

Quantum Search on Encrypted Data Based on Quantum Homomorphic Encryption

Qing Zhou¹, Songfeng Lu^{1,2,*}, Yongquan Cui^{1,*}, Li Li³, and Jie Sun¹

¹School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China

²Shenzhen Huazhong University of Science and Technology Research Institute, Shenzhen 518063, China

³College of Mathematics and Statistics, Shenzhen University, Shenzhen 518060, China

*corresponding author: Songfeng Lu (lusongfeng@hotmail.com) or Yongquan Cui (yqcui1977@hust.edu.cn)

January 28, 2020

Supplement: The quantum homomorphic search circuit for two-qubit encrypted states

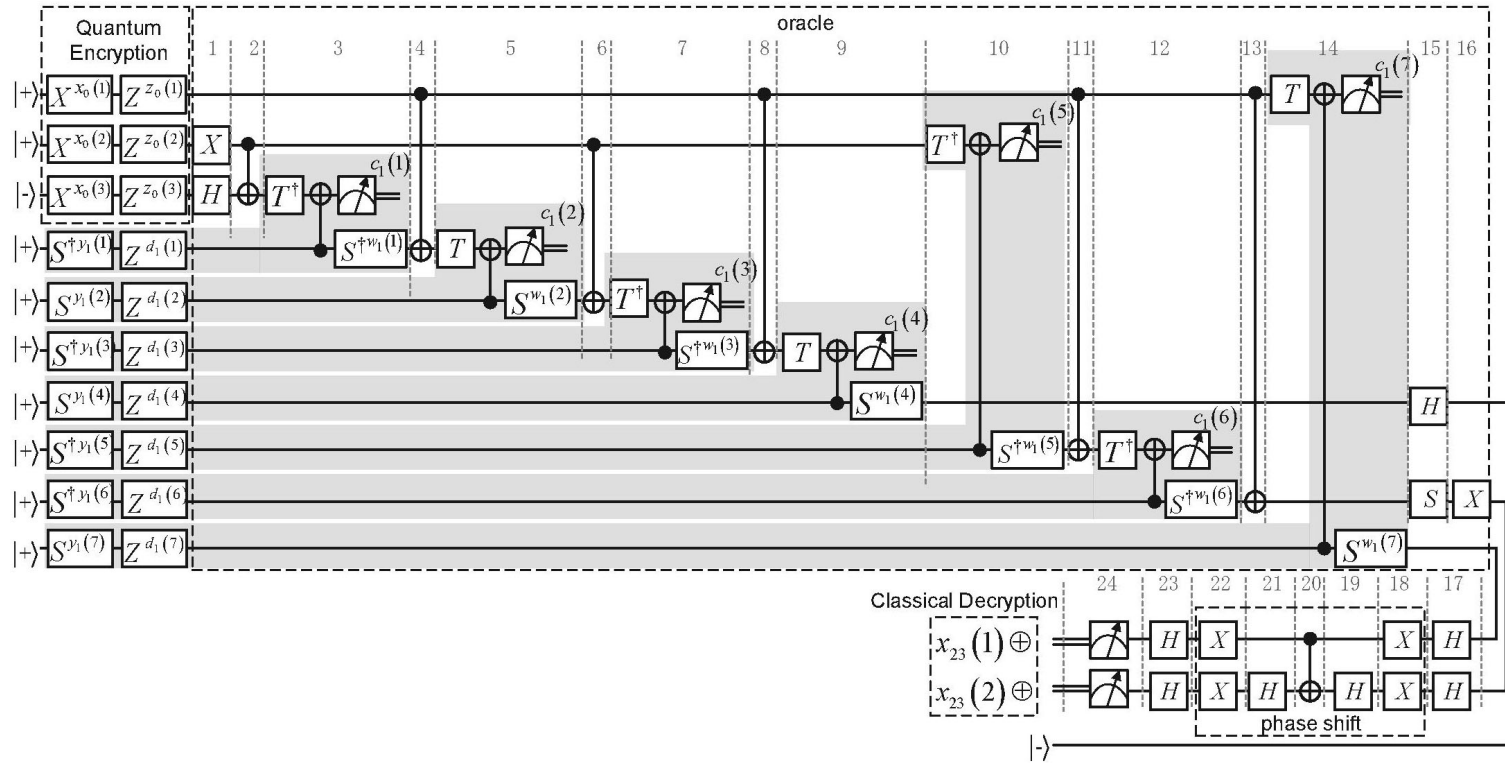


Figure S1. The quantum homomorphic search circuit for two-qubit encrypted states. The circuit can be divided into 24 steps (plus quantum encryption and classical decryption); each step corresponds to a round of key refresh. There are seven T (or $T^\dagger$) gadgets, each of which is marked by a shadowed area. The two-qubit input is encrypted with four key bits — $x_0(1), x_0(2), z_0(1)$ and $z_0(2)$, and the oracle qubit $|-\rangle$ can be thought of as being encrypted with key bits $x_0(3) = z_0(3) = 0$.