Journal of Engineering and Applied Sciences 2017 vol.12 N4, pages 877-880

Minimizing collisions for quantum hashing

Vasiliev A., Latypov M., Ziatdinov M.
Kazan Federal University, 420008, Kremlevskaya 18, Kazan, Russia

Abstract

© Medwell Journals, 2017. Hashing is a widely used technique in computer science. The recently proposed quantum hashing has also proved its usefulness in a number of applications. The key property of both classical and quantum hashing is the ability to withstand collisions however, the notion of collision itself is different in the classical and quantum setting. In this study we analyze the set of numeric parameters that determine the probability of quantum collisions for the quantum hashing. Although, there is a general method of obtaining good hashing parameters, it makes sense for comparatively large inputs. That is why we construct different methods to complement the general one. We present two explicit optimization algorithms for computation of quantum hashing parameters: one is based on the genetic approach and the other uses the annealing simulation. The solution to the considered optimization problem can be used for the variety of quantum hash functions and also provides a solution to the general problem of constructing sets of pairwise distinguishable states in low-dimensional spaces.

http://dx.doi.org/10.3923/jeasci.2017.877.880

Keywords

Annealing simulation algorithm, Genetic algorithm, Quantum computation, Quantum hashing, Quantum information

References

[1] Ablayev, F. and A. Marat, 2015. On the concept of cryptographic quantum hashing. MSc Thesis, Cornell University, Ithaca, New York

[2] Ablayev, F. and A. Vasiliev, 2014. Computing Boolean Functions via Quantum Hashing. In: Computing with New Resources, Cristian, S.C., F. Rusins and K. Iwama (Eds.). Springer, Switzerland, Europe, ISBN:978-3-319-13349-2, pp: 149-160

[3] Ablayev, F. and M. Ablayev, 2014. Quantum Hashing via E-Universal Hashing Constructions and Freivalds Fingerprinting Schemas. Proceedings of the 16th International Workshop on Descriptional Complexity of Formal Systems (DCFS) 2014, August 5-8, 2014, Springer, Turku, Finland, pp: 42-52

[4] Buhrman, H., R. Cleve, J. Watrous and R.D. Wolf, 2001. Quantum fingerprinting. Phys. Rev. Lett., Vol. 87

[5] Gottesman, D. and I. Chuang, 2001. Quantum digital signatures. MSc Thesis, Cornell University, Ithaca, New York, USA

[6] Holland, J.H., 1975. Adaptation in Natural and Artificial Systems: An Introductory Analysis with Applications to Biology, Control and Artificial Intelligence. 1st Edn., University of Michigan Press, Ann Arbor, MI., USA., ISBN-13: 9780472084609, Pages: 183

[7] Kirkpatrick, S., C.D. Gelatt Jr. and M.P. Vecchi, 1983. Optimization by simulated annealing. Science, 220: 671-680

[8] Razborov, A., E.N.D.R.E. Szemeredi and A. Wigderson, 1993. Constructing small sets that are uniform in arithmetic progressions. Comb. Probab. Comput., 2: 513-518

[9] Vasiliev, A., 2015. Quantum communications based on quantum hashing. Intl. J. Appl. Eng. Res., 10: 31415-31426