Lobachevskii Journal of Mathematics 2016 vol.37 N6, pages 753-757

Quantum hashing for finite abelian groups

Vasiliev A.

Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2016, Pleiades Publishing, Ltd.We propose a generalization of the quantum hashing technique based on the notion of small-bias sets. These sets have proved useful in different areas of computer science, and here their properties give an optimal construction for succinct quantum presentation of elements of any finite abelian group, which can be used in various computational and cryptographic scenarios. We consider two special cases of the proposed quantum hashing which turn out to be the known quantum fingerprinting schemas.

http://dx.doi.org/10.1134/S1995080216060184

Keywords

finite groups, Quantum cryptography, quantum hashing, small-bias sets