Quantum homomorphic encryption for circuits of low T-gate complexity

Abstract for QCRYPT 2015 contributed talk*

Anne Broadbent and Stacey Jeffery

A fully homomorphic encryption scheme is an encryption scheme with the property that any computation on the plaintext can be performed by a party having access to the ciphertext only. Here, we formally define and give schemes for *quantum* homomorphic encryption, which is the encryption of *quantum* information such that *quantum* computations can be performed given the ciphertext only. Our schemes allow for arbitrary Clifford group gates, but become inefficient for circuits with large complexity, measured in terms of the non-Clifford portion of the circuit (we use the "$\pi/8$" non-Clifford group gate, also known as the T-gate).

More specifically, two schemes are proposed: the first scheme has a decryption procedure whose complexity scales with the square of the *number* of T-gates (compared with a trivial scheme in which the complexity scales with the total number of gates); the second scheme uses a quantum evaluation key of length given by a polynomial of degree exponential in the circuit's T-gate depth, yielding a homomorphic scheme for quantum circuits with constant T-depth. Both schemes build on a classical fully homomorphic encryption scheme.

A further contribution of ours is to formally define the security of encryption schemes for quantum messages: we define *quantum indistinguishability under chosen plaintext attacks* in both the public- and private-key settings. In this context, we show the equivalence of several definitions.

Our schemes are the first of their kind that are secure under modern cryptographic definitions, and can be seen as a quantum analogue of classical results establishing homomorphic encryption for circuits with a limited number of *multiplication* gates. Historically, such results appeared as precursors to the breakthrough result establishing classical fully homomorphic encryption.

I. INTRODUCTION

An encryption scheme is *homomorphic* over some set of circuits $\mathscr{S}$ if any circuit in $\mathscr{S}$ can be evaluated on an encrypted input. That is, given an encryption of the message m, it is possible to produce a ciphertext that decrypts to the output of the circuit C on input m, for any $\mathsf{C} \in \mathscr{S}$. In *fully homomorphic encryption (FHE)*, $\mathscr{S}$ is the set of all classical circuits. FHE was introduced in 1978 by Rivest, Adleman and Dertouzos [25], but the existence of such a scheme was an open problem for over 30 years. Some early public-key encryption schemes were homomorphic over the set of circuits consisting of only additions [19, 23] or over the set of circuits consisting of only multiplications [15]. Several steps were made towards FHE, with schemes that were homomorphic over increasingly large circuit classes, such as circuits containing additions and a single multiplication [6], or of logarithmic depth [27], until finally in 2009, Gentry established a breakthrough result by giving the first fully homomorphic encryption scheme [17]. Follow-up work showed that FHE could be simplified [12], and based on standard assumptions, such as *learning with errors* [7]. The advent of FHE has unleashed a series of far-reaching consequences, such as delegating computations in a cloud architecture, and functional encryption [18].

A number of works have studied the secure delegation of quantum computation [1, 9–11, 16, 30] None directly address the question of quantum homomorphic encryption, since they are interactive schemes, and the work of the client is proportional to the size of the circuit being evaluated (and thus, they do not satisfy the *compactness* requirement of FHE, even if we allow interaction). Non-interactive approaches are given by [4], [26] and [29]. However, [4] and [26] are applicable to very restricted function families. Furthermore, in the case of [4], security is given only in terms of cheat sensitivity, while both [26] and [29] only bound the leakage of their encoding schemes and thus do not provide security according to standard cryptographic definitions.

Recent work [31] examines the question of perfect security and correctness for quantum fully homomorphic encryption (QFHE), concluding that the trivial scheme is optimal in this context. In light of this result, it is natural to consider computational assumptions in achieving QFHE. Indeed, the question of computationally secure QFHE remains an open problem. Such a scheme must satisfy three properties: 1) it must be

---

* Full version available at `arXiv:1412.8766`

computationally secure under some suitable security definition; 2) it must be compact — the complexity of decryption should be independent of the complexity of the evaluated circuit; and 3) it must be homomorphic for all quantum circuits. Our contribution makes progress towards this goal from two directions: we present the first computationally secure scheme that is compact and homomorphic for a large class of quantum circuits, satisfying (1) and (2) and making progress towards (3); and the first computationally secure scheme that is "quasi-compact" (the complexity of decryption depends on the number of T-gates in the evaluated circuit) and homomorphic for all quantum circuits in a standard universal gate set, satisfying (1) and (3) and making progress towards (2).

A. Summary of Contributions and Techniques

We introduce schemes for *quantum homomorphic encryption (QHE)*, the quantum version of classical homomorphic encryption; we are thus interested in establishing functionality for the evaluation of *quantum* circuits on encrypted *quantum* data. In terms of definitions, we contribute by giving the first definition of quantum homomorphic encryption in the computational security setting, in the case of both public-key and symmetric-key cryptosystems. As a consequence, we give the first formal definition (and scheme) for the public-key encryption of quantum information, where security is given in terms of *quantum indistinguishability under chosen plaintext attacks*—for which we show the equivalence of a number of definitions, including security for multiple messages.

In terms of QHE schemes, we start by using straightforward techniques to construct a scheme that is homomorphic for Clifford circuits. This can be seen as an analogue to a classical scheme that is homomorphic for linear circuits (circuits performing only additions). While Clifford circuits are not universal for quantum computation, this already yields a range of applications for quantum information processing, including encoding and decoding into stabilizer codes. Our quantum public-key encryption scheme is a hybrid of a classical public-key fully homomorphic encryption scheme and the quantum one-time pad [2]. Intuitively, the scheme works by encrypting the quantum register with a quantum one-time pad, and then encrypting the one-time pad encryption keys with a classical public-key FHE scheme. Since Clifford circuits conjugate Pauli operators to Pauli operators, any Clifford circuit can be directly applied to the encrypted quantum register; the homomorphic property of the classical encryption scheme is used to update the encryption key. Of course, we specify that the classical FHE scheme should be secure against quantum adversaries. By using, *e.g.*, the scheme from [7], we get security based on the *learning with errors* (LWE) assumption [24]; this has been equated with worst-case hardness of "short vector problems" on arbitrary lattices [22], which is widely believed to be a quantum-safe (or "post-quantum") assumption.

For universal quantum computations, we must be able to evaluate a non-Clifford gate, for which we choose the "T" gate (also known as "R" or "$\pi/8$" gate). Applying the above principle we run into trouble, since $\mathsf{T}\mathsf{X}^a\mathsf{Z}^b = \mathsf{X}^a\mathsf{Z}^{a\oplus b}\mathsf{P}^a\mathsf{T}$. That is, conditioned on the quantum one-time pad encryption key $a, b \in \{0, 1\}$, the output picks up an undesirable non-Pauli error. Our main contribution is to present two schemes, EPR and AUX, that deal with this situation in two different ways:

EPR: The main idea of EPR is to use entangled quantum registers to enable corrections *within the circuit* at the time of decryption. This scheme is homomorphic (and efficient) for any quantum circuit, however, it fails to meet a requirement for fully homomorphic encryption called *compactness*, which requires that the complexity of the decryption procedure be independent of the evaluated circuit. More specifically, the complexity of the decryption procedure for EPR scales with the square of the number of T-gates. This gives an advantage over the trivial scheme whenever the number of T-gates in the evaluated circuit is less than the squareroot of the number of gates. (The *trivial* scheme consists of appending to the ciphertext a description of the circuit to be evaluated, and specifying that it should be applied as part of the decryption procedure.)

AUX: Compared to EPR, the scheme AUX takes a more proactive approach to performing the correction required for a T-gate: to do this, it uses a number of auxiliary qubits that are given as part of the evaluation key. Intuitively, these auxiliary qubits encode the required corrections. In order to ensure universality, a large number of possible corrections must be available — the length of the evaluation key is thus given by a polynomial of degree exponential in the circuit's T-gate *depth*, yielding a homomorphic scheme that is efficient for quantum circuits with constant T-depth.

The two main schemes are incomparable. The scheme EPR becomes less *compact* (and therefore less interesting, since it approaches the trivial scheme), as the *number* of T-gates increases, while the scheme AUX becomes inefficient (*extremely* rapidly) as the *depth* of T-gates increases.

Our results can be viewed as a quantum analogue of precursory results to classical FHE, which established schemes with the homomorphic property for circuits with a limited number of multiplications. One difference is that, while these schemes started with the *very* modest goal of just a *single* multiplication (the addition operation being "easy"), we have already allowed for at the very least a *constant* number, and, depending on the circuit, up to a polynomial number of "hard" operations, namely of T-gates.

Our schemes use the existence of classical FHE, although at the expense of a slightly more complicated exposition, a classical scheme that is homomorphic only for linear circuits would suffice. We see the relationship between our schemes and classical FHE as a strength of our result, via the following interpretation: classical FHE is sufficient to enable QHE for a large family of circuits, and perhaps by taking greater advantage of the *fully* homomorphic property of the classical scheme in some as yet unknown way, our ideas might be extended to larger classes of quantum circuits.

An additional contribution of ours is conceptual: in the context of quantum circuits, it had been known for some time now that the non-Clifford part of a quantum computation is the "difficult" one (this phenomena appears, *e.g.* in the context of quantum simulations [20], fault-tolerant quantum computation [8] and quantum secure function evaluation [5, 13, 14]). This has motivated a series of theoretical work seeking to optimize quantum circuits in terms of their T-gate complexity [21, 28]. In particular, Ref. [3] recently proposed T-depth as a cost function, the idea being to count the number of T-layers in a quantum circuit and optimize over this parameter. Our contribution adds to this understanding, showing that, in the context of quantum homomorphic encryption, the main challenge is to evaluate non-Clifford gates.

[1] D. Aharonov, M. Ben-Or, and E. Eban. Interactive proofs for quantum computations. In *Proc. ICS '10*, pages 453–469, 2010.

[2] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Proc. FOCS '00*, pages 547–553, 2000.

[3] M. Amy, D. Maslov, M. Mosca, and M. Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, 32(6):818–830, June 2013.

[4] P. Arrighi and L. Salvail. Blind quantum computation. *Int. J. Quantum Inf.*, 4:883–898, 2006.

[5] M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *Proc. FOCS '06*, pages 249–260, 2006.

[6] D. Boneh, E.-J. Goh, and K. Nissim. Evaluating 2-DNF formulas on ciphertexts. In *Proc. TCC '05*, pages 325–341, 2005.

[7] Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *Proc. FOCS '11*, pages 97–106, 2011.

[8] S. Bravyi and A. Kitaev. Universal quantum computation with ideal Clifford gates and noisy ancillas. *Phys. Rev. A*, 71:022316, 2005.

[9] A. Broadbent, J. Fitzsimons, and E. Kashefi. Universal blind quantum computation. In *Proc. FOCS '09*, pages 517–526, 2009.

[10] A. Broadbent, G. Gutoski, and D. Stebila. Quantum one-time programs. In *Proc. CRYPTO '13*, pages 344–360, 2013.

[11] A. Childs. Secure assisted quantum computation. *Quantum Inf. Comput.*, 5:456–466, 2005.

[12] M. Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan. Fully homomorphic encryption over the integers. In *Proc. EUROCRYPT '10*, pages 24–43, 2010.

[13] F. Dupuis, J. B. Nielsen, and L. Salvail. Secure two-party quantum evaluation of unitaries against specious adversaries. In *Proc. CRYPTO '10*, pages 685–706, 2010.

[14] F. Dupuis, J. B. Nielsen, and L. Salvail. Actively secure two-party evaluation of any quantum operation. In *Proc. CRYPTO '12*, pages 794–811, 2012.

[15] T. Elgamal. A public key cryptosystem and a signature scheme based on discrete logarithms. In *Proc. CRYPTO '85*, pages 10–18, 1985.

[16] 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.*, 5, 2014.

[17] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proc. STOC '09*, pages 169–178, 2009.

[18] S. Goldwasser, Y. Kalai, R. A. Popa, V. Vaikuntanathan, and N. Zeldovich. Reusable garbled circuits and succinct functional encryption. In *Proc. STOC '13*, pages 555–564, 2013.

[19] S. Goldwasser and S. Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*, 28(2):270 – 299, 1984.
[20] D. Gottesman. The Heisenberg representation of quantum computers. In *Proc. ICGTMP '98*, pages 32–43, 1998.
[21] V. Kliuchnikov, D. Maslov, and M. Mosca. Asymptotically optimal approximation of single qubit unitaries by clifford and T circuits using a constant number of ancillary qubits. *Phys. Rev. Lett.*, 110:190502, May 2013.
[22] D. Micciancio and O. Regev. Lattice-based cryptography. In *Post-Quantum Cryptography*, pages 147–191. Springer, 2009.
[23] P. Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Proc. EUROCRYPT '99*, pages 223–238, 1999.
[24] O. Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6):34:1–34:40, September 2009.
[25] R. Rivest, L. Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. In *Foundations of Secure Computation*, pages 169–177. 1978.
[26] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist. Quantum walks with encrypted data. *Phys. Rev. Lett.*, 109:150501, Oct 2012.
[27] T. Sander, A. Young, and M. Yung. Non-interactive cryptocomputing for NC^1. In *Proc. FOCS '99*, pages 554–566, 1999.
[28] P. Selinger. Quantum circuits of T-depth one. *Phys. Rev. A*, 87:042302, Apr 2013.
[29] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L.Chen, and J. F. Fitzsimons. A quantum approach to fully homomorphic encryption. `arXiv:1411.5254`, 2014.
[30] D. Vedran, J. F. Fitzsimons, C. Portmann, and R. Renner. Composable security of delegated quantum computation. `arXiv:1301.3662`, 2013.
[31] L. Yu, C. A. Perez-Delgado, and J. F. Fitzsimons. Limitations on information theoretically secure quantum homomorphic encryption. `arXiv:1406.2456`, 2014.