Laser Physics Letters 2015 vol.12 N12

On the concept of cryptographic quantum hashing

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

Abstract

© 2015 Astro Ltd. In the letter we define the notion of a quantum resistant ((ε, δ)-resistant) hash function which consists of a combination of pre-image (one-way) resistance (ε-resistance) and collision resistance (δ-resistance) properties. We present examples and discussion that supports the idea of quantum hashing. We present an explicit quantum hash function which is 'balanced', one-way resistant and collision resistant and demonstrate how to build a large family of quantum hash functions. Balanced quantum hash functions need a high degree of entanglement between the qubits. We use a phase transformation technique to express quantum hashing constructions, which is an effective way of mapping hash states to coherent states in a superposition of time-bin modes. The phase transformation technique is ready to be implemented with current optical technology.

http://dx.doi.org/10.1088/1612-2011/12/12/125204

Keywords

quantum hashing, quantum one-way function, quantum signature