Journal of Physics: Conference Series 2016 vol.681 N1

On the balanced quantum hashing

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

Abstract

In the paper we define a notion of a resistant quantum hash function which combines a notion of pre-image (one-way) resistance and the notion of collision resistance. In the quantum setting one-way resistance property and collision resistance property are correlated: the "more" a quantum function is one-way resistant the "less" it is collision resistant and vice versa. We present an explicit quantum hash function which is "balanced" one-way resistant and collision resistant and demonstrate how to build a large family of balanced quantum hash functions.

http://dx.doi.org/10.1088/1742-6596/681/1/012019