Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 2014 vol.8614, pages 42-52

Quantum hashing via ε-universal hashing constructions and Freivalds' fingerprinting schemas

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

Abstract

We define the concept of a quantum hash generator and offer a design, which allows one to build a large number of different quantum hash functions. The construction is based on composition of a classical ε-universal hash family and a given family of functions - quantum hash generators. 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 with respect to the number of qubits needed for the construction. © 2014 Springer International Publishing.

http://dx.doi.org/10.1007/978-3-319-09704-6_5

Keywords

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