Quantum walk algorithm in chaos based cryptography

V. Berec

University of Belgrade, Serbia

The system exhibiting dynamical chaos is characterized by the pseudorandom local instabilities of trajectories in the phase space. This is essentially deterministic nonlinear system, highly receptive to initial conditions and environmental inputs. As a result, numerical errors during computations on classical computers increase exponentially with time by perturbing the dynamical trajectories from the statistics of initial parameters after a few cycles of the periodic motion. In order to prevent the accumulation of errors, the simulation of trajectory distributions in total phase space even for moderate times demands an exponential number of orbits and soon exceeds the capacity of classical information systems [1]. On the other hand, the ergodicity of chaotic orbits and the fact that amply set of unstable periodic orbits are embedded within the chaotic attractor, lay foundation for the control of chaos by guarantying that the system evolution, within the attractor, will always reach close proximity of any point of any unstable periodic orbit in finite time. Quantum computing appears to redefine the problem of chaos control in terms of quantum cryptography by utilizing the development of quantum keys with Shor discovery of efficient algorithms for factorization of large integers and findings of discrete logarithms. The difficulty of factoring and discrete logarithms feasibility is at the core of present public-key cryptography. Furthermore, the implementations of realistic quantum simulators which utilize the quantum interference of various computational paths to reduce computation complexity and suppress erroneous outcomes of computations can produce extensive computational speedup.

In this paper we will outline the construction of quantum walk algorithm considered to solve plethora of problems [2] such as triangle-finding, commutativity testing, matrix product verification and data clustering. Moreover, quantum walk [3] relies on intrinsically unpredictably 'chaotic' nonlinear dynamic behavior resulting that it can be employed as an excellent key generator. The infinite resources of the permutations over the coin states make quantum walk a prime candidate for producing a theoretically infinite key manifold to resist brute-force attacks.

[l] V. Berec, EPJ Web of Conf. **95**, 04007 (2015).

[2] Q. Li, Y. He, Jiang J.-P., Quantum Inf. Process **10(1)**, 13 (2011).

[3] S.E. Venegas-Andraca, Quantum Inf. Process **11(5)**, 1015 (2012).