Russian Mathematics 2016 vol.60 N9, pages 61-65

Binary quantum hashing

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

Abstract

© 2016, Allerton Press, Inc.We propose a binary quantum hashing technique that allows to present binary inputs by quantum states. We prove the cryptographic properties of the quantum hashing, including its collision resistance and preimage resistance. We also give an efficient quantum algorithm that performs quantum hashing, and altogether this means that this function is quantum one-way. The proposed construction is asymptotically optimal in the number of qubits used.

http://dx.doi.org/10.3103/S1066369X16090073

Keywords

binary linear codes, quantum branching programs, quantum computation, quantum cryptography, quantum hashing