HOMOMORPHIC ENCRYPTION OF THE K=2 BERNSTEIN-VAZIRANI ALGORITHM

Pablo Fernández*

Departamento de Física Teórica, Universidad Complutense, 28040 Madrid, Spain

Miguel Ángel Martín-Delgado†

Departamento de Física Teórica, Universidad Complutense, 28040 Madrid, Spain and

CCS-Center for Computational Simulation,

Campus de Montegancedo UPM, 28660 Boadilla del Monte, Madrid, Spain

(Dated: June 2, 2023)

The recursive Bernstein-Vazirani algorithm was the first quantum algorithm to show a superpolynomial improvement over the corresponding best classical algorithm. Here we define a class of circuits that solve a particular case of this problem for second-level recursion. This class of circuits simplifies the number of gates T required to construct the oracle by making it grow linearly with the number of qubits in the problem. We find an application of these circuits to quantum homomorphic encryption (QHE) which is a cryptographic technology useful for delegated quantum computation. It allows a remote server to perform quantum computations on encrypted quantum data, so that the server cannot know anything about the client's data. QHE schemes suitable for circuits with a polynomial number of gates $T/T^\dagger$ have been developed recently. Following these schemes, the simplified circuits we have constructed can be evaluated homomorphically in an efficient way.

---

[1] P. Fernández and M. A. Martin-Delgado, **Prerpint**, arXiv:2303.17426 (2023).

[2] M. Liang, Quantum Information Processing **19**, 28 (2020).

[3] E. Bernstein and U. Vazirani, **Proceedings of the 25th Annual ACM Symposium on Theory of Computing**, 11 (1993).

[4] L. Yu, C. A. Pérez-Delgado and J. F. Fitzsimons, Phys. Rev. A **90**, 050303(R) (2014).

* pabfer23@ucm.es

† mardel@fis.ucm.es