

Lobachevskii Journal of Mathematics 2015 vol.36 N2, pages 89-96

Quantum hashing via ϵ -universal hashing constructions and classical fingerprinting

Ablayev F., Ablayev M.

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

Abstract

© 2015, Pleiades Publishing, Ltd. In the paper, we define the concept of the quantum hash generator and offer design, which allows to build a large amount of different quantum hash functions. The construction is based on composition of classical ϵ -universal hash family and a given family of functions-quantum hash generator. In particular, using the relationship between ϵ -universal hash families and Freivalds fingerprinting schemas we present explicit quantum hash function and prove that this construction is optimal in the sense of number of qubits needed for construction.

<http://dx.doi.org/10.1134/S199508021502002X>

Keywords

error-correcting codes, quantum hash function, quantum hashing, ϵ -universal hashing