Quantum homomorphic encryption from quantum codes

Yingkai Ouyang and Si-Hui Tan
*Singapore University of Technology and Design, 8 Somapah Road, Singapore**

Joseph Fitzsimons
Singapore University of Technology and Design, 8 Somapah Road, Singapore and
Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore*

Homomorphic encryption has been recognised as an important primitive for building secure delegated computation protocols for many decades [1]. It provides a processing functionality for encrypted data which stays secret during the evaluation, and a scheme is *fully-homomorphic* if it allows for arbitrary computation. Despite widespread interest in this problem, it was not until 2009 that the first computationally secure classical scheme for fully homomorphic encryption (FHE) was discovered [2], with many improvements following rapidly from this initial discovery [3, 4], and has recently drawn attention within the quantum information community [5–12]. One might wonder if quantum cryptosystems might offer unconditionally secure homomorphic encryption schemes and whether the privacy homomorphisms could be extended to allow for evaluation of quantum circuits.

Like their classical counterparts, quantum homomorphic encryption (QHE) schemes comprise of four parts: key generation, encryption, evaluation, and decryption. Unlike blind quantum computation [13], in which the computation to be performed forms part of the secret, QHE schemes do not have secret circuit evaluations. They serve to obscure only the information that is contained within the state to be processed using the chosen circuit. The extent to which a scheme is secure depends on its specifics, and in previous work has varied depending on the precise nature of the computation which can be performed on the encrypted input. QHE schemes described in Refs. [9, 10] offer some information theoretic security, but this is only in the form of a gap between the information accessible with and without the secret key, a notion of security which does not imply the stronger notion of security under composition. These schemes are also limited in the set of operations that can be performed on the encrypted data. The scheme in [9] only allows computations in the BosonSampling model, while that in [10] is not known to support encoded universal quantum computing. Broadbent and Jeffrey's scheme [11] enables quantum homomorphic encryption of fixed depth circuits by bootstrapping onto a classical fully homomorphic encryption scheme and as such is only computationally secure. Recently Dulek, Schaffner and Speelman [12] used the garden-hose model of computation with Broadbent and Jeffrey's quantum homomorphic schemes to allow the evaluation of polynomial-depth circuits. Several other schemes for computing on encrypted data have previously been introduced which offer universal quantum computation, but require interactions between the client and evaluator [5–8]. This requirement for interaction places them outside of the formalism of homomorphic encryption, although confusingly several of these schemes use that terminology [5, 6].

The difficulty in creating a perfectly secure quantum fully homomorphic encryption (QFHE) scheme persists, and is in line with the no-go result provided by [14] that perfect information-theoretic security whilst enabling arbitrary processing of encrypted data is impossible, unless the size of the encoding grows exponentially. Nonetheless, given the growing interest in QHE schemes and the multitude of possibilities, Broadbent and Jeffrey set out to provide a rigorous framework for defining QHE schemes [11], basing their security definitions on the requirement for indistinguishability of codewords under chosen plaintext attack with additional computation assumptions. Broadbent and Jeffery also require that a quantum *fully* homomorphic encryption satisfies two properties: correctness and compactness. Perfect correctness occurs when the evaluated output on the cipherstate after decryption is exactly the correct evaluated input.

Here we present a quantum encryption scheme which is homomorphic for arbitrary classical and quantum circuits which have at most some constant number of non-Clifford gates. Unlike classical schemes, the security of the scheme we present is information theoretic, satisfying entropic security definitions, and hence independent of the computational power of an adversary. The QHE scheme we present builds on constructions taken from quantum error correction codes to provide gates for universal quantum computation. The block of qubits that contains the code is embedded in a much larger set of qubits that are initialized in a maximally mixed state. The qubits are then shuffled in a specific but random way to hide the qubits that contain that code. Our protocol guarantees that the trace distance between ciphertexts corresponding to any two quantum inputs is exponentially suppressed. This is a significantly stronger security guarantee than previous homomorphic encryption schemes presented in [9]. Moreover the computation power of our scheme is similar to that of Broadbent and Jeffrey's while avoiding bootstrapping on the classical ho-

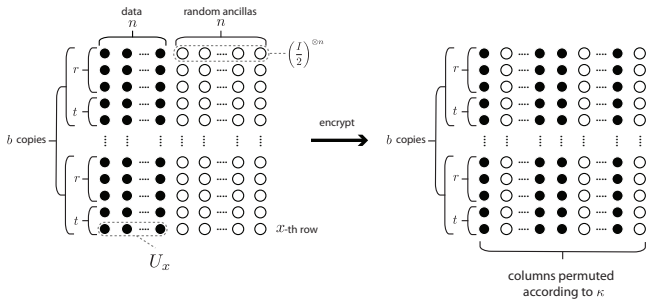

FIG. 1: Figure shows qubits arranged on a grid with shaded circles representing data qubits. Within the x-th row, the n data qubits are in a code encoded by U_x. The unshaded circles are ancilla qubits which are in the completely mixed state. There are r sets of codes, and b copies of such sets. A random permutation of the columns completes the encryption procedure of our quantum homomorphic encryption scheme.

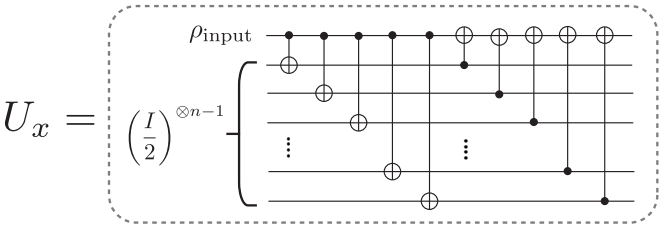

FIG. 2: Figure shows the encoding quantum circuit U_x that is applied on the first n qubits in the x-th row. Each line represents one qubit and the gates are applied in the order from left to right.

momorphic encryption scheme.

Our QHE scheme takes as its input a r-qubit state ρ_{input}, and t independent copies of the magic state $|T\rangle\langle T| = \frac{I}{2} + \frac{X-Y}{2\sqrt{2}}$, all arranged in a single column (See Figure 1). We then introduce $(2n-1)$ more columns of maximally mixed qubits to obtain a grid of qubits with $r+t$ rows and $2n$ columns. Here, we choose n to such that $\frac{n-1}{4}$ is a non-negative integer. Of the new columns introduced, $n-1$ of them will be incorporated as data qubits while the remaining n columns will be used as ancillae in the encryption. An encoding quantum circuit $U = U_1 \otimes \cdots \otimes U_{r+t}$ is applied row-wise on the first n columns. Applying U spreads the quantum input from just the first column to the first n columns. Since every qubit not residing on the first column is maximally mixed, the encoding circuit on each row encodes the quantum data on the first column into a random quantum code, the resultant quantum information of which resides in a random codespace on the first n columns. Encryption is then achieved via randomly permuting the $2n$ columns with a permutation κ. Permuting the columns brings the quantum information to be processed from the first n columns to the columns $k_1, \ldots, k_n$, where $1 \leq k_1 < \cdots < k_n \leq 2n$. For the decryption algorithm, one performs the inverse permutation κ^{-1} of the columns, followed by the inverse unitary $U^\dagger$ on the first n columns of the grid. Finally every qubit in the rows $r+1$ to $r+t$ are measured in the computation basis. The quantum output of our scheme is then located on the first r rows of the first column of our grid of qubits.

To evaluate the circuit, the evaluator operates independently and identically (i.i.d) on not n but $2n$ columns of qubits, n columns of which are the maximally mixed state. The i.i.d structure of the evaluator's operations allows these operations to commute with any secret permutation of the columns of the qubits on the grid. In addition, the evaluators' operations necessarily leave the n columns of qubits initialized in the maximally mixed state unchanged, thereby implementing i.i.d quantum operations on only the columns containing the encoded quantum data. Hence the evaluator, by applying transversal gates on the $2n$ columns, achieves the application of the corresponding transversal gates on the n columns with the quantum data without requiring knowledge of the location of the columns containing the encoded quantum information.

The circuit to be evaluated can always be written as $V = V_d \ldots V_1$, where the evaluator is to apply privacy homomorphisms of the gates V_1 to V_d sequentially. Here, each V_i applies either a Clifford gate or a T gate locally on a single qubit, or applies a CNOT locally on a pair of qubits.

When V_i is a unitary operation that applies a Clifford gate G locally on the x-th qubit, the evaluator can apply the logical G-gate on our random code on the x-th row without any knowledge of the data columns $k_1, \ldots, k_n$. To do so, the evaluator simply applies the unitary $G^{\otimes 2n}$ on the $2n$ qubits located on the x-th row on each copy. Since any unitary operation leaves a maximally mixed qubit state unchanged, the evaluator effectively only applies the unitary $G^{\otimes n}$ on the qubits in the encrypted data columns $k_1, \ldots, k_n$ on the x-th row, which is the logical G-gate on the x-th row.

When V_i is a unitary operation that applies a CNOT gate with control on the x-th qubit and target on the y-th qubit, denoted as $\text{CNOT}_{x,y}$, the evaluator can also apply the corresponding logical CNOT gate on our random code on the x-th and y-th row without any knowledge of the data columns $k_1, \ldots, k_n$. To do so, the evaluator simply applies a CNOT with control qubit on the x-th row and the j-th column and target qubit on the y-th row and the j-th column for every $j = 1, \ldots, 2n$. Since any unitary operation on two qubits leaves a maximally mixed two-qubit state unchanged, the evaluator effectively only applies the unitary $\text{CNOT}^{\otimes n}$ on the qubits in the encrypted data columns $k_1, \ldots, k_n$ with control qubits on the x-th row and target qubits on the y-th row, which is the correct logical CNOT-gate, which we denote as $\overline{\text{CNOT}}_{x,y}$.

When V_i is a unitary operation that applies the k-th non-Clifford gate T on the x-th qubit, the evaluator has to perform gate teleportation [15, 16]. Now consider gate teleportation of a single-qubit gate T. Omitting the correction operation required by gate teleportation allows this procedure to succeed with probability $\frac{1}{2}$ as depicted in Figure 3. The required measurement can be deferred until decryption due to the principle of deferred measurement [17].

To implement gate teleportation of the logical T operation, the evaluator applies privacy homomorphism for $\mathrm{CNOT}_{x,r+k}$ followed by the privacy homomorphism for $\mathrm{CNOT}_{r+k,x}$. Because of the ancilla columns being in the maximally mixed state, the unitary $\overline{\mathrm{CNOT}}_{x,r+k}$ followed by the the unitary $\overline{\mathrm{CNOT}}_{r+k,x}$ are effectively applied on the data columns $k_1, \ldots, k_n$.

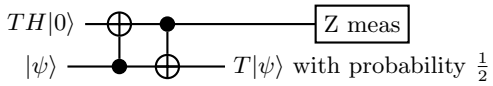

FIG. 3: Gate teleportation of the T-gate without correction.

Our scheme satisfies the correctness and compactness condition of Broadbent and Stacey. Each copy of our scheme yields the correct quantum output with constant probability 2^{-t}. Extra copies simply amplify the probability of success. Thus although each instance of our scheme implements T non-deterministically, it can be said to have *heralded* perfect completeness: namely, $b = \lfloor \sqrt{\frac{\alpha}{2}} + 1 \rfloor^2 2^{2t}$ copies of our scheme yields the correct output in at least one copy with probability at least $1 - e^{-\alpha}$, and we know which of the b copies yield the correct output. An arbitrarily large α brings the success probability arbitrarily close to unity. Since t, b are constant, and the total number of gates required for decryption is independent of the depth of the circuit to be evaluated. Hence, our scheme is compact for circuits with a constant maximum number of T gates and unbounded Clifford gates.

Randomly permuting the columns of qubits obfuscates the subset of columns where the quantum information resides, thereby encrypting the quantum data. The maximum trace distance between any two outputs is exponentially suppressed in n, with value at most $e\left(\frac{4n}{\pi}\right)^{1/4} 4^{b(r+t)} 2^{-n}$, which is exponentially suppressed in n for constant r and t. For full details, see Ref. [18].

This material is based on research supported in part by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01. JFF and ST acknowledges support from the Air Force Office of Scientific Research under AOARD grant FA2386-15-1-4082.

* Electronic address: yingkai_ouyang@sutd.edu.sg

[1] R. L. Rivest, L. Adleman, and M. L. Dertouzos, "On data banks and privacy homomorphisms," *Foundations of secure computation*, vol. 4, no. 11, pp. 169–180, 1978.

[2] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing*, STOC '09, (New York, NY, USA), pp. 169–178, ACM, 2009.

[3] M. Van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, "Fully homomorphic encryption over the integers," in *Advances in cryptology–EUROCRYPT 2010*, pp. 24–43, Springer, 2010.

[4] C. Gentry, S. Halevi, and N. Smart, "Fully homomorphic encryption with polylog overhead," in *Advances in Cryptology EUROCRYPT 2012* (D. Pointcheval and T. Johansson, eds.), vol. 7237 of *Lecture Notes in Computer Science*, pp. 465–482, Springer Berlin Heidelberg, 2012.

[5] M. Liang, "Symmetric quantum fully homomorphic encryption with perfect security," *Quantum Information Processing*, vol. 12, no. 12, pp. 3675–3687, 2013.

[6] M. Liang, "Quantum fully homomorphic encryption scheme based on universal quantum circuit," *Quantum Information Processing*, pp. 1–11, 2015.

[7] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, "Quantum computing on encrypted data," *Nat. Commun.*, vol. 5, 01 2014.

[8] A. M. Childs, "Secure assisted quantum computation," *Quantum Info. Comput.*, vol. 5, pp. 456–466, Sept. 2005.

[9] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, "Quantum walks with encrypted data," *Phys. Rev. Lett.*, vol. 109, p. 150501, Oct 2012.

[10] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen, and J. F. Fitzsimons, "A quantum approach to fully homomorphic encryption," *arXiv prnote arXiv:1411.5254*, 2014.

[11] A. Broadbent and S. Jeffery, "Quantum homomorphic encryption for circuits of low T-gate complexity," *arXiv prnote arXiv:1412.8766*, 2014.

[12] Y. Dulek, C. Schaffner, and F. Speelman, "Quantum homomorphic encryption for polynomial-sized circuits," 2016. arXiv:1603.09717v1.

[13] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on*, pp. 517–526, Oct 2009.

[14] L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Limitations on information-theoretically-secure quantum homomorphic encryption," *Phys. Rev. A*, vol. 90, p. 050303, Nov 2014.

[15] D. Gottesman and I. L. Chuang, "Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations," *Nature*, vol. 402, pp. 390–393, 1999.

[16] X. Zhou, D. W. Leung, and I. L. Chuang, "Methodology for quantum logic gate construction," *Phys. Rev. A*, vol. 62, p. 052316, Oct 2000.

[17] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge University Press, second ed., 2000.

[18] Y. Ouyang, S.-H. Tan, and J. Fitzsimons, "Quantum homomorphic encryption from quantum codes," *arXiv preprint arXiv:1508.00938*, 2015.