AIP Conference Proceedings 2018 vol.1936

Computing quantum hashing in the model of quantum branching programs

Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2018 Author(s). We investigate the branching program complexity of quantum hashing. We consider a quantum hash function that maps elements of a finite field into quantum states. We require that this function is preimage-resistant and collision-resistant. We consider two complexity measures for Quantum Branching Programs (QBP): a number of qubits and a number of compu-tational steps. We show that the quantum hash function can be computed efficiently. Moreover, we prove that such QBP construction is optimal. That is, we prove lower bounds that match the constructed quantum hash function computation.

http://dx.doi.org/10.1063/1.5025458

References

[1] F. Ablayev and A. Vasiliev, Laser Physics Letters 11, p. 025202 (2014). 10.1088/1612-2011/11/2/025202

[2] D. Gottesman and I. Chuang, "Quantum digital signatures," Tech. Rep. arXiv:quant-ph/0105032 (Cornell University Library, 2001).

[3] A. S. Holevo, Probl. Pered. Inform. [Probl. Inf. Transm.] 9, 3-11 (1973).

[4] R. Amiri and E. Andersson, Entropy 17, 5635-5659 (2015), arXiv:1508.01893.

[5] J. Naor and M. Naor, "Small-bias probability spaces: Efficient constructions and applications," in Proceed-ings of the Twenty-second Annual ACM Symposium on Theory of Computing, STOC '90 (ACM, New York, NY, USA, 1990), pp. 213-223.

[6] F. Ablayev and A. Vasiliev, in Computing with New Resources, Lecture Notes in Computer Science, edited by C. S. Calude, R. Freivalds, and I. Kazuo (Springer International Publishing, 2014), pp. 149-160.

[7] A. Nayak, "Optimal lower bounds for quantum automata and random access codes," in Foundations of Computer Science, 1999. 40th Annual Symposium on (1999), pp. 369-376.

[8] F. Ablayev and M. Ablayev, in Descriptional Complexity of Formal Systems, Lecture Notes in Computer Science, Vol. 8614, edited by H. Jurgensen, J. Karhumaki, and A. Okhotin (Springer International Publishing, 2014), pp. 42-52.

[9] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. 87, p. 167902 Sep (2001). 10.1103/PhysRevLett.87.167902

[10] A. Vasiliev, Lobachevskii Journal of Mathematics 37, 751-754 (2016). 10.1134/S1995080216060184

[11] A. Ben-Aroya and A. Ta-Shma, Theory of Computing 9, 253-272 (2013). 10.4086/toc.2013.v009a005