F.M. Ablayev, M.F. Ablayev, A.V. Vasiliev

Title: QUANTUM HASHING

Abstract:

In [1] we explicitly defined a notion of quantum hashing as a generalization of classical hashing and presented examples of quantum hash functions. It appeared that Gottesman-Chuang quantum signature scheme [2] is based on the functions which are actually quantum hash functions. Unlike classical hash functions that are secure under some computational assumptions, these functions have ``unconditionally one-way'' property based on Holevo Theorem [3].

A good source of information on the state of now days development in area of cryptographic hashing and quantum signatures presented the review paper [4].

Recall that in the classical setting a cryptographic hash function h should be computed efficiently and should have the following properties (see for example [4]). (1) Pre-image resistance: Given h(x), it should be difficult to find x, that is, these hash functions are one-way functions. (2) Second pre-image resistance: Given x_1, it should be difficult to find an x_2, such that h(x_1) = h(x_2). (3) Collision resistance: It should be difficult to find any pair of distinct x_1, x_2, such that h(x_1) = h(x_2). Note, that there are no classical one-way functions that are known to be provably more difficult to invert than to compute, the security of such cryptographic hash functions is ``computationally conditional''.

In the talk we consider a quantum hash function construction based on epsilon-biased sets [5]. Such a function hashes elements of finite field F_q into the s-qubit quantum states. The notion of (delta, epsilon)-hash function combines the notion of pre-image (one-way) quantum delta-resistance property and the notion of quantum collision epsilon-resistance property. These properties are quantum generalizations of classical one-way resistance and collision resistance properties required for classical hash functions.

An important part of the one-way property is computational efficiency. In this paper we show that the considered construction of quantum (delta, epsilon)-hash function can be computed efficiently in the model of Quantum Branching Programs (QBP). We consider two complexity measures: a number of qubits Mem(Q) that a QBP Q uses for computation and a number of computational steps Time(Q) that Q performs. Such a QBP for our hash function requires s=O(log{log q}) qubits and performs log q steps. Note that a number Time(Q) of computational steps corresponds to query complexity of quantum algorithm Q.

We prove that the proposed QBP construction is optimal. That is, we prove lower bounds of Omega(log{log q}) for the memory Mem(Q) and Omega(log{q}) for the time Time(Q) of quantum (delta,epsilon)-hash function implementation.

REFERENCES

[1] F. Ablayev and A. Vasiliev, Laser Physics Letters 11, p. 025202 (2014).

[2] D. Gottesman and I. Chuang, "Quantum digital signatures," arXiv:quant-ph/0105032.

[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 Proceedings of the Twenty-second Annual ACM Symposium on Theory of Computing, STOC '90 (ACM, USA, 1990), pp. 213-223.