On quantum homomorphic encryption with passive third party (extended abstract)

Li Yu[1,2,*] and Carlos A. Pérez-Delgado[1]

[1] *Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682*

[2] *National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo, Japan*

(Dated: November 27, 2014)

Quantum homomorphic encryption is a form of encryption in which two parties named Alice and Bob have the input data and program, respectively, and Bob computes the program on the encrypted input data and returns the result to Alice, without knowing Alice's input data. We have recently shown that any quantum homomorphic encryption with perfect data privacy cannot keep the program private at all, and that deterministic fully homomorphic encryption necessarily incurs exponential overhead if perfect security is required. The latter conclusion has been shown to hold in the case that the programs are implemented approximately by some other unitary operations. But in the results above it was assumed that any shared entangled state on the two parties is a pure state. In this paper we prove that in any exact deterministic quantum homomorphic encryption scheme with a passive third party which only distributes initial entanglement, if the data is perfectly private, then the effective program cannot be private at all. But for Alice to learn all information about Bob's program in one-shot, her allowed input data states are restricted to be of some special type, possibly entangled with ancillas. This conclusion implies that quantum homomorphic encryption cannot be secure even with the help of shared keys, including classical public keys. The case of inexact implementation of the programs is also discussed.

In classical cryptography, homomorphic encryption is a form of encryption to allow another party to do computation on the encrypted data without knowing the original data (this requirement is called data-privacy). Generally we have another requirement called "program privacy" which requires that the party who has the initial data (Alice) is not able to learn the algorithm used in the computation by the second party (Bob), except what can be learnt from the output for one particular input. Homomorphic encryption itself is a feature of an information processing protocol, i.e. it is a set of algorithms or routines used in some protocols. The context in which homomorphic encryption is usually used is computation tasks with one round of classical communication.

There have been schemes [1–4] of classical homomorphic encryption that work for any security

*Electronic address: liyu@nii.ac.jp

parameter but not information-theoretically secure, and with overhead polynomial in the security parameter and the size of the circuit to be evaluated. An exactly correct and information-theoretically secure scheme (with bounded overhead) has not been found. It is still an active research problem of searching for information theoretically secure homomorphic encryption systems which support arbitrary algebraic operations or are fully homomorphic, see [5] for a survey and [6] for a recent paper on the latter topic. Assuming the world is quantum, we note that the results in [7, 8] could be viewed as at least partially solving the problem for classical homomorphic encryption in some indirect way.

The concept of quantum homomorphic encryption has appeared in the literature [9]. It was left open whether there is a quantum homomorphic encryption scheme that allows universal quantum computation and still keep both data privacy and program privacy, but it was shown in [9] that such a scheme does not exist under a specific encryption method known as the quantum one-time-pad. Some other works in the literature include [10] and [11]. Note that they are interactive protocols, but the non-interactive cases as special cases of their protocols should be subject to our analysis here. In [12], it is proven that (i) quantum homomorphic encryption with perfect data privacy cannot keep the program private at all, and (ii) that deterministic fully homomorphic encryption necessarily incurs exponential overhead if perfect security is required, where "fully" refers to the unitary program to be performed being arbitrary. It can be shown that the statement (ii) still holds with passive third parties that only distributes tripartite entanglement initially but do not interact with other systems later. But generalizations to statement (i) does not follow immediately. In this paper we show that there is no perfect scheme in the case that there is a passive third party, and in fact we show a stronger result: if the scheme is correct in its computation results, and perfectly secure in data privacy, i.e. Bob is not able to learn any information about the input data, then Alice must be able to learn all information about Bob's program, or an equivalent program, using one run of the protocol, albeit with special choices of input states which may be entangled with ancillas.

The Theorem 1 below is our main result. A generalized quantum homomorphic encryption scheme is similar to that in [12], but allowing initially mixed entangled states shared by Alice and Bob. This is equivalent to introducing a passive third party.

Theorem 1 *In a (generalized) quantum homomorphic encryption scheme with perfect data privacy, a cheating Alice is able to learn all information about Bob's program or an equivalent program, by choosing a suitable input state, which may be an entangled state on the input system and ancillas.*

Note that we assume the input data state could be any state in a finite-dimensional complex Hilbert space, i.e. it is not limited to a subset of such space.

Note that Corollary 1 in [12] holds in the case of mixed entangled resource state, if we regard all systems except Bob's as belonging to Alice. As a result of Corollary 1(3) in [12] extended to the case of mixed entangled resource state, we have

Corollary 2 *In a (generalized) quantum homomorphic encryption scheme with perfect data privacy, with the permissible set of unitary operations denoted S, if S is a set that is ϵ-approximately universal on n qubits, that is every element of $\mathrm{SU}(2^n)$ can be approximated to an accuracy of ϵ, then the required amount of classical or quantum communication grows proportional to $\left(2^{2n}-1\right)\log_2\left(1/\epsilon\right)$.*

This means the communication cost (for Bob's message to Alice) is roughly exponential in the number of input qubits.

Conclusions. We have shown that in perfect information-theoretically secure quantum homomorphic encryption with a passive third party which only distributes initial entanglement, if the data is perfectly private, then the program cannot be private at all. But for Alice to perfectly learn about the program in one-shot, the input state she could use is restricted in general. The allowed classes of quantum circuits are arbitrary sets of unitary operators, and we require that the possible input states take up an entire finite-dimensional complex Hilbert space. Since shared public classical key is a special case of the initial tripartite entanglement, our conclusion implies that quantum homomorphic encryption cannot be perfectly secure in both the data and the program, even with classical public keys. We also discussed the approximate implementation of the circuits. The results in this paper could have further implications for other cases, such as when data privacy is partially broken. Further topics of study include schemes with partial data privacy, and interactive homomorphic schemes, i.e. those allowing multiple rounds of communication, and practical limits to security under realistic experimental conditions.

---

[1] Craig Gentry. Fully homomorphic encryption using ideal lattices. *Proceedings of the 41st annual ACM Symposium on Theory of Computing (STOC)*, pages 169–178, 2009.

[2] Marten van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. *In* Advances in Cryptology—EUROCRYPT 2010*, Lecture Notes in Computer Science*, 6110:24–43, 2010.

[3] Nigel P Smart and Frederik Vercauteren. Fully homomorphic encryption with relatively small key and ciphertext sizes. In *Public Key Cryptography–PKC 2010*, pages 420–443. Springer, 2010.

[4] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. In *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*, pages 97–106. IEEE, 2011.

[5] Caroline Fontaine and Fabien Galand. A survey of homomorphic encryption for nonspecialists. *EURASIP Journal on Information Security*, 2007, 2007.

[6] Michal Hojsik and Veronika Pulpanova. A fully homomorphic cryptosystem with approximate perfect secrecy. In Ed Dawson, editor, *Topics in Cryptology CT-RSA 2013*, volume 7779 of *Lecture Notes in Computer Science*, pages 375–388. Springer Berlin Heidelberg, 2013.

[7] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56:1154–1162, Aug 1997.

[8] Harry Buhrman, Matthias Christandl, and Christian Schaffner. Complete insecurity of quantum protocols for classical two-party computation. *Phys. Rev. Lett.*, 109:160501, Oct 2012.

[9] Min Liang. Symmetric quantum fully homomorphic encryption with perfect security. *Quantum Inf. Process.*, 12:3675–3687, 2013.

[10] Andrew Childs. Secure assisted quantum computation. *Quantum Information and Computation*, 5(6):456, 2005.

[11] K. 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.*, 5:3074, 2014.

[12] Li Yu, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. Limitations on information-theoretically-secure quantum homomorphic encryption. *Phys. Rev. A*, 90:050303, Nov 2014.