Homomorphic Encryption of the k=2 Bernstein-Vazirani Algorithm

Pablo Fernández
Miguel Ángel Martín-Delgado

Universidad Complutense de Madrid, Plaza Ciencias 1 Ciudad Universitaria 28040, Madrid, Spain

pabfer23@ucm.es

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 that allows a remote server to perform quantum computations on encrypted quantum data, so that the server cannot know anything about the client's data. Liang developed QHE schemes suitable for circuits with a polynomial number of gates *T*/*T*†. Following these schemes, the simplified circuits we have constructed can be evaluated homomorphically in an efficient way.

References

[1] M. Liang, Quantum Information Processing, 19 (2020) 28
[2] E. Bernstein, U. Vazirani, Proceedings of the 25th Annual ACM Symposium on Theory of Computing, (1993) 11
[3] C. Gong, J. Du, Z. Dong et al., Quantum Information Processing, 19 (2020) 105
[4] L. Yu, C. A. Pérez-Delgado, J. F. Fitzsimons, Phys. Rev. A, 90 (2014) 050303(R)
[5] P. Fernández, M. A. Martin-Delgado, arXiv:2303.17426, (2023)

Figures

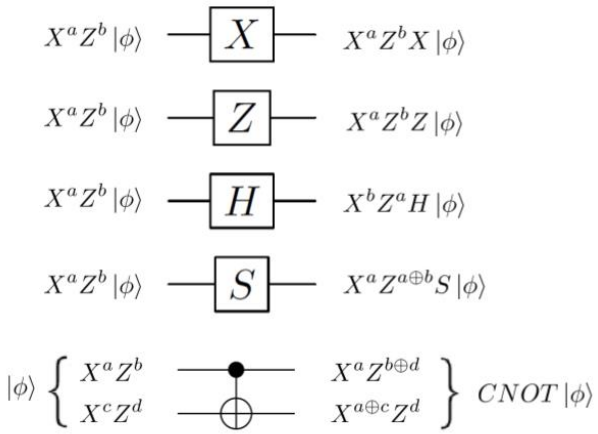

Figure 1: Key updating rules for homomorphic evaluation of Clifford gates

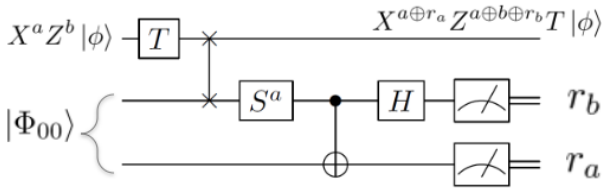

Figure 2: Homomorphic evaluation of *T* gate