québec, 5 February 2001, *La téléportation quantique*, Canal Savoir, 8 March 2017. Interviewed on the radio for *Aujourd'hui la science*, now *Les années lumière* (four times); *Les Actualités*, January 1992; *L'heure de pointe* (Saguenay-Lac-St.-Jean), 19 November 2008; *Quirks and Quarks*, 5 June 2010; *Voyage North* (Thunder Bay), 17 February 2011; *CBC Radio Noon*, 20 September 2012; *La grande équation*, 5 October 2012; *La sphère*, 13 février 2016; *Les années lumière*, 12 May 2019; *Le 21e*, 13 April 2020; *Moteur de recherche*, 17 June 2020.
- ◇ Featured in "Entrevue du lundi", *Le Devoir*, 1st March 1993; "Sciences et techniques", *La Presse*, 6 December 1993; *L'Actualité*, 15 September 1997; *The Montreal Gazette*, 11 February 2005; *Time Magazine* (Canadian Edition), 8 August 2005; *Report on Business Magazine*, 26 August 2005; *innovationCANADA.ca* **24**, Sept.-Oct. 2006; *The Vancouver Sun*, *The Calgary Herald* and *The StarPhoenix*, 21 February 2008; *Jobboom*, January 2012; *montrealgazette.com* ("Quantum teleportation, Montrealer tipped for Nobel Prize"), 19 September 2012; *Le Devoir*, 28 September 2012; *La Presse*, 12 July 2014; *Science et Avenir*, October 2015; *Le Devoir*, 28 May 2018; *La Presse+*, 9 December 2018; *Le Soir* (Belgium), 6 February 2019; *Daily Science* (Belgium), 6 February 2019; Phys arXiv Blog of *Discover Magazine*, 28 August 2020.

Publications

Notes: (1) All hyperlinks (`http`) and cross references (such as "[176]") are clickable if viewed with Acrobat. (2) According to the general practice in Theoretical Computer Science and Theoretical Quantum Information Science, *all* my papers in career list authors in alphabetical order. (3) For papers that had been cited at least 100 times according to Clarivate's Web of Science (WoS—formerly owned by Thomson Reuters and ISI) as of 5 December 2025, the number of citations is indicated in square brackets, for a total count of 30 713 citations (of which less than 1% are self-citations) coming from 25 123 different papers; see `https://www.webofscience.com`. (4) *Only* for papers and books *not indexed* by WoS, the number of citations is indicated in parenthesis if it exceeds 100 according to Google Scholar, for a total citation count of 78 947 and an h-index of 71 see `http://scholar.google.ca/citations?hl=en&user=Rh7_srgAAAAJ&view_op=list_works&pagesize=100`.

Refereed Journals

1. G. Brassard, "Who Told You That Nature Is Nonlocal?", *Physics in Canada* **81**(2), to appear, 2025. (Also the French version "Qui vous a dit que la nature est nonlocale ?" in the same Volume of *La Physique au Canada*.)

2. S. Berthelette, G. Brassard, X. Coiteux-Roy, "On computable numbers, with an application to the Druckproblem", *Theoretical Computer Science* **1002**:114573, 29 June 2024. Open access at `http://dx.doi.org/10.1016/j.tcs.2024.114573`.

3. G. Brassard, "Profile of John Clauser, Alain Aspect and Anton Zeilinger: 2022 Nobel laureates in Physics", *Proceedings of the National Academy of Sciences* **120**(23):e2304809120, 30 May 2023. Open access at `http://dx.doi.org/10.1073/pnas.2304809120`.

4. E. Aïmeur, S. Amri and G. Brassard, "Fake news, disinformation and misinformation in social media: A review", *Social Network Analysis and Mining* **13**(1):30, February 2023. Open access at `http://dx.doi.org/10.1007/s13278-023-01028-5`. [364 citations] [364]

5. M. Boyer, G. Brassard, N. Godbout, R. Liss and S. Virally, "Simple and rigorous proof method for the security of practical quantum key distribution in the single-qubit regime using mismatched basis measurements", *Quantum Reports* **5**(1):52–77, January 2023. Open access at `http://dx.doi.org/10.3390/quantum5010005`.

6. E. Aïmeur, G. Brassard and M. Guo, "How data brokers endanger privacy", *Transactions on Data Privacy* **15**(1):41–85, April 2022. Open access at `http://www.tdp.cat/issues21/tdp.a448a21.pdf`.

7. G. Brassard, "Relativity could ensure security for cash machines" (invited *News & Views*), *Nature* **599**(7883):36–37, 4 November 2021. Available at `http://dx.doi.org/10.1038/d41586-021-02950-4`. Read-only open access at `https://rdcu.be/cA5Bz`.

8. Alexandre Bibeau-Delisle and G. Brassard, "Probability and consequences of living inside a computer simulation", *Proceedings of the Royal Society A* **477**(2247), March 2021. Open access at `http://dx.doi.org/10.1098/rspa.2020.0658`.

9. G. Brassard, A. Nayak, A. Tapp, D. Touchette and F. Unger, "Noisy interactive quantum communication", *SIAM Journal on Computing* **48**(4):1147–1195, 2019. Available at `http://dx.doi.org/10.1137/16M109867X`. Preliminary version available at `http://arXiv.org/abs/1309.2643`.

10. G. Brassard, P. Høyer, K. Kalach, M. Kaplan, S. Laplante and L. Salvail, "Key establishment à la Merkle in a quantum world", *Journal of Cryptology* **32**(3):601–634, 2019. Open access at `http://dx.doi.org/10.1007/s00145-019-09317-z`.

11. G. Brassard, "Was Edgar Allan Poe wrong after all?" (Invited Technical Perspective), *Communications of the ACM* **62**(4):132, April 2019. Available at `http://dx.doi.org/10.1145/3310976`.

12. G. Brassard, L. Devroye and C. Gravel, "Remote sampling with applications to general entanglement simulation", *Entropy* **21**(1):92, January 2019. Open access at `http://dx.doi.org/10.3390/e21010092`.

13. G. Brassard and P. Raymond-Robichaud, "Parallel Lives: A local-realistic interpretation of 'nonlocal' boxes", *Entropy* **21**(1):87, January 2019. Open access at `http://dx.doi.org/10.3390/e21010087`, but please read Authoritative version available at `http://arXiv.org/abs/arXiv:1709.10016` instead.

14. G. Brassard, L. Devroye and C. Gravel, "Exact classical simulation of the quantum-mechanical GHZ distribution", *IEEE Transactions on Information Theory* **62**(2):876–890, February 2016. Open access at `http://dx.doi.org/10.1109/TIT.2015.2504525`.

15. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", *Theoretical Computer Science* **560**(Part 1):7–11, December 2014. This is a reproduction of the historical BB84 paper [176] in honour of the 30th anniversary of its original publication. Open access at `http://dx.doi.org/10.1016/j.tcs.2014.05.025`. [3721 citations] [3721]

16. G. Brassard, Y. Elias, J. M. Fernandez, H. Gilboa, J. A. Jones, T. Mor, Y. Weinstein and L. Xiao, "Experimental heat-bath cooling of spins", *European Physical Journal Plus* **129**(12):266, December 2014. Open access at `http://dx.doi.org/10.1140/epjp/i2014-14266-0`.

17. C. H. Bennett, G. Brassard and S. Breidbart, "Quantum cryptography II: How to reuse a one-time pad safely even if $\mathsf{P} = \mathsf{NP}$", *Natural Computing* **13**(4):453–458, December 2014. Open access at `http://dx.doi.org/10.1007/s11047-014-9453-6`.

18. G. Brassard, Y. Elias, T. Mor and Y. Weinstein, "Prospects and limitations of algorithmic cooling", *European Physical Journal Plus* **129**(11):258, November 2014. Preliminary version available at `http://arXiv.org/abs/arXiv:1404.6824`.

19. G. Brassard, A. Broadbent, E. Hänggi, A. A. Méthot and S. Wolf, "Classical, quantum and nonsignalling resources in bipartite games", *Theoretical Computer Science* **486**:61–72, May 2013.

20. G. Brassard and A. A. Méthot, "Strict hierarchy among Bell theorems", *Theoretical Computer Science* **486**:4–10, May 2013.

21. E. Aïmeur, G. Brassard and S. Gambs, "Quantum speed-up for unsupervised learning", *Machine Learning* **90**(2):261–287, February 2013. Available at `http://dx.doi.org/10.1007/s10994-012-5316-5`. Read-only open access at `https://rdcu.be/cA6BF`. [178 citations] [178]

22. E. Aïmeur, G. Brassard, S. Gambs and D. Schőnfeld, "P3ERS: Privacy-Preserving PEer Review System", *Transactions on Data Privacy* **5**(3):553–578, December 2012.

23. G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater and W. Tittel, "Experimental loss-tolerant quantum coin flipping", *Nature Communications* **2**(11):561, 29 November 2011. Open access at `http://www.nature.com/ncomms/journal/v2/n11/pdf/ncomms1572.pdf`.

24. G. Brassard, "The conundrum of secure positioning" (invited *News & Views*), *Nature* **479**(7373):307–308, 17 November 2011. Available at `http://dx.doi.org/10.1038/479307a`. Read-only open access at `https://rdcu.be/cA6Bw`.

25. G. Brassard and A. A. Méthot, "Can quantum-mechanical description of physical reality be considered *correct*?", *Foundations of Physics* **40**(4):463–468, April 2010. Available at `http://dx.doi.org/10.1007/s10701-010-9411-9`. Read-only open access at `https://rdcu.be/cA6BO`.

26. G. Berlín, G. Brassard, F. Bussières and N. Godbout, "Fair loss-tolerant quantum coin flipping", *Physical Review A* **80**(6):062321, December 2009. Preliminary version available at `http://arXiv.org/abs/0904.3945`.

27. S. Bandyopadhyay, G. Brassard, S. Kimmel and W. K. Wootters, "Entanglement cost of nonlocal measurements", *Physical Review A* **80**(1):012313, July 2009. Preliminary version available at `http://arXiv.org/abs/0809.2264`.

28. E. Aïmeur, G. Brassard, J. M. Fernandez and F. S. Mani Onana, "ALAMBIC: A privacy-preserving recommender system for electronic commerce", *International Journal of Information Security* **7**(5):307–334, October 2008. [115 citations] [115]

29. E. Aïmeur, G. Brassard and F. S. Mani Onana, "Blind electronic commerce", *Journal of Computer Security* **14**(6):535–559, 2006.

30. G. Brassard, H. Buhrman, N. Linden, A. A. Méthot, A. Tapp and F. Unger, "Limit on nonlocality in any world in which communication complexity is not trivial", *Physical Review Letters* **96**(25):250401, 30 June 2006. Preliminary version available at `http://arXiv.org/abs/quant-ph/0508042`. [254 citations] [254]

31. E. Aïmeur, G. Brassard and F. S. Mani Onana, "Secure anonymous physical delivery", *IADIS International Journal on WWW/Internet* **4**(1):55–69, June 2006.

32. G. Brassard and A. A. Méthot, "Can quantum-mechanical description of physical reality be considered *in*complete?", *International Journal of Quantum Information* **4**(1):45–54, February 2006. Preliminary version available at `http://arXiv.org/abs/quant-ph/0701001`.

33. G. Brassard, A. Broadbent and A. Tapp, "Quantum pseudo-telepathy", *Foundations of Physics* **35**(11):1877–1907, November 2005. Available at `http://dx.doi.org/10.1007/s10701-005-7353-4`. Read-only open access at `https://rdcu.be/cA6BL`. [153 citations] [153]

34. G. Brassard, A. Broadbent and A. Tapp, "Recasting Mermin's multi-player game into the framework of pseudo-telepathy", *Quantum Information and Computation* **5**(7):538–550, November 2005. Preliminary version available at `http://arXiv.org/abs/quant-ph/0408052`.

35. G. Brassard, "Is information the key?" (Commentary invited to open inaugural issue), *Nature Physics* **1**(1):2–4, October 2005. Available at `http://dx.doi.org/10.1038/nphys134`. Read-only open access at `https://rdcu.be/cA6Bu`.

36. G. Brassard, A. A. Méthot and A. Tapp, "Minimum entangled state dimension required for pseudo-telepathy", *Quantum Information and Computation* **5**(4&5):275–284, July 2005. Preliminary version available at `http://arXiv.org/abs/quant-ph/0412136`.

37. E. Aïmeur, G. Brassard and S. Paquet, "Personal knowledge publishing: Fostering interdisciplinary communication", *IEEE Intelligent Systems* **20**(2):46–53, March–April 2005.

38. G. Berlín, G. Brassard, F. Bussières, N. Godbout, S. Lacroix, S. O'Reilly and D. Summers-Lépine, "Towards an implementation of quantum key distribution in optical fibre telecommunication networks", *Photons: Technical Review of the Canadian Institute for Photonic Innovations* **2**(1):21–23, 2004.

39. E. Biham, G. Brassard, D. Kenigsberg and T. Mor, "Quantum computing without entanglement", *Theoretical Computer Science* **320**(1):15–33, June 2004. Preliminary version available at `http://arXiv.org/abs/quant-ph/0306182`.

40. G. Brassard, P. Horodecki and T. Mor, "TelePOVM—A generalized quantum teleportation scheme", *IBM Journal of Research and Development* **48**(1):87–97, January 2004.

41. G. Brassard, "Quantum communication complexity", *Foundations of Physics* **33**(11):1593–1616, November 2003. Available at `http://dx.doi.org/10.1023/A:1026009100467`. Read-only open access at `https://rdcu.be/cA6BM`.

42. G. Brassard, C. Crépeau and S. Wolf, "Oblivious transfers and privacy amplification", *Journal of Cryptology* **16**(4):219–237, 2003.

43. E. Biham, M. Boyer, G. Brassard, J. van de Graaf and T. Mor, "Security of quantum key distribution against all collective attacks", *Algorithmica* **34**(4):372–388, December 2002. Preliminary version available at `http://arXiv.org/abs/quant-ph/9801022`.

44. G. Brassard and T. Mor, "Multi-particle entanglement via two-party entanglement", *Journal of Physics A* **34**(35):6807–6814, 7 September 2001.

45. G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, "Limitations on practical quantum cryptography", *Physical Review Letters* **85**(6):1330–1333, 7 August 2000. Preliminary version available at `http://arXiv.org/abs/quant-ph/9911054`. [1117 citations] [1117]

46. G. Brassard, "Ordinateurs quantiques", *TSI: Technique et Science Informatiques* **19**(1–3):99–105, January–March 2000.

47. G. Brassard, R. Cleve and A. Tapp, "Cost of exactly simulating quantum entanglement with classical communication", *Physical Review Letters* **83**(9):1874–1877, 30 August 1999. Preliminary version available at `http://arXiv.org/abs/quant-ph/9901035`. [193 citations] [193]

48. G. Brassard, I. Chuang, S. Lloyd and C. Monroe, "Quantum computing", *Proceedings of the National Academy of Sciences of the USA* **95**(19):11032–11033, 15 September 1998.

49. G. Brassard, S. Braunstein and R. Cleve, "Teleportation as a quantum computation", *Physica D* **120**(1&2):43–47, September 1998. Available at `http://dx.doi.org/10.1016/S0167-2789(98)00043-8`. Preliminary version with Brassard as single author available at `http://arXiv.org/abs/quant-ph/9605035`. [133 citations] [133]

50. M. Boyer, G. Brassard, P. Høyer and A. Tapp, "Tight bounds on quantum searching", *Fortschritte Der Physik* **46**(4&5):493–505, 1998. Preliminary version available at `http://arXiv.org/abs/quant-ph/9605034`. [811 citations] [811]

51. C. H. Bennett, E. Bernstein, G. Brassard and U. V. Vazirani, "Strengths and weaknesses of quantum computing", *SIAM Journal on Computing* **26**(5):1510–1523, October 1997. Preliminary version available at `http://arXiv.org/abs/quant-ph/9701001`. [941 citations] [941]

52. G. Brassard, "Quantum computing — Searching a quantum phone book", *Science* **275**(5300):627–628, 31 January 1997.

53. G. Brassard, C. Crépeau and M. Sántha, "Oblivious transfers and intersecting codes", *IEEE Transactions on Information Theory* **42**(6):1769–1780, November 1996.

54. C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin and W. K. Wootters, "Purification of noisy entanglement and faithful teleportation via noisy channels", *Physical Review Letters* **76**(5):722–725, 29 January 1996. Errata in *ibid* **78**(10):2031, 10 March 1997. Preliminary version available at `http://arXiv.org/abs/quant-ph/9511027`. [2671 citations for the main paper and 65 for the errata] [2736]

55. J. Boyar, G. Brassard and R. Peralta, "Subquadratic zero-knowledge", *Journal of the ACM* **42**(6):1169–1193, November 1995.

56. C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, "Generalized privacy amplification", *IEEE Transactions on Information Theory* **41**(6):1915–1923, November 1995. [1161 citations] [1161]

57. G. Brassard, "Time for another paradigm shift", *ACM Computing Surveys* **27**(1): 19–21, March 1995.

58. A. Berthiaume and G. Brassard, "Oracle quantum computing", *Journal of Modern Optics* **41**(12):2521–2535, December 1994.

59. C. H. Bennett, G. Brassard, R. Jozsa, D. Mayers, A. Peres, B. Schumacher and W. K. Wootters, "Reduction of quantum entropy by reversible extraction of classical information", *Journal of Modern Optics* **41**(12):2307–2314, December 1994.

60. C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels", *Physical Review Letters* **70**(13):1895–1899, 29 March 1993. *[12684 citations]* [*12684*]

61. C. H. Bennett, G. Brassard and N. D. Mermin, "Quantum cryptography without Bell's theorem", *Physical Review Letters* **68**(5):557–559, 3 February 1992. [2149 citations] [2149]

62. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. A. Smolin, "Experimental quantum cryptography", *Journal of Cryptology* **5**(1):3–28, 1992. [1342 citations] [1342]

63. S. Bengio, G. Brassard, Y. G. Desmedt, C. Goutier and J.–J. Quisquater, "Secure implementation of identification systems", *Journal of Cryptology* **4**(3):175–183, 1991. (154 citations according to Google Scholar—not indexed by WoS) (154)

64. G. Brassard, C. Crépeau and M. Yung, "Constant-round perfect zero-knowledge computationally convincing protocols", *Theoretical Computer Science* **84**(1):23–52, July 1991.

65. G. Brassard, D. Chaum and C. Crépeau, "Minimum disclosure proofs of knowledge", *Journal of Computer and System Sciences* **37**(2):156–189, October 1988. [591 citations] [591]

66. G. Brassard and S. Kannan, "The generation of random permutations on the fly", *Information Processing Letters* **28**(4):207–212, 29 July 1988.

67. P. Beauchemin and G. Brassard, "A generalization of Hellman's extension to Shannon's approach to cryptography", *Journal of Cryptology* **1**(2):129–131, 1988.

68. C. H. Bennett, G. Brassard and J.–M. Robert, "Privacy amplification by public discussion", *SIAM Journal on Computing* **17**(2):210–229, April 1988. [662 citations] [662]

69. G. Brassard, D. Chaum and C. Crépeau, "An introduction to minimum disclosure", *CWI Quarterly* **1**(1):3–17, March 1988.

70. P. Beauchemin, G. Brassard, C. Crépeau, C. Goutier and C. Pomerance, "The generation of random numbers that are probably prime", *Journal of Cryptology* **1**(1): 53–64, 1988.

71. G. Brassard, S. Monet and D. Zuffellato, "Algorithmes pour l'arithmétique des très grands entiers", *TSI : Technique et Science Informatiques* **5**(2):89–102, March 1986.

72. G. Brassard, "L'indécidabilité théorique en pratique", *TSI : Technique et Science Informatiques* **3**(1):63–66, January 1984.

73. G. Brassard, "Relativized cryptography", *IEEE Transactions on Information Theory* **29**(6):877–894, November 1983.

74. G. Brassard, "Indécidable... bien sûr !", *TSI : Technique et Science Informatiques* **1**(6):519–521, November 1982.

75. G. Brassard, "A time–luck tradeoff in relativized cryptography", *Journal of Computer and System Sciences* **22**(3):280–311, June 1981.

76. G. Brassard, "A note on the complexity of cryptography", *IEEE Transactions on Information Theory* **25**(2):232–233, March 1979.

Articles in Popular Science Literature

77. G. Brassard and B. Courteau, "Calcul réversible et démon de Maxwell", *Bulletin AMQ* **XLVII**(3):12–18, October 2007.

78. G. Brassard and C. Crépeau, "Nous avons inventé la téléportation en un jour !", *La Recherche* **386**:32–34, May 2005. Reprinted in *Le monde quantique* (Dossier de *La Recherche* numéro 29), 2007.

79. C. H. Bennett, G. Brassard and A. K. Ekert, "Quantum cryptography", *Scientific American* **267**(4):50–57, October 1992. Translated into Spanish as "Criptografía cuántica", *Investigación y ciencia* **195**:14–22, 1992. Reprinted with updates in *The Computer in the 21st Century*, Scientific American, Inc., pp. 164 – 171, 1995. Translated into French as "Cryptographie quantique", *L'Art du secret*, Dossier no. 36, *Pour la Science*, pp. 114 – 117, July-October 2002. [291 citations] [291]

Books

80. G. Brassard and P. Bratley, *Fundamentals of Algorithmics*, Prentice Hall, Englewood Cliffs, 524 pages, 1996. Translated into Spanish under the title *Fundamentos de Algoritmía*, Prentice Hall International, Madrid, 1997. Translated into Chinese, Tsinghua University Press, Beijing, 2003. (1352 citations according to Google Scholar—books are not indexed by WoS) (1352)

81. G. Brassard (editor), *Advances in Cryptology — Proceedings of Crypto '89*, Santa Barbara, California, August 1989, Lecture Notes in Computer Science **435**, Springer, 634 pages, 1990.

82. G. Brassard, *Modern Cryptology: A Tutorial*, Lecture Notes in Computer Science **325**, Springer, 107 pages, 1988. Translated into Italian as *Introduzione alla Criptologia Moderna*, Masson, Milano, 1990. Translated into French by C. Goutier and fully updated by the author as *Cryptologie contemporaine*, Masson, Paris, 1992. Translated into Russian, Moscow, 1999. (392 citations according to Google Scholar—books are not indexed by WoS, although in this case individual chapters are) (392)

83. G. Brassard and P. Bratley, *Algorithmique : Conception et analyse*, Masson, Paris, 344 pages, 1987. Translated into English by the authors with significant improvements as *Algorithmics: Theory and Practice*, Prentice Hall, Englewood Cliffs, 1988. Translated into Spanish as *Algorítmica: Concepción y análisis*, Masson, Barcelona, 1990. Translated into Japanese, Denki Daigaku Shuppankyoku, Tokyo, 1992. Translated into German as *Algorithmik: Theorie und Praxis*, Wolfram's Verlag, Attenkirchen, 1993. (709 citations according to Google Scholar—books are not indexed by WoS) (709)

Book Chapters

84. G. Brassard, L. Devroye and C. Gravel, "Remote sampling with applications to general entanglement simulation", in *Quantum Communication—Celebrating the Silver Jubilee of Teleportation*, R. Liss and T. Mor (editors), Multidisciplinary Digital Publishing Institute, pp. 37 – 54, 2020, (Reprinted from [12])

85. G. Brassard and P. Raymond-Robichaud, "Parallel Lives: A local-realistic interpretation of 'nonlocal' boxes", in *Quantum Nonlocality*, L. Vaidman (editor), Multidisciplinary Digital Publishing Institute, pp. 6 – 18, 2019, but please read Authoritative version available at `http://arXiv.org/abs/arXiv:1709.10016` instead. (Reprinted from [13])

86. G. Brassard and P. Raymond-Robichaud, "Can free will emerge from determinism in quantum theory?", in *Is Science Compatible with Free Will? Exploring Free Will and Consciousness in the Light of Quantum Physics and Neuroscience*, A. Suarez and P. Adams (editors), Springer, pp. 41 – 61, 2013. Preliminary version available at `http://arXiv.org/abs/1204.2128`.

87. G. Brassard, P. Høyer, M. Mosca and A. Tapp, "Quantum amplitude amplification and estimation", in *Quantum Computation and Quantum Information*, Samuel J. Lomonaco, Jr. and Howard E. Brandt (editors), *Contemporary Mathematics* **305**:53–74, AMS, 2002. Preliminary version available at `http://arXiv.org/abs/quant-ph/0005055`. (2588 citations according to Google Scholar—not indexed by WoS) (2588)

88. G. Brassard, "Ordinateurs quantiques", in *Informatiques : Enjeux, tendances & évolutions*, René Jacquart (editor), Hermes Science, Paris, pp. 99 – 105, 2000. (Reprinted from [46])

89. M. Boyer, G. Brassard, P. Høyer and A. Tapp, "Tight bounds on quantum searching", in *Quantum Computing: Where Do We Want to Go Tomorrow?*, Samuel L. Braunstein (editor), Wiley-VCH, Weinheim, pp. 187 – 199, 1999. (Reprinted from [50])

90. G. Brassard, "A quantum jump in computer science", in *Computer Science Today*, Jan van Leeuwen (editor), Lecture Notes in Computer Science, Vol. 1000 (Special Anniversary Volume), Springer, pp. 1 – 14, 1995.

Encyclopædia Articles

91. G. Brassard and C. Crépeau, "Quantum cryptography", *Encyclopedia of Cryptography and Security*, Henk van Tilborg and Sushil Jajodia (editors), Springer, pp. 495 – 500, 2005. Second edition, pp. 1005 – 1010, 2011. *Encyclopedia of Cryptography, Security and Privacy*, Sushil Jajodia, Pierangela Samarati and Moti Yung (editors), Springer Nature, page 2032, 2025.

92. G. Brassard, "Cryptology", *Encyclopaedia of Mathematics*, Vol. 2, Kluwer Academic Publishers, pp. 468 – 473, 1988.

Government Publication

93. C. H. Bennett, D. Bethune, G. Brassard, N. Donnangelo, A. Ekert, C. Elliott, J. Franson, C. Fuchs, M. Goodman, R. Hughes (Chair), P. Kwiat, A. Migdall, S.–W. Nam, J. Nordholt, J. Preskill and J. Rarity, "A quantum information science and technology roadmap, Part 2: Quantum cryptography", *Advanced Research and Development Activity (ARDA)*, Version 1.0, July 2004. Available at `http://qist.lanl.gov/qcrypt_map.shtml`.

Refereed Conference Proceedings

94. E. Aïmeur, G. Brassard and D. Sallami "Too Focused on Accuracy to Notice the Fallout: Towards Socially Responsible Fake News Detection", *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society* **8**(1), Madrid, October 2025, pp. 55 – 65. Available at `http://dx.doi.org/10.1609/aies.v8i1.36530`.

95. A. Belovs, G. Brassard, P. Høyer, M. Kaplan, S. Laplante and L. Salvail, "Provably secure key establishment against quantum adversaries", *Proceedings of 12th Conference on Theory of Quantum Computation, Communication and Cryptography (TQC)*, Paris, June 2017. Open access at `http://dx.doi.org/10.4230/LIPIcs.TQC.2017.3`.

96. Ä. Baumeler, G. Brassard, C. A. Bédard and S. Wolf, "Kolmogorov amplification from Bell correlation", *IEEE International Symposium on Information Theory (ISIT)*, Aachen, Germany, June 2017, pp. 1544 – 1558.

97. E. Aïmeur, G. Brassard and J, Rioux, "CLiKC: A privacy-mindful approach when sharing data", *Proceedings of 11th International Conference on Risks and Security of Internet and Systems (CRiSIS)*, Roscoff, France, September 2016, pp. 3 – 10.

98. G. Brassard, "Cryptography in a quantum world" (invited paper), *42nd International Conference on Current Trends in Theory and Practice of Computer Science (SOFSEM)*, Harrachov, Czech Republic, Springer, pp. 3 – 16, January 2016. Preliminary version available at `http://arXiv.org/abs/1510.04256`.

99. G. Brassard, B. Salwey and S. Wolf, "Non-locality distillation as cryptographic game", *IEEE Information Theory Workshop (ITW)*, Jerusalem, April 2015, Available at `http://dx.doi.org/10.1109/ITW.2015.7133124`.

100. G. Brassard, A. Nayak, A. Tapp, D. Touchette and F. Unger, "Noisy interactive quantum communication", *Proceedings of 55th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, Philadelphia, USA, pp. 296 – 305, October 2014. (Preliminary version of [9])

101. G. Brassard, L. Devroye and C. Gravel, "Exact classical simulation of the GHZ distribution", *Proceedings of 9th Conference on Theory of Quantum Computation, Communication and Cryptography (TQC)*, Singapore, pp. 7 – 23, May 2014. Open access at `http://dx.doi.org/10.4230/LIPIcs.TQC.2014.7`. (Preliminary version of [14])

102. E. Aïmeur, G. Brassard and P. Molins, "Reconstructing profiles from information disseminated on the Internet", *Workshop for Security and Privacy in Social Networks (SPSN)*, in conjunction with *ASE/IEEE International Conference on Social Computing (SocialCom)*, Amsterdam, pp. 875 – 883, September 2012.

103. G. Brassard and M. Kaplan, "Simulating equatorial measurements on GHZ states with finite expected communication cost", *Proceedings of 7th Conference on Theory of Quantum Computation, Communication and Cryptography (TQC)*, Tokyo, pp. 65 – 73, May 2012. Preliminary version available at `http://arXiv.org/abs/1112.3382`.

104. G. Brassard, P. Høyer, K. Kalach, M. Kaplan, S. Laplante and L. Salvail, "Merkle puzzles in a quantum world", *Advances in Cryptology — Proceedings of Crypto 2011*, Santa Barbara, USA, Springer, pp. 391 – 410, August 2011. (Preliminary version of [10])

105. G. Brassard, L. Salvail and A. Tapp, "Oblivious transfer à la Merkle", *Proceedings of Third International Conference on Quantum, Nano, and Micro Technologies (ICQNM 2009)*, Cancún, Mexico, pp. 102 – 108, February 2009. **Best Paper Award**.

106. G. Berlín, G. Brassard, F. Bussières and N. Godbout, "A fair loss-tolerant quantum coin flipping protocol", *Proceedings of 9th International Conference on Quantum Communication, Measurement and Computing (QCMC)*, Calgary, Canada, pp. 384 – 387, August 2008 (published in 2009). (Preliminary version of [26])

107. E. Aïmeur, G. Brassard, J. M. Fernandez, F. S. Mani Onana and Z. Rakowski, "Experimental demonstration of a hybrid privacy-preserving recommender system", *Proceedings of the Third International Conference on Availability, Reliability and Security (ARES 2008)*, Barcelona, pp. 161 – 170, March 2008.

108. G. Berlín, G. Brassard, F. Bussières and N. Godbout, "Loss-tolerant quantum coin flipping", *Proceedings of Second International Conference on Quantum, Nano, and Micro Technologies (ICQNM 2008)*, Sainte-Luce, Martinique, pp. 1 – 9, February 2008. **Best Paper Award**. (Preliminary version of [26])

109. G. Brassard and L. Salvail, "Quantum Merkle puzzles", *Proceedings of Second International Conference on Quantum, Nano, and Micro Technologies (ICQNM 2008)*, Sainte-Luce, Martinique, pp. 76 – 79, February 2008. (Preliminary version of [104])

110. G. Brassard, A. Broadbent, E. Hänggi, A. A. Méthot and S. Wolf, "Classical, quantum and non-signalling resources in bipartite games", *Proceedings of Second International Conference on Quantum, Nano, and Micro Technologies (ICQNM 2008)*, Sainte-Luce, Martinique, pp. 80 – 89, February 2008. (Preliminary version of [19])

111. G. Brassard and A. A. Méthot, "Strict hierarchy of Bell theorems", *Proceedings of Second International Conference on Quantum, Nano, and Micro Technologies (ICQNM 2008)*, Sainte-Luce, Martinique, pp. 98 – 103, February 2008. (Preliminary version of [20])

112. G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs and A. Tapp, "Anonymous quantum communication", *Advances in Cryptology — Proceedings of Asiacrypt '2007*, Kuching, Sarawak, Malaysia, Springer, pp. 460 – 473, December 2007. Preliminary version available at `http://arXiv.org/abs/0706.2356`.

113. E. Aïmeur, G. Brassard and S. Gambs, "Quantum clustering algorithms", *Proceedings of 24th Annual International Conference on Machine Learning (ICML)*, Corvallis, Oregon, USA, pp. 1 – 8, June 2007. (Preliminary version of [21]) (156 citations according to Google Scholar—not indexed by WoS) (156)

114. G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs and A. Tapp, "Anonymous quantum communication (extended abstract)" (invited paper), *Proceedings of 2nd International Conference on Information Theoretic Security (ICITS)*, Madrid, Spain, May 2007, pp. 181 – 182. (Preliminary version of [112])

115. G. Brassard, "And God said, Let there be Confidentiality" (invited paper), *Proceedings of IEEE Lasers & Electro-Optics Society (LEOS) Summer Topical Meeting*, Québec City, Canada, July 2006. Proceedings on CD-ROM. Available at `http://dx.doi.org/10.1109/LEOSST.2006.1693986`.

116. E. Aïmeur, G. Brassard and S. Gambs, "Machine learning in a quantum world", *Proceedings of the 19th Canadian Conference on Artificial Intelligence (Canadian AI)*, Québec City, Canada, pp. 431 – 442, June 2006. [124 citations] [124]

117. E. Aïmeur, G. Brassard, J. M. Fernandez and F. S. Mani Onana, "Privacy-preserving demographic filtering", *Proceedings of the 21st Annual ACM Symposium on Applied Computing*, Dijon, France, pp. 872 – 878, April 2006.

118. E. Aïmeur, G. Brassard and F. S. Mani Onana, "Privacy-preserving physical delivery in electronic commerce", *Proceedings of IADIS International Conference on e-Commerce*, Porto, Portugal, pp. 25 – 33, December 2005. (Preliminary version of [31]). **Best Paper Award**.

119. G. Brassard, "Brief history of quantum cryptography: A personal perspective" (invited paper), *Proceedings of IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security*, Awaji Island, Japan, pp. 19 – 23, October 2005. Preliminary version available at `http://arXiv.org/abs/quant-ph/0604072`.

120. G. Brassard and C. A. Fuchs, "Quantum foundations in the light of quantum cryptography (abstract)", *Quantum Physics of Nature – QuPoN: Theory, Experiment and Interpretation*, M. Żukowski (editor), in collaboration with *6th European QIPC workshop General Information*, Institut für Experimentalphysik, University of Vienna, page 107, May 2005. Available at `https://inis.iaea.org/search/search.aspx?orig_q=RN:38074036`.

121. E. Aïmeur, G. Brassard and F. S. Mani Onana, "Blind negotiation in electronic commerce", *Montreal Conference on eTechnologies*, Montréal, Canada, pp. 35 – 43, January 2005.

122. E. Aïmeur, G. Brassard and F. S. Mani Onana, "Blind sales in electronic commerce", *Proceedings of 6th ACM International Conference on Electronic Commerce (ICEC'04)*, Delft, the Netherlands, pp. 148 – 157, October 2004. (Preliminary version of [29])

123. E. Aïmeur, G. Brassard, S. Gambs and B. Kégl, "Privacy-preserving boosting", *Proceedings of International Workshop on Privacy and Security Issues in Data Mining*, Satellite of *8th European Conference on Principles and Practice of Knowledge Discovery in Databases (PKDD'04)*, Pisa, Italy, pp. 51 – 69, September 2004.

124. G. Brassard, A. A. Méthot and A. Tapp, "Minimum entangled state dimension required for pseudo-telepathy", *Conference on Quantum Information and Quantum Control*, Toronto, pp. 19 – 23, July 2004. (Preliminary version of [36])

125. G. Brassard, F. Bussières, N. Godbout and S. Lacroix, "Entanglement and wavelength division multiplexing for quantum cryptography networks", *Proceedings of 7th International Conference on Quantum Communication, Measurement and Computing* ⟨QCMC | 2004⟩, Glasgow, Scotland, pp. 323 – 326, July 2004.

126. G. Brassard, "Quantum communication complexity: A survey" (invited paper), *Proceedings of 34th IEEE International Symposium on Multiple-Valued Logic (ISMVL 2004)*, Toronto, Canada, page 56, May 2004.

127. G. Brassard, "Un quart de siècle de cryptographie quantique" (invited paper), *Actes du Colloque Optique Guidée et Photonique* VIII—*72ième Congrès de l'ACFAS*, Montréal, Canada, page 31, May 2004.

128. G. Brassard, F. Bussières, N. Godbout and S. Lacroix, "Cryptographie quantique à plusieurs utilisateurs par multiplexage en longueur d'onde", *Actes du Colloque Optique Guidée et Photonique* VIII—*72ième Congrès de l'ACFAS*, Montréal, Canada, pp. 43 – 46, May 2004.

129. E. Aïmeur, G. Brassard and S. Gambs, "Towards a new knowledge elicitation algorithm", *Proceedings of IJCAI Workshop on Knowledge Representation and Automated Reasoning for e-Learning Systems*, Acapulco, Mexico, pp. 1 – 7, August 2003.

130. G. Brassard, F. Bussières, N. Godbout and S. Lacroix, "Multi-user quantum key distribution using wavelength division multiplexing", *Proceedings of 6th International Conference on Applications of Photonic Technology, SPIE, Vol. 5260*, Montréal, Canada, pp. 149 – 153, May 2003.

131. G. Brassard, A. Broadbent and A. Tapp, "Multi-party pseudo-telepathy" (invited paper), *Proceedings of 8th Workshop on Algorithms and Data Structures (WADS 2003)*, Ottawa, Canada, pp. 1 – 11, July 2003. Preliminary version available at `http://arXiv.org/abs/quant-ph/0306042`.

132. E. Aïmeur, G. Brassard and S. Paquet, "Using personal knowledge publishing to facilitate sharing across communities", *(Virtual) Community Informatics Workshop*, Satellite of *12th International World Wide Web Conference*, Budapest, Hungary, May 2003. Proceedings on CD-ROM only. (Preliminary version of [37])

133. E. Aïmeur, G. Brassard, H. Dufort and S. Gambs, "CLARISSE: A machine learning tool to initialize student models", *Proceedings of Sixth International Conference on Intelligent Tutoring Systems (ITS'02)*, San Sebastián, Spain, pp. 718 – 728, June 2002.

134. E. Aïmeur, E. Blanchard, G. Brassard and S. Gambs, "QUANTI: A multidisciplinary knowledge-based system for quantum information processing", *Proceedings of International Conference on Computer Aided Learning in Engineering Education (CALIE'01)*, Tunis, Tunisia, pp. 51 – 57, November 2001.

135. E. Aïmeur, E. Blanchard, G. Brassard, B. Fusade and S. Gambs, "Designing a multidisciplinary curriculum for quantum information processing", *Proceedings of 10th International Conference on Artificial Intelligence in Education (AI-ED 2001)*, San Antonio, USA, pp. 524 – 526, May 2001.

136. G. Brassard, "Quantum communication complexity"(invited paper), *Proceedings of NATO Workshop on Decoherence and its Implications in Quantum Computing and Information Transfer*, Mykonos, Greece, IOS Press, pp. 199 – 210, June 2000 (published in 2001).

137. G. Brassard, N. Lütkenhaus, T. Mor and B. C. Sanders, "Security aspects of practical quantum cryptography", *Advances in Cryptology — Proceedings of Eurocrypt '2000*, Bruges, Belgium, Springer, pp. 289 – 299, May 2000. (Preliminary version of [45])

138. G. Brassard, T. Mor and B. C. Sanders, "Quantum cryptography via parametric down-conversion", *Proceedings of the 4th International Conference on Quantum Communication, Measurement and Computing (QCMC 1998)*, Evanston, USA, Kluwer Academic, pp. 381 – 386, August 1998 (published in 2001). Preliminary version available at `http://arXiv.org/abs/quant-ph/9906074`.

139. G. Brassard, C. Crépeau, D. Mayers and L. Salvail, "The security of quantum bit commitment schemes" (invited paper), *Proceedings of Workshop on Randomized Algorithms*, Satellite of *23rd International Symposium on Mathematical Foundations of Computer Science (MFCS'98)*, Brno, Czech Republic, pp. 13 – 15, August 1998.

140. G. Brassard, "New horizons in quantum information processing" (invited paper), *Proceedings of 25th International Conference on Automata, Languages and Programming (ICALP)*, Aalborg, Denmark, Springer, pp. 769 – 771, July 1998.

141. G. Brassard, P. Høyer and A. Tapp, "Quantum counting", *Proceedings of 25th International Conference on Automata, Languages and Programming (ICALP)*, Aalborg, Denmark, Springer, pp. 820 – 831, July 1998. Preliminary version available at `http://arXiv.org/abs/quant-ph/9805082`. [294 citations] [294]

142. G. Brassard, P. Høyer and A. Tapp, "Quantum cryptanalysis of hash and claw-free functions" (invited paper), *Proceedings of 3rd Latin American Theoretical Informatics Conference (LATIN 1998)*, Campinas, Brazil, Springer, pp. 163 – 169, April 1998. Preliminary version available under a different title at `http://arXiv.org/abs/quant-ph/9705002`. [108 citations] [108]

143. G. Brassard and T. Mor, "Multi-particle entanglement via two-particle entanglement" (invited paper), *Proceedings of NASA International Conference on Quantum Computing and Quantum Communications (QCQC98)*, Palm Springs, USA, Springer, pp. 1 – 9, February 1998 (published in 1999). (Preliminary version of [44])

144. G. Brassard, "Quantum information processing: The good, the bad and the ugly" (invited paper), *Advances in Cryptology — Proceedings of Crypto '97*, Santa Barbara, USA, Springer, pp. 337 – 341, August 1997.

145. G. Brassard and P. Høyer, "An exact quantum polynomial-time algorithm for Simon's problem", *Proceedings of Fifth Israeli Symposium on Theory of Computing and Systems (ISTCS'97)*, Ramat-Gan, Israel, IEEE Computer Society Press, pp. 12 – 23, June 1997. Preliminary version available at `http://arXiv.org/abs/quant-ph/9704027`. [179 citations] [179]

146. G. Brassard and C. Crépeau, "Oblivious transfers and privacy amplification", *Advances in Cryptology — Proceedings of Eurocrypt '97*, Konstanz, Germany, Springer, pp. 334 – 347, May 1997. (Preliminary version of [42])

147. M. Boyer, G. Brassard, P. Høyer and A. Tapp, "Tight bounds on quantum searching", *Proceedings of 4th Workshop on Physics and Computation (PhysComp '96)*, Boston, USA, pp. 36 – 43, November 1996. (Preliminary version of [50, 89])

148. G. Brassard, "Teleportation as a quantum computation", *Proceedings of 4th Workshop on Physics and Computation (PhysComp '96)*, Boston, USA, pp. 48 – 50, November 1996. (Preliminary version of [49])

149. G. Brassard, "Recent developments in quantum cryptography" (invited paper), *Proceedings of Pragocrypt '96*, Prague, Czech Republic, CTU Publishing House, pp. 183 – 192, October 1996.

150. G. Brassard, "New trends in quantum computing" (invited paper), *Proceedings of 13th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, Grenoble, France, Springer, pp. 3 – 10, February 1996. Preliminary version available at `http://arXiv.org/abs/quant-ph/9602014`.

151. G. Brassard, "Quantum information theory" (invited paper), *Proceedings of IEEE International Symposium on Information Theory*, Whistler, Canada, page 4, September 1995.

152. C. H. Bennett, G. Brassard, C. Crépeau and U. M. Maurer, "Generalized privacy amplification", *Proceedings of IEEE International Symposium on Information Theory*, Trondheim, Norway, page 350, July 1994. (Preliminary version of [56])

153. G. Brassard, C. Crépeau, R. Jozsa and D. Langlois, "A quantum bit commitment scheme provably unbreakable by both parties", *Proceedings of 34th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, Palo Alto, USA, pp. 362 – 371, November 1993.

154. G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion", *Advances in Cryptology — Proceedings of Eurocrypt '93*, Lofthus, Norway, Springer, pp. 410 – 423, May 1993. (1408 citations according to Google Scholar—not indexed by WoS) (1408)

155. A. Berthiaume and G. Brassard, "Oracle quantum computing", *Proceedings of Second Workshop on Physics and Computation (PhysComp '92)*, Dallas, USA, IEEE Press, pp. 195 – 199, October 1992. (Preliminary version of [58])

156. A. Berthiaume and G. Brassard, "The quantum challenge to structural complexity theory" (invited paper), *Proceedings of 7th Annual IEEE Structure in Complexity Theory Conference*, Boston, USA, pp. 132 – 137, June 1992.

157. J. Boyar, G. Brassard and R. Peralta, "Subquadratic zero-knowledge", *Proceedings of 32nd Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, San Juan, Puerto Rico, pp. 69 – 78, October 1991. (Preliminary version of [55])

158. C. H. Bennett, G. Brassard, C. Crépeau and M.–H. Skubiszewska, "Practical quantum oblivious transfer", *Advances in Cryptology — Proceedings of Crypto '91*, Santa Barbara, USA, Springer, pp. 351 – 366, August 1991. [110 citations] [110]

159. G. Brassard, C. Crépeau, S. Laplante and C. Léger, "Computationally convincing proofs of knowledge", *Proceedings of 8th Annual Symposium on Theoretical Aspects of Computer Science (STACS)*, Hamburg, Germany, Springer, pp. 251 – 262, February 1991.

160. G. Brassard and C. Crépeau, "Quantum bit commitment and coin tossing protocols", *Advances in Cryptology — Proceedings of Crypto '90*, Santa Barbara, USA, Springer, pp. 49 – 61, August 1990 (published in 1991).

161. G. Brassard and M. Yung, "One-way group actions", *Advances in Cryptology — Proceedings of Crypto '90*, Santa Barbara, USA, Springer, pp. 94 – 107, August 1990 (published in 1991).

162. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail and J. A. Smolin, "Experimental quantum cryptography", *Advances in Cryptology — Proceedings of Eurocrypt '90*, Aarhus, Denmark, Springer, pp. 253 – 265, May 1990. (Preliminary version of [62])

163. G. Brassard, C. Crépeau and M. Yung, "Everything in **NP** can be argued in *perfect* zero-knowledge in a *bounded* number of rounds", *Proceedings of 16th International Conference on Automata, Languages and Programming (ICALP)*, Stresa, Italy, Springer, pp. 123 – 136, July 1989. (Preliminary version of [64])

164. G. Brassard, "How to improve signature schemes", *Advances in Cryptology — Proceedings of Eurocrypt '89*, Houthalen, Belgium, Springer, pp. 16 – 22, April 1989.

165. G. Brassard and C. Crépeau, "Sorting out zero-knowledge", *Advances in Cryptology — Proceedings of Eurocrypt '89*, Houthalen, Belgium, Springer, pp. 181 – 191, April 1989.

166. G. Brassard, C. Crépeau and M. Yung, "Everything in **NP** can be argued in *perfect* zero-knowledge in a *bounded* number of rounds", *Advances in Cryptology — Proceedings of Eurocrypt '89*, Houthalen, Belgium, Springer, pp. 192 – 195, April 1989. (Preliminary version of [163])

167. G. Brassard et I. B. Damgård, "'Practical **IP**' $\subseteq$ **MA**", *Advances in Cryptology — Proceedings of Crypto '88*, Santa Barbara, USA, Springer, pp. 580 – 582, August 1988 (published in 1990).

168. P. Beauchemin and G. Brassard, "A generalization of Hellman's extension of Shannon's approach to cryptography (abstract)", *Advances in Cryptology — Proceedings of Crypto '87*, Santa Barbara, USA, Springer, page 461, August 1987. (Preliminary version of [67])

169. G. Brassard, "Cryptology in academia: A ten year retrospective" (invited paper), *Proceedings of 29th Annual IEEE Computer Conference (CompCon)*, San Francisco, USA, pp. 222 – 226, February 1987.

170. G. Brassard and C. Crépeau, "Non-transitive transfer of confidence: A *perfect* zero-knowledge interactive protocol for SAT and beyond", *Proceedings of 27th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, Toronto, Canada, pp. 188 – 195, October 1986. (191 citations according to Google Scholar—not indexed by WoS) (191)

171. G. Brassard, C. Crépeau and J.–M. Robert, "Information theoretic reductions among disclosure problems", *Proceedings of 27th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, Toronto, Canada, pp. 168 – 173, October 1986. (250 citations according to Google Scholar—not indexed by WoS) (250)

172. P. Beauchemin, G. Brassard, C. Crépeau and C. Goutier, "Two observations on probabilistic primality testing", *Advances in Cryptology — Proceedings of Crypto '86*, Santa Barbara, USA, Springer, pp. 443 – 450, August 1986. (Preliminary version of [70])

173. G. Brassard, C. Crépeau and J.–M. Robert, "All-or-nothing disclosure of secrets", *Advances in Cryptology — Proceedings of Crypto '86*, Santa Barbara, USA, Springer, pp. 234 – 238, August 1986. [165 citations] [165]

174. G. Brassard and C. Crépeau, "Zero-knowledge simulation of Boolean circuits", *Advances in Cryptology — Proceedings of Crypto '86*, Santa Barbara, USA, Springer, pp. 223 – 233, August 1986.

175. C. H. Bennett, G. Brassard and J.–M. Robert, "How to reduce your enemy's information", *Advances in Cryptology — Proceedings of Crypto '85*, Santa Barbara, USA, Springer, pp. 468 – 476, August 1985 (published in 1986). (Preliminary version of [68])

176. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing" (invited paper), *Proceedings of International Conference on Computers, Systems and Signal Processing*, Bangalore, India, pp. 175 – 179, December 1984. Facsimile available at `http://arXiv.org/abs/arXiv:2003.06557`. (*16384* citations according to Google Scholar for this original Bangalore version, known as the *BB84 paper*—note that only the 30th anniversary reprint in TCS [15] is indexed by WoS) (*16384*)

177. C. H. Bennett and G. Brassard, "An update on quantum cryptography", *Advances in Cryptology — Proceedings of Crypto '84*, Santa Barbara, USA, Springer, pp. 475 – 480, August 1984. (400 citations according to Google Scholar—not indexed by WoS) (400)

178. C. H. Bennett and G. Brassard, "Quantum cryptography and its application to provably secure key expansion, public-key distribution, and coin-tossing", *Proceedings of IEEE International Symposium on Information Theory*, St-Jovite, Canada, page 91, September 1983.

179. C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, "Quantum cryptography, or Unforgeable subway tokens", *Advances in Cryptology: Proceedings of Crypto 82*, Santa Barbara, USA, Plenum Press, pp. 267 – 275, August 1982. (359 citations according to Google Scholar—not indexed by WoS) (359)

180. G. Brassard, "On computationally secure authentication tags requiring short secret shared keys", *Advances in Cryptology: Proceedings of Crypto 82*, Santa Barbara, USA, Plenum Press, pp. 79 – 86, August 1982. (140 citations according to Google Scholar—not indexed by WoS) (140)

181. G. Brassard, "An optimally secure relativized cryptosystem", *Proceedings of Crypto 81*, Santa Barbara, USA, pp. 54 – 58, August 1981.

182. G. Brassard, "A time–luck tradeoff in cryptography", *Proceedings of 21st Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, Syracuse, USA, pp. 380 – 386, October 1980. (Preliminary version of [75])

183. G. Brassard, "Relativized cryptography", *Proceedings of 20th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, San Juan, Puerto Rico, pp. 383 – 391, October 1979. (Preliminary version of [73])

Unrefereed Papers (`arXiv` papers are included below *only* if unpublished)

184. G. Brassard, "≪ D'Einstein à Wheeler ≫ : Grande Conférence d'Alain Aspect", *Bulletin du Centre de recherches mathématiques* **19**(1):7–8, spring 2013.

185. G. Brassard, F. Dupuis, S. Gambs and A. Tapp, "An optimal quantum algorithm to approximate the mean and its application for approximating the median of a set of points over an arbitrary distance", `http://arXiv.org/abs/1106.4267`, June 2011.

186. G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater and W. Tittel, "Flipping quantum coins", `http://arXiv.org/abs/0904.3946`, April 2009. (Preliminary version of [23] containing additional material)

187. S. Beauregard, G. Brassard and J. M. Fernandez, "Quantum arithmetic on Galois fields", `http://arXiv.org/abs/quant-ph/0301163`, January 2003.

188. G. Brassard, C. Crépeau, D. Mayers and L. Salvail, "Defeating classical bit commitments with a quantum computer", `http://arXiv.org/abs/quant-ph/9806031`, June 1998.

189. G. Brassard, C. Crépeau, D. Mayers and L. Salvail, "A brief review on the impossibility of quantum bit commitment", `http://arXiv.org/abs/quant-ph/9712023`, December 1997.

190. G. Brassard, P. Høyer and A. Tapp, "Cryptology column — Quantum cryptanalysis of hash and claw-free functions", *Sigact News* **28**(2):14–19, 1997. (Preliminary version of [142])

191. G. Brassard, P. Høyer and A. Tapp, "Quantum algorithm for the collision problem", `http://arXiv.org/abs/quant-ph/9705002`, May 1997. (Preliminary version of [190, 142]) (226 citations according to Google Scholar—not indexed by WoS) (226)

192. G. Brassard and P. Høyer, "On the power of exact quantum polynomial time", `http://arXiv.org/abs/quant-ph/9612017`, December 1996. (Preliminary version of [145])

193. G. Brassard and C. Crépeau, "Cryptology column — 25 years of quantum cryptography", *Sigact News* **27**(3):13–24, 1996.

194. G. Brassard, "Cryptology column — The book I've always wanted to write (almost)", *Sigact News* **26**(2):18–20, 1995.

195. G. Brassard, "The impending demise of RSA?", *RSA Laboratories CryptoBytes* **1**(1): 1–4, 1995.

196. G. Brassard, "Cryptology column — Quantum computing: The end of classical cryptography?", *Sigact News* **25**(4):15–21, 1994.

197. G. Brassard, "Cryptology column — Quantum cryptography: A bibliography", *Sigact News* **24**(3):16–20, 1993.

198. G. Brassard, "Cryptology column — New and coming books", *Sigact News* **23**(4): 8–11, 1992.

199. G. Brassard, "Cryptology column — From Moskva with love", *Sigact News* **22**(2): 8–13, 1991.

200. G. Brassard, "Cryptology column — How convincing is your protocol?", *Sigact News* **22**(1):5–12, 1991.

201. G. Brassard, "Cryptology column — Hiding information from oracles", *Sigact News* **21**(2):5–11, 1990.

202. G. Brassard, "Cryptology column — Hot news on interactive protocols", *Sigact News* **21**(1):7–11, 1990.

203. G. Brassard and K. McCurley, "Crypto 89 conference report", *IACR Newsletter* **7**(1): 9–11, 1990.

204. G. Brassard, "Cryptology column 2", *Sigact News* **20**(4):13, 1989.

205. C. H. Bennett and G. Brassard, "The dawn of a new era for quantum cryptography: The experimental prototype is working", *Sigact News* **20**(4):78–82, 1989. (277 citations according to Google Scholar—not indexed by WoS) (277)

206. G. Brassard, "Cryptology column 1", *Sigact News* **20**(3):15–19, 1989.

207. C. H. Bennett and G. Brassard, "Quantum public key distribution reinvented", *Sigact News* **18**(4):51–53, 1987.

208. C. H. Bennett and G. Brassard, "Quantum public key distribution system", *IBM Technical Disclosure Bulletin* **28**(7):3153–3163, December 1985. (174 citations according to Google Scholar—not indexed by WoS) (174)

209. G. Brassard, "Crusade for a better notation", *Sigact News* **17**(1):60–64, 1985.

210. C. H. Bennett, G. Brassard, S. Breidbart and S. Wiesner, "Eavesdrop-detecting quantum communications channel", *IBM Technical Disclosure Bulletin* **26**(8):4363–4366, January 1984.

211. G. Brassard, "An optimally secure relativized cryptosystem", *Sigact News* **15**(1): 28–33, 1983. (Reprinted from [181])

212. G. Brassard, S. Fortune and J. E. Hopcroft, "A note on cryptography and $\mathrm{NP} \cap \mathrm{CoNP} - \mathrm{P}$", Technical Report TR78-338, Department of Computer Science, Cornell University, 1978.