Contribution ID: **34** Type: **not specified**

Dense Quantum Hashing

Monday 27 May 2024 16:20 (20 minutes)

In [1] we have proposed a cryptographic quantum hash function and later in [2] provided its generalized version for arbitrary finite abelian groups based on the notion of -biased sets. However, the physical implementation of such functions nowadays poses a great challenge for the engineers since the proposed constructions of quantum hashing require completely entangled quantum states, which are hard to create and maintain. Therefore, in [3] we have proposed a simplified version of the quantum hash function that minimizes quantum state engineering and experimentally verified the collision resistance of such function. In this research we improve this approach by introducing a dense encoding of the classical information by the quantum states. Let $S = s_1, ..., s_m \; Z_q$ be the set of numeric parameters. We propose a quantum hash function $\psi(x, y)$ that encodes classical information by the following superposition:

$$|\psi_j(x,y) \; = \cos \; \frac{\pi s_j x}{2q} |0 \; + e^{i 2\pi s_j y/q} \sin \; \frac{\pi s_j x}{2q} |1 \;, |\psi(x,y) \; = |\psi_1(x,y) \; |\psi_2(x,y) \quad |\psi_m(x,y) \; .$$

That is, the quantum hash $|\psi(x,y)$ of the classical input (x,y) is composed of m independent hashes $|\psi_j(x,y)$ of smaller size. The only difference between them is the value of the numeric parameter s_j. The pair of arguments (x,y) can be interpreted as the split of a larger input, or as a pair of an input and a key. In any case this means that we can double the amount of information encoded in the same number of qubits as compared to [3]. The main idea behind quantum hashing is to provide the minimal fidelity of different quantum hash codes (collision resistance) with the minimal possible number of qubits (that affects the one-way property) [4]. The fidelity in our case can be expressed by the following formula:

$$\prod_{j=1}^{m} \cos^2 \; \frac{\pi s_j (x_2 - x_1)}{2q} - \sin \; \frac{\pi s_j x_1}{2q} \sin \; \frac{\pi s_j x_2}{2q} \sin^2 \; \frac{\pi s_j (y_2 - y_1)}{q} \; .$$

The formula above gives the probability of considering hashes $|\psi(x_1, y_1)$ and $|\psi(x_2, y_2)$ to be equal, and the set of parameters $S = s_1, ..., s_m$ should be computed as the result of minimization of this formula over all pairs of unequal inputs.

References

1. Ablayev F.M., Vasiliev A.V. Cryptographic quantum hashing // Laser Physics Letters. –2014. –V.11, No. 2. –Art. No. 025202.

2. Vasiliev A. Quantum hashing for finite abelian groups // Lobachevskii Journal of Mathematics. –2016. –Vol. 37, No. 6. –P. 751-754.

3. Turaykhanov D.A., Akat'ev D.O., Vasiliev A.V., Ablayev F.M., Kalachev A.A. Quantum hashing via single-photon states with orbital angular momentum // Phys. Rev. A. –2021. –V. 104. –Art. no 052606.

4. Ablayev F., Ablayev M., Vasiliev A. On the balanced quantum hashing // Journal of Physics: Conference Series. –2016. –Vol. 681, No. 1. –Art. No. 012019.

Author: VASILIEV, Alexander (Kazan Federal University)

Presenter: VASILIEV, Alexander (Kazan Federal University)