Bibliography

[AK15a] Emily Adlam and Adrian Kent. Deterministic relativistic quantum bit commitment. *International Journal of Quantum Information*, 13(05):1550029, aug 2015.

[AK15b] Emily Adlam and Adrian Kent. Device-independent relativistic quantum bit commitment. *Physical Review A*, 92:022315, Aug 2015.

[AK16] Emily Adlam and Adrian Kent. Quantum paradox of choice: More freedom makes summoning a quantum state harder. *Physical Review A*, 93:062327, Jun 2016.

[BB84] Charles Bennet and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *IEEE International Conference on Computers, Systems and Signal Processing*, volume 1, pages 175–179, 1984.

[BC96] Gilles Brassard and Claude Crépeau. 25 years of quantum cryptography. *SIGACT News*, 27(3):13–24, 1996.

[BC16] Rémi Bricout and André Chailloux. Recursive cheating strategies for the relativistic $\mathbb{F}_Q$ bit commitment protocol. *ArXiv e-prints*, arXiv:1608.03820 [quant-ph], 2016. `https://arxiv.org/abs/1608.03820`.

[BCC88] Gilles Brassard, David Chaum, and Claude Crépeau. Minimum disclosure proofs of knowledge. *Journal of Computer and System Sciences*, 37(2):156–189, October 1988.

[BCF+11] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-Based Quantum Cryptography: Impossibility and Constructions. In Phillip Rogaway, editor, *Advances in Cryptology - CRYPTO 2011*, pages 429–446, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[Bel64] John Stewart Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[BGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-Prover Interactive Proofs: How to Remove Intractability Assumptions. In Janos Simon, editor, *STOC 1988*, pages 113–131. ACM, 1988.

[Blu82] Manuel Blum. Coin flipping by telephone. In Allen Gersho, editor, *Advances in Cryptology: A Report on CRYPTO 81*, pages 11–15. U. C. Santa Barbara, Dept. of Elec. and Computer Eng., 1982.

[BS15] Mohammad Bavarian and Peter W. Shor. Information Causality, Szemerédi-Trotter and Algebraic Variants of CHSH. In Tim Roughgarden, editor, *ITCS 2015*, pages 123–132. ACM, 2015.

[CCM98] Christian Cachin, Claude Crépeau, and Julien Marcil. Oblivious transfer with a memory-bounded receiver. In *FOCS 1998* [DBL98], pages 493–502.

[CHSH69] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters*, 23:880–884, 1969.

[CK88] Claude Crépeau and Joe Kilian. Achieving oblivious transfer using weakened security assumptions (extended abstract). In *FOCS 1988*, pages 42–52. IEEE Computer Society, 1988.

[CK06] Roger Colbeck and Adrian Kent. Variable-bias coin tossing. *Physical Review A*, 73:032320, Mar 2006.

[CK12] Sarah Croke and Adrian Kent. Security details for bit commitment by transmitting measurement outcomes. *Physical Review A*, 86:052309, Nov 2012.

[CKW00] Valerie Coffman, Joydip Kundu, and William K. Wootters. Distributed entanglement. *Physical Review A*, 61:052306, Apr 2000.

[CM97] Christian Cachin and Ueli M. Maurer. Unconditional security against memory-bounded adversaries. In Burton S. Kaliski Jr., editor, *Advances in Cryptology - CRYPTO '97*, volume 1294 of *Lecture Notes in Computer Science*, pages 292–306. Springer, 1997.

[Col06] Roger Colbeck. *Quantum And Relativistic Protocols For Secure Multi-Party Computation*. PhD thesis, University of Cambridge, 2006.

[Col07] Roger Colbeck. Impossibility of secure two-party classical computation. *Physical Review A*, 76:062308, Dec 2007.

[CSST11] Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two Provers in Isolation. In Dong Hoon Lee and Xiaoyun Wang, editors, *Advances in Cryptology - ASIACRYPT 2011*, volume 7073 of *Lecture Notes in Computer Science*, pages 407–430. Springer, 2011.

[DBL98] *FOCS 1998*. IEEE Computer Society, 1998.

[DFSS05] Ivan Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded quantum-storage model. In *FOCS 2005*, pages 449–458. IEEE Computer Society, 2005.

[Dir39] Paul A. M. Dirac. A new notation for quantum mechanics. *Mathematical Proceedings of the Cambridge Philosophical Society*, 35(3):416–418, 1939.

[EGL83] Shimon Even, Oded Goldreich, and Abraham Lempel. A randomized protocol for signing contracts. In David Chaum, Ronald L. Rivest, and Alan T. Sherman, editors, *Advances in Cryptology: Proceedings of CRYPTO '82*, pages 205–210. Plenum Press, New York, 1983.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47:777–780, May 1935.

[FF15] Serge Fehr and Max Fillinger. Multi-Prover Commitments Against Non-Signaling Attacks. In Rosario Genaro and Matthew Robshaw, editors, *Advances in Cryptology - CRYPTO 2015, part II*, volume 9216 of *Lecture Notes in Computer Science*, pages 403–421. Springer, 2015.

[FF16] Serge Fehr and Max Fillinger. On the Composition of Two-Prover Commitments, and Applications to Multi-round Relativistic Commitments. In Marc Fischlin and Jean-Sébastien Coron, editors, *Advances in Cryptology - EUROCRYPT 2016, part II*, volume 9665 of *Lecture Notes in Computer Science*, pages 477–496. Springer, 2016.

[FL92] Uriel Feige and László Lovász. Two-prover one-round proof systems: Their power and their problems (extended abstract). In S. Rao Kosaraju, Mike Fellows, Avi Wigderson, and John A. Ellis, editors, *Proceedings of the 24th Annual ACM Symposium on Theory of Computing*, pages 733–744. ACM, 1992.

[For98] Lance Fortnow. *Complexity-Theoretic Aspects of Interactive Proof Systems*. PhD thesis, Massachusetts Institute of Technology, 1998.

[Hol09] Thomas Holenstein. Parallel Repetition: Simplification and the No-Signaling Case. *Theory of Computing*, 5(8):141–172, 2009.

[IL89] Russell Impagliazzo and Michael Luby. One-way functions are essential for complexity based cryptography (extended abstract). In *FOCS 1989*, pages 230–235. IEEE Computer Society, 1989.

[Kan15] Jędrzej Kaniewski. *Relativistic quantum cryptography*. PhD thesis, University of Cambridge, 2015.

[Ken99] Adrian Kent. Unconditionally Secure Bit Commitment. *Physical Review Letters*, 83(7):1447–1450, 1999.

[Ken05] Adrian Kent. Secure Classical Bit Commitment Using Fixed Capacity Communication Channels. *Journal of Cryptology*, 18(4):313–335, 2005.

[Ken11] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011.

[Ken12] Adrian Kent. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes. *Physical Review Letters*, 109:130501, Sep 2012.

[Ken13] Adrian Kent. A no-summoning theorem in relativistic quantum theory. *Quantum Information Processing*, 12(2):1023–1032, 2013.

[Ken18] Adrian Kent. Summoning, No-Signaling and Relativistic Bit Commitments. *ArXiv e-prints*, arXiv:1804.05246 [quant-ph], April 2018. `https://arxiv.org/abs/1804.05246`.

[KMS11] Adrian Kent, William Munro, and Timothy Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Phys. Rev. A*, 84:012326, Jul 2011.

[KMSB06] Adrian Kent, William Munro, Timothy Spiller, and Raymond Beausoleil. Tagging systems, 2006. Patent No. US 7075438.

[KTHW13] Jędrzej Kaniewski, Marco Tomamichel, Esther Hänggi, and Stephanie Wehner. Secure bit commitment from relativistic constraints. *IEEE Transactions on Information Theory*, 59:4687–4699, 2013.

[LC97] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78:3410–3413, 1997.

[LKB+13] Tommaso Lunghi, Jędrzej Kaniewski, Felix Bussières, Raphael Houlmann, Marco Tomamichel, Adrian Kent, Nicolas Gisin, Stephanie Wehner, and Hugo Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Physical Review Letters*, 111:180504, 2013.

[LKB+15] Tommaso Lunghi, Jędrzej Kaniewski, Felix Bussières, Raphael Houlmann, Marco Tomamichel, Stephanie Wehner, and Hugo Zbinden. Practical Relativistic Bit Commitment. *Physical Review Letters*, 115, 2015.

[LWW+10] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686–689, Aug 2010.

[MAG06] Ll. Masanes, A. Acin, and N. Gisin. General properties of nonsignaling theories. *Physical Review A*, 73:012112, Jan 2006.

[Mal10a] Robert Malaney. Location-dependent communications using quantum entanglement. *Phys. Rev. A*, 81:042319, Apr 2010.

[Mal10b] Robert Malaney. Quantum location verification in noisy channels. In *2010 IEEE Global Telecommunications Conference GLOBECOM 2010*, pages 1–6, 2010.

[May97] Dominic Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Physical Review Letters*, 18:3414–3417, 1997.

[MY98] Dominic Mayers and Andrew Chi-Chih Yao. Quantum cryptography with imperfect apparatus. In *FOCS 1998* [DBL98], pages 503–509.

[Nao91] Moni Naor. Bit commitment using pseudorandomness. *Journal of Cryptology*, 4(2):151–158, 1991.

[NC00] Michael Nielsen and Isaac Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[Par70] James L. Park. The concept of transition in quantum mechanics. *Foundations of Physics*, 1(1):23–33, Mar 1970.

[PR94] Sandu Popescu and Daniel Rohrlich. Quantum nonlocality as an axiom. *Foundations of Physics*, 24(3):379–385, 1994.

[RAM16] Ravishankar Ramanathan, Remigiusz Augusiak, and Gláucia Murta. Generalized xor games with d outcomes and the task of nonlocal computation. *Physical Review A*, 93:022333, Feb 2016.

[RK05] Renato Renner and Robert König. Universally Composable Privacy Amplification Against Quantum Adversaries. In Joe Kilian, editor, *Theory of Cryptography*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer, 2005.

[RKKM14] I. V. Radchenko, K. S. Kravtsov, S. P. Kulik, and S. N. Molotkov. Relativistic quantum cryptography. *Laser Physics Letters*, 11(6):065203, 2014.

[Sca16] Giada Scalpelli. On the Binding Property of Two-Prover Commitment Schemes: Definitions and Composability. Master's thesis, Università degli Studi Di Padova, 2016.

[SCK14] Jamie Sikora, André Chailloux, and Iordanis Kerenidis. Strong Connections Between Quantum Encodings, Non-Locality and Quantum Cryptography. *Physical Review A*, page 9, 2014.

[Sha49] Claude Shannon. Communication Theory of Secrecy Systems. *The Bell System Technical Journal*, 28(4):656–715, Oct 1949.

[Sho97] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997.

[Sim07] Jean-Raymond Simard. Classical and quantum strategies for bit commitment schemes in the two-prover model. Master's thesis, McGill University, Montréal, Québec, 2007.

[SRA81] Adi Shamir, Ronald L. Rivest, and Leonard M. Adleman. Mental poker. In David A. Klarner, editor, *The Mathematical Gardner*, pages 37–43. Springer US, Boston, MA, 1981.

[VMH+16] Ephanielle Verbanis, Anthony Martin, Raphaël Houlmann, Gianluca Boso, Félix Bussieres, and Hugo Zbinden. 24-Hour Relativistic Bit Commitment. *Physical Review Letters*, 117(14):140506, 2016. ID: unige:88082.

[WCSL10] Stephanie Wehner, Marcos Curty, Christian Schaffner, and Hoi-Kwong Lo. Implementation of two-party protocols in the noisy-storage model. *Physical Review A*, 81(5):052336, May 2010.

[Wil13] Mark Wilde. *Quantum Information Theory*. Cambridge University Press, New York, NY, USA, 2013.

[Wyn75] Aaron D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, Oct 1975.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802, October 1982.