Quantum Hashing via ε-Universal Hashing Constructions

Farid Ablayev[1], **Marat Ablayev**[1], **and Alexander Vasiliev**[1]
[1]*Kazan Federal University, 18 Kremlyovskaya St., Kazan 420008, Russian Federation*

e-mail: *fablayev@gmail.com*

Quantum computing is inherently a very mathematical subject, and discussions of how quantum computers can be more efficient than classical computers in breaking encryption algorithms have started since Peter Shor invented his famous quantum algorithm. The reaction of a cryptography community was a "Post-quantum cryptography", which refers to the research of problems (usually public-key cryptosystems) that are not efficiently breakable using quantum computers. Currently post-quantum cryptography includes different approaches, in particular, hash-based signature schemes such as Lamport signature and Merkle signature scheme. Hashing itself is an important basic concept of computer science. The concept known as "universal hashing" was invented by Carter and Wegman in 1979.

In our research we define a quantum hashing as a quantum generalization of the classical hashing. We define the concept of a quantum hash generator and offer 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 generator.

The relationship between ε-universal hash families and error-correcting codes give possibilities to build a large amount of different quantum hash functions. In particular, we present quantum hash function based on Reed-Solomon code, and we prove, that this construction is optimal in the number of qubits needed.

Using the relationship between ε-universal hash families and Freivalds' fingerprinting schemas we present an explicit quantum hash function and prove that this construction is optimal with respect to the number of qubits.

Acknowledgements. The work is performed according to the Russian Government Program of Competitive Growth of Kazan Federal University. Work was in part supported by the Russian Foundation for Basic Research (under the grants 14-07-00878, 15-37-21160).

[1] F. Ablayev, A. Vasiliev. Cryptographic quantum hashing // Laser Physics Letters. - Volume 11, Number 2, 2014.

[2] F. Ablayev, M. Ablayev. Quantum Hashing via ϵ-universal Hashing Constructions and Freivalds Fingerprinting Schemas // Proceedings of the 16th International Workshop on Descriptional Complexity of Formal Systems (DCFS), Springer LNCS volume 8614. - 2014. - P. 42-52.