Lobachevskii Journal of Mathematics 2016 vol.37 N6, pages 705-712

From graphs to keyed quantum hash functions

Ziatdinov M.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© 2016, Pleiades Publishing, Ltd.We present two new constructions of quantum hash functions: the first based on expander graphs and the second based on extractor functions and estimate the amount of randomness that is needed to construct them. We also propose a keyed quantum hash function based on extractor function that can be used in quantum message authentication codes and assess its security in a limited attacker model.

http://dx.doi.org/10.1134/S1995080216060202

Keywords

expander graph, extractor, keyed quantum hash function, message authentication, Quantum hash function