Laser Physics Letters 2014 vol.11 N2

Cryptographic quantum hashing

Ablayev F., Vasiliev A.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

We present a version of quantum hash functions based on non-binary discrete functions. The proposed quantum procedure is 'classical-quantum', that is, it takes a classical bit string as an input and produces a quantum state. The resulting function has the property of a one-way function (pre-image resistance); in addition it has properties analogous to classical cryptographic hash second pre-image resistance and collision resistance. We also show that the proposed function can be naturally used in a quantum digital signature protocol. © 2014 Astro Ltd.

http://dx.doi.org/10.1088/1612-2011/11/2/025202

Keywords

quantum cryptography, quantum digital signature, quantum fingerprinting, quantum hashing, quantum one-way function