Quantum Hashing *Via* Single Photons

D O Akat'ev[1], D A Turaykhanov[1], N M Shafeev[2], A V Vasiliev[2], F M Ablayev[2], and A A Kalachev[1]

[1]*Kazan Scientific Center of RAS, 2/31, Lobachevsky st., 420111, , Kazan, Russia*
[2]*Kazan Federal University, 18, Lobachevsky st., 420111, , Kazan, Russia*
Contact Email: a.a.kalachev@mail.ru

Hashing is an important tool in computer science that today has become essential in cybersecurity, cryptography, data-intensive research, etc. Hashing algorithms compress a message of any length into a digest of a fixed length (hash), so that hashing is widely used in various data storage and retrieval applications to reduce the data access time. In particular, hashing algorithms can reliably inform us whether two files are identical without opening and comparing them, and they are key ingredient for verification of message integrity, digital signatures, fingerprinting and other cryptographic applications. Moreover, a universal hash function is an important part of the privacy amplification process of the quantum key distribution. For such applications, a good hashing algorithm should satisfy two main properties: one-way property and collision resistance. The first means that restoring an input string from its hash (decoding) should be a computationally hard problem, while the second means that the situation when two different inputs have the same hash (which is called a collision) is hard to observe.

A quantum hashing is a promising generalization of the cryptographic hashing concept on the quantum domain. In this case, the hash function encodes a classical input state into a quantum state so that to optimize the trade-off between one-way property and collision resistance. In the present work, we consider a new version of quantum hashing technique wherein a quantum hash is constructed as a sequence of single-photon qubits [1] or qudits [2]. A proof-of-principle implementation of the quantum hashing protocol using orbital-angular momentum encoding of single photons demonstrates good agreement with theoretical predictions. In particular, it shows that the number of qudits decreases with increase of their dimension for an optimal ratio between collision probability and decoding probability of the hash [2]. The prospects of increasing dimension of information carriers, which makes quantum hashing with single photons more efficient, are discussed.

References

[1] D A Turaykhanov, D O Akat'ev, A V Vasiliev, F M Ablayev and A A Kalachev. Phys. Rev. A **104**, 052606 (2021)

[2] D O Akat'ev, A V Vasiliev, N M Shafeev, F M Ablayev and A A Kalachev, Laser Phys. Lett. **19**, 125205 (2022)