# References

[1] Ronald de Wolf. *Quantum Computing and Communication Complexity.* PhD thesis, 2001.

[2] Sean Hallgren, Alexander Russell, and Amon Ta-Shma. The hidden subgroup problem and quantum computation using group representations. *SIAM Journal on Computin*, 32(4):916–934, 2003. Earlier version in STOC'00.

[3] G. H. Hardy and E. M. Wrigh. *An Introduction to the Theory of Numbers.* Oxford University Press, New York, fifth edition, 1979.

[4] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Experimental loophole-free violation of a bell inequality using entangled electron spins separated by 1.3 km. *Nature*, 526, 29 October 2015.

[5] A. S. Holevo. Bounds for the quantity of information transmitted by a quantum communication channel. *Problemy Peredachi Informatsii*, 9(3):3–11, 1973. English translation in *Problems of Information Transmission*, 9:177-183, 1973.

[6] Peter Høyer, Troy Lee, and Robert palek. Negative weights make adversaries stronger. In *Proceedings of 39th ACM STOC*, pages 526–535, 2007.

[7] Peter Høyer and Robert palek. Lower bounds on quantum query complexity. *Bulletin of the EATCS*, 87:78–108, October 2005.

[8] Gbor Ivanyos, Luc Sanselme, and Miklos Santha. An effcient quantum algorithm for the hidden subgroup problem in nil-2 groups. *Algorithmica*, 62(1–2):480–492, 2012.

[9] Stacey Jeffery, Robin Kothari, and Frederic Magniez. Nested quantum walks with quantum data structures. In *Proceedings of 24th ACM-SIAM SODA*, pages 1474–1485, 2013.

[10] Jonathan Katz and Luca Trevisan. On the effciency of local decoding procedures for error-correcting codes. In *Proceedings of 32nd ACM STOC*, pages 80–86, 2000.

[11] Iordanis Kerenidis and Ronald de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. *Journal of Computer and System Sciences*, 69(3):395–420, 2004. Earlier version in STOC'03.

[12] A. Yu. Kitaev. Quantum measurements and the abelian stabilizer problem, 12 November 1995.

[13] Boaz Klartag and Oded Regev. Quantum one-way communication is exponentially stronger than classical communication. *Proceedings of 43rd ACM STOC*, 2011.

[14] Emanuel Knill, Raymond Laflamme, and Wojciech Zurek. Threshold accuracy for quantum computation, 15 October 1996.

[15] Donald E. Knuth. *The Art of Computer Programming. Volume 2: Seminumerical Algorithms.* Addison-Wesley, third edition, 1997.

[16] Francois Le Gall. Improved quantum algorithm for triangle finding via combinatorial arguments. In *Proceedings of 55th IEEE FOCS*, pages 216–225, 2014.

[17] Troy Lee, Frdric Magniez, and Miklos Santha. Improved quantum query algorithms for triangle finding and associativity testing. *Algorithmica*, 77(2):459–486, 2017.

[18] Arjen K. Lenstra and Hendrik W. Jr. Lenstra. *The Development of the Number Field Sieve*, volume 1554 of *Lecture Notes in Mathematics*. Springer, 1993.

[19] Hendrik W. Jr. Lenstra and Carl Pomerance. A rigorous time bound for factoring integers. *Journal of the American Mathematical Society*, 5:483–516, 1992.

[20] Hoi-Kwong Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances, 3 March 1998.

[21] Frdric Magniez, Miklos Santha, and Mario Szegedy. Quantum algorithms for the triangle problem. In *Proceedings of 16th ACM-SIAM SODA*, pages 1109–1117, 2005.

[22] Yuri Manin. *Vychislimoe i nevychislimoe (computable and noncomputable).* Soviet Radio, 1980. In Russian.

[23] Yuri Manin. Classical computing, quantum computing, and shors factoring algorithm, 2 March 1999.

[24] Dominic Mayers. Unconditional security in quantum cryptography, 10 February 1998.

[25] Cristopher Moore, Daniel Rockmore, and Alexander Russell. Generic quantum fourier transforms. *ACM Transactions on Algorithms*, 2(4):707–723, 2006.

[26] Cristopher Moore, Alexander Russell, and Leonard J. Schulman. The symmetric group defies strong fourier sampling. *SIAM Journal on Computing*, 37(6):1842–1864, 2008. Earlier version in FOCS05.

[27] Michele Mosca and Artur Ekert. The hidden subgroup problem and eigenvalue estimation on a quantum computer. In *Proceedings of 1st NASA QCQC conference*, volume 1509 of *Lecture Notes in Computer Science*, pages 174–188. Springer, 1998.

[28] Ashwin Nayak. Optimal lower bounds for quantum automata and random access codes. In *Proceedings of 40th IEEE FOCS*, pages 369–376, 1999.

[29] Ilan Newman. Private vs. common random bits in communication complexity. *Information Processing Letters*, 39(2):67–71, 1991.

[30] Ilan Newman and Mario Szegedy. Public vs. private coin ips in one round communication games. In *Proceedings of 28th ACM STOC*, volume 39, pages 561–570, 1996.

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

[32] Christos H. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[33] Alexander Razborov. Quantum communication complexity of symmetric predicates. *Izvestiya of the Russian Academy of Sciences, mathematics*, 67(1):159–176, 2003.

[34] Ben Reichardt. Span programs and quantum query complexity: The general adversary bound is nearly tight for every boolean functio. In *Proceedings of 50th IEEE FOCS*, pages 544–551, 2009.

[35] R. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[36] R. L. Rivest. *Cryptography*, pages 717–755. In [46], 1990.

[37] Miklos Santha. Quantum walk based search algorithms. In *Proceedings of 5th TAMC*, pages 31–46, 2008.

[38] A. Schönhage and V. Strassen. Schnelle multiplikation grosser zahlen. *Computing*, 7:281–292, 1971.

[39] uwe Schöning. A probabilistic algorithm for k-sat and constraint satisfaction problems. In *proceedings of 40th IEEE FOCS*, pages 410–414, 1999.

[40] Alexander Sherstov. Approximating the and-or tree. *Theory of Computing*, 9(20):653–663, 2013.

[41] Peter Shor. Scheme for reducing decoherence in quantum memory. *Physical Review A*, 52:2493, 1995.

[42] Peter Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997. Earlier version in FOCS94.

[43] Daniel Simon. On the power of quantum computation. *SIAM Journal on Computing*, 26(5):1474–1483, 1997. Earlier version in FOCS94.

[44] Barbara M. Terhal. Quantum error correction for quantum memories. *Reviews of Modern Physics*, 87:307, 2015.

[45] Luca Trevisan. Some applications of coding theory in computational complexity. *Quaderni di Matematica*, 13:347–424, 2004.

[46] Jan van Leeuwen. *Handbook of Theoretical Computer Science. Volume A: Algorithms and Complexity.* MIT Press, Cambridge, MA, 1990.

[47] Lieven Vandersypen, Matthias Steffen, Gregory Breyta, Constantino Yannoni, Richard Cleve, and Isaac Chuang. Experimental realization of an order-nding algorithm with an nmr quantum computer. *Physical Review Letters*, 85(25):5452–545, 2000.

[48] John Watrous. Quantum algorithms for solvable groups. In *Proceedings of 33rd ACM STOC*, pages 60–67, 2001.

[49] John Watrous. Quantum computational complexity. In *Encyclopedia of Complexity and System Science*. Springer, 2009.

[50] W. K. Wootters and W. H. Zurek. A single quantum cannot be copied. *Nature*, 299:802–803, 1982.

[51] Andrew Chi-Chih Yao. Some complexity questions related to distributive computing. In *Proceedings of 11th ACM STOC*, pages 209–213, 1979.

[52] Andrew Chi-Chih Yao. Quantum circuit complexity. In *Proceedings of 34th IEEE FOCS*, pages 352–360, 1993.