Lobachevskii Journal of Mathematics 2016 vol.37 N6, pages 758-767

On quantum (δ, ϵ)-resistant hashing

Ablayev M.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2016, Pleiades Publishing, Ltd.In the paper we define a notion of quantum resistant ((δ, ϵ)-resistant) hash function which combine together a notion of pre-image (one-way) resistance (δ-resistance) property and the notion of collision resistance (ϵ-resistance) properties. We present a discussion that supports the idea of quantum hashing oriented for cryptographical purposes. We propose a quantum setting of a classical digital signature scheme do demonstrate a theoretical possibilities and restrictions of (δ, ϵ)-hashing. The assumption we use is that a set of qubits (quantum hash) we generate, send, and receive during the execution of a protocol can be stored for a certain (a large enough) amount of time; next, the scheme requires the high degree of entanglement between the qubits which makes such a quantum hash. These properties make quantum hash cryptographically efficient.

http://dx.doi.org/10.1134/S1995080216060081

Keywords

errorcorrecting codes, quantum hash function, Quantum hashing, quantum signature, δ-universal hashing