Quantum homomorphic encryption for polynomial-sized circuits
(extended abstract of arXiv:1603.09717 for QCRYPT 2016)

Yfke Dulek[1,3], Christian Schaffner[1,2,3], and Florian Speelman[2,3]

[1] University of Amsterdam
[2] CWI, Amsterdam
[3] QuSoft

We present a new scheme for quantum homomorphic encryption which is compact and allows for efficient evaluation of arbitrary polynomial-sized quantum circuits. Building on the framework of Broadbent and Jeffery [BJ15] and recent results in the area of instantaneous non-local quantum computation [Spe15], we show how to construct quantum gadgets that allow perfect correction of the errors which occur during the homomorphic evaluation of T gates on encrypted quantum data. Our scheme can be based on any classical (leveled) fully homomorphic encryption (FHE) scheme and requires no computational assumptions besides those already used by the classical scheme. The size of our quantum gadget depends on the space complexity of the classical decryption function – which aligns well with the current efforts to minimize the complexity of the decryption function.

Motivation

Rivest, Adleman and Dertouzous were the first to observe the possibility of manipulating encrypted data in a meaningful way, rather than just storing and retrieving it [RAD78]. Early classical homomorphic encryption schemes were limited in the sense that they could not facilitate arbitrary operations on the encrypted data: some early schemes only implemented a single operation (addition or multiplication)[RSA78,GM84,Pai99]; later on it became possible to combine several operations in a limited way [BGN05,GHV10,SYY99]. A breakthrough happened in 2009 when Gentry presented a fully homomorphic encryption (FHE) scheme [Gen09]. In subsequent work [VDGHV10,BGV12,BV11], FHE schemes have been simplified and based on more standard computational assumptions such as the hardness of learning with errors (LWE), which is believed to be hard also for quantum attackers. The exciting developments around FHE have sparked a large amount of research in other areas such as functional encryption [GKP+13b,GVW13,GKP+13a,SW14] and obfuscation [GGH+13].

Developing quantum computers is a formidable technical challenge, so it currently seems likely that quantum computing will not immediately be available for everyone and hence quantum computations have to be outsourced. Given the importance of classical FHE for "computing in the cloud", it is natural to wonder about the existence of encryption schemes which can encrypt *quantum data* in such a way that a server can carry out arbitrary *quantum computations* on the encrypted data (without interacting with the encrypting party[4]).

A recent result by Ouyang, Tan and Fitzsimons provides information-theoretic security for circuits with at most a constant number of non-Clifford operations [OTF15]. However, Yu, Pérez-Delgado and Fitzsimons [YPDF14] showed that information-theoretically secure quantum fully homomorphic encryption (QFHE) is not possible unless the size of the encryption grows exponentially in the input size. Computational assumptions could allow bypassing this impossibility result.

A natural idea is to encrypt a message qubit with the quantum one-time pad (i.e. by applying a random Pauli operation), and send the classical keys for the quantum one-time pad along as classical information, encrypted using a classical FHE scheme. Any computational assumptions on the classical scheme are also required for the quantum scheme. Broadbent and Jeffery, who were the first to thoroughly investigate QFHE schemes based on computational assumptions [BJ15], call this basic scheme CL. It is easy to see that CL allows an evaluator to compute arbitrary Clifford operations on encrypted qubits, simply by performing the actual Clifford circuit, followed by homomorphically updating the quantum one-time pad keys according to the commutation rules between the performed Clifford gates and the Pauli encryptions. The CL scheme can be regarded as analogous to additively homomorphic encryption schemes in the classical setting. The challenge, like multiplication in the classical case, is to perform non-Clifford gates such as the T gate. After a T gate is performed on a one-time-pad encrypted qubit

[4] In contrast to *blind* or *delegated quantum computation* where some interaction between client and server is usually required.

$\mathsf{X}^a\mathsf{Z}^b|\psi\rangle$, the result might contain an unwanted (non-Pauli) phase P^a depending on the key a with which the qubit $|\psi\rangle$ was encrypted, since $\mathsf{T}\mathsf{X}^a\mathsf{Z}^b = \mathsf{P}^a\mathsf{X}^a\mathsf{Z}^b\mathsf{T}$. Obviously, the evaluator is not allowed to know the key a, so he cannot easily resolve the error.

Broadbent and Jeffery propose two different approaches for extending CL, accomplishing homomorphic encryption for circuits with a limited number of T gates. In one of their schemes, called AUX, the evaluator is supplied with auxiliary quantum states, stored in the evaluation key. These auxiliary states allow him to evaluate T gates and immediately remove any error P^a that may have occurred. Unfortunately, the required auxiliary states grow doubly exponentially in size with respect to the T depth of the circuit, rendering AUX useful only for circuits with constant T depth.

Main result

Our work is concerned with answering the following question:

Is it possible to construct a computationally secure quantum homomorphic encryption scheme that allows evaluation of polynomial-sized quantum circuits?

We answer it in the affirmative by presenting a new scheme TP (as abbreviation for teleportation) for quantum homomorphic encryption which is both compact and efficient for circuits with polynomially many T gates. The scheme is secure against chosen plaintext attacks from quantum adversaries, as formalized by the security notion *q-IND-CPA security* [BJ15].

Our scheme TP is related to AUX in that it extends the Clifford scheme CL by providing extra resources in the evaluation key for removing errors, which we call *gadgets*. In sharp contrast to AUX, the size of the evaluation key in TP only grows linearly in the number of T gates in the circuit (and polynomially in the security parameter), allowing the scheme to be leveled fully homomorphic.

In TP, we require exactly one evaluation gadget for every T gate that we would like to evaluate homomorphically. After applying a T gate, the evaluator can teleport the resulting qubit $\mathsf{P}^a\mathsf{X}^a\mathsf{Z}^b\mathsf{T}|\psi\rangle$ "through the gadget" [GC99] in a way that depends on a classical FHE encryption of a, in order to remove the unwanted phase. The quantum part of the gadget is consumed in the process. On a high level, the use of an evaluation gadget corresponds to an *instantaneous non-local quantum computation*[5] of the classical decryption function, where one party holds the secret key of the classical FHE scheme, and the other party holds the input qubit and a classical encryption of the key to the quantum one-time pad. Together, this information determines whether an inverse phase gate $\mathsf{P}^\dagger$ needs to be performed on the qubit or not.

If the classical decryption function has a circuit in $\mathbf{NC}^1$, then we can show explicitly how to construct a gadget for correcting T gate errors. By Barrington's Theorem [Bar89], there exists a width-5 permutation branching program (PBP) of polynomial length that computes the decryption function. A width-5 PBP is a list of instructions, each of which queries a single bit of the input, and selects a permutation on the set $\{1, 2, 3, 4, 5\}$ based on the bit value. The program is executed by concatenating the selected permutations: the execution results in the identity permutation if the function evaluates to 0, and in a fixed 5-cycle otherwise. Since only a single input bit is queried per instruction, all permutations that depend on bits of the secret key can be prepared in advance by the creator of the gadget. They are prepared as groups of five intertwined EPR pairs: if a set of five qubits is teleported through such a group, they will be permuted according to the corresponding program instruction. The evaluator can 'fill in the gaps' by connecting the groups of EPR pairs (through Bell measurements) according to the program instructions that depend on bits of the encryption of a. The qubit $\mathsf{P}^a\mathsf{X}^a\mathsf{Z}^b\mathsf{T}|\psi\rangle$, when teleported through the resulting state starting at the first position, remains at the first position if $a = 0$, and is permuted to a different position if $a = 1$. Applying the correction $\mathsf{P}^\dagger$ to all but the first position ensures that the phase error is corrected if and only if $a = 1$. As a technicality, an entire reverse copy of the permutation branching program is performed afterwards, to ensure that the qubit ends up at a known position.

The structure of the gadget can be hidden from the evaluator using an additional quantum one-time pad on the entire state. Even without knowledge of the structure (i.e. how the pairs are intertwined), the evaluator can perform Bell measurements according to the PBP instructions. Because of the Bell measurements and quantum one-time pad, the keys a and b need to be updated after the gadget use.

[5] This term is not related to the term 'instantaneous quantum computation', and instead first was used for a specific form of non-local quantum computation, one where all parties have to act simultaneously.

Some encrypted classical information is provided with the gadget that allows the evaluator perform these updates.

Recent results by Speelman [Spe15] show that there exist protocols to construct and use these gadgets for an even wider class of classical decryption functions, namely those with polynomial *garden-hose complexity* [BFSS13]. In particular, if the decryption function is log-space computable, then the number of EPR pairs in the gadget is polynomial in the security parameter. This relation turns out to be very convenient, as classical FHE schemes are often optimized with respect to the complexity of the decryption operation (in order to make them bootstrappable). As a concrete example, if we instantiate our scheme with the classical FHE scheme by Brakerski and Vaikuntanathan [BV11], each evaluation gadget of our scheme consists of a number of qubits which is polynomial in the security parameter. Since the evaluation of the other gates causes no errors on the quantum state, no gadgets are needed for those; any circuit containing polynomially many T gates can be efficiently evaluated in TP.

We prove computational security of TP by reducing it to CL in several steps, replacing one gadget with a completely mixed quantum state at every step. The encrypted classical information that accompanies the gadget is simultaneously replaced with an encryption of a string of zeros. Leveraging the q-IND-CPA security of the classical scheme, we show that these replacements cannot significantly influence the winning probability for any polynomial-time adversary in a quantum CPA indistinguishability experiment. After all gadgets have been replaced with completely mixed states, the scheme is equivalent to the Clifford scheme CL, which has already been proven q-IND-CPA secure [BJ15].

Properties and applications of our scheme

The quantum part of our evaluation gadget is strikingly simple, which provides a number of advantages.

To start with, the evaluation of a T gate requires only one gadget, and does not cause any errors to accumulate on the quantum state. The scheme is very compact in the sense that the state of the system after the evaluation of a T gate has the same form as after the initial encryption, except for any classical changes caused by the classical FHE evaluation. This kind of compactness also implies that individual evaluation gadgets can be supplied "on demand" by the holder of the secret key. Once an evaluator runs out of gadgets, the secret key holder can simply supply more of them.

Furthermore, TP does not depend on a specific classical FHE scheme, hence any advances in classical FHE can directly improve our scheme. Our requirements for the classical FHE scheme are quite modest: we only require the classical scheme to have a space-efficient decryption procedure and to be secure against quantum adversaries. In particular, no circular-security assumption is required. Since we supply at most a polynomial number of evaluation gadgets, our scheme TP is leveled homomorphic by construction, and we can simply switch to a new classical key after every evaluation gadget. In fact, the Clifford gates in the quantum evaluation circuit only require additive operations from the classical homomorphic scheme, while each T gate needs a fixed (polynomial) number of multiplications. Hence, we do not actually require fully homomorphic classical encryption, but leveled fully homomorphic schemes suffice.

Finally, circuit privacy in the passive setting almost comes for free. When wanting to hide which circuit was evaluated on the data, the evaluating party can add an extra randomization layer to the output state by applying his own one-time pad. We show that if the classical FHE scheme has the circuit-privacy property, then this extra randomization completely hides the circuit from the decrypting party. This is not unique to our specific scheme: the same is true for CL.

In terms of applications, our construction can be appreciated as a round-optimal scheme for *blind delegated quantum computation*, using computational assumptions. With only a single round of communication, the server can evaluate a universal quantum circuit on the encrypted input, consisting of the client's quantum input and a (classical) description of the client's circuit. In this context, it is desirable to minimize the number and complexity of quantum operations that the client needs to perform. In our scheme, the encryption and decryption only requires the client to apply Pauli operations. We show that even the creation of the evaluation gadgets can be performed (with the help of the server) using only swap and Pauli operations, at the expense of an extra communication round.

As another application, we can instantiate our construction with a classical FHE scheme that allows for *distributed* key generation and decryption amongst different parties that all hold a share of the secret key [AJLA+12]. In that case, we expect that our construction can be adapted to perform *multi-party quantum computation* [BCG+06] in the semi-honest case. We also consider it likely that our new techniques will be useful in other contexts such as quantum indistinguishability obfuscation [AF16].

References

AF16. Gorjan Alagic and Bill Fefferman. On quantum obfuscation. *arXiv preprint arXiv:1602.01771*, 2016.

AJLA+12. Gilad Asharov, Abhishek Jain, Adriana López-Alt, Eran Tromer, Vinod Vaikuntanathan, and Daniel Wichs. Multiparty computation with low communication, computation and interaction via threshold FHE. In *Advances in Cryptology–EUROCRYPT 2012*, pages 483–501. Springer, 2012.

Bar89. David A. Barrington. Bounded-width polynomial-size branching programs recognize exactly those languages in NC1. *Journal of Computer and System Sciences*, 164:150–164, 1989.

BCG+06. Michael Ben-Or, Claude Crépeau, Daniel Gottesman, Avinatan Hassidim, and Adam Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006), 21-24 October 2006, Berkeley, California, USA, Proceedings*, pages 249–260. IEEE Computer Society, 2006.

BFSS13. Harry Buhrman, Serge Fehr, Christian Schaffner, and Florian Speelman. The garden-hose model. In *Proceedings of the 4th Conference on Innovations in Theoretical Computer Science*, ITCS '13, pages 145–158, New York, NY, USA, 2013. ACM.

BGN05. Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-DNF formulas on ciphertexts. In *Theory of cryptography*, pages 325–341. Springer, 2005.

BGV12. Zvika Brakerski, Craig Gentry, and Vinod Vaikuntanathan. (Leveled) fully homomorphic encryption without bootstrapping. In *Proceedings of the 3rd Innovations in Theoretical Computer Science Conference*, pages 309–325. ACM, 2012.

BJ15. Anne Broadbent and Stacey Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. In *Advances in Cryptology–CRYPTO 2015*, pages 609–629. Springer, 2015.

BV11. 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, Oct 2011.

GC99. Daniel Gottesman and Isaac L. Chuang. Quantum Teleportation is a Universal Computational Primitive. *Nature*, 402:390–393, August 1999.

Gen09. Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC*, volume 9, pages 169–178, 2009.

GGH+13. Shelly Garg, Craig Gentry, Shai Halevi, Mariana Raykova, Anant Sahai, and Brent Waters. Candidate indistinguishability obfuscation and functional encryption for all circuits. In *Foundations of Computer Science (FOCS), 2013 IEEE 54th Annual Symposium on*, pages 40–49. IEEE, 2013.

GHV10. Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. A simple bgn-type cryptosystem from lwe. In *Advances in Cryptology–EUROCRYPT 2010*, pages 506–522. Springer, 2010.

GKP+13a. Shafi Goldwasser, Yael Kalai, Raluca Ada Popa, Vinod Vaikuntanathan, and Nickolai Zeldovich. Reusable garbled circuits and succinct functional encryption. In *Proceedings of the 45th annual ACM symposium on Symposium on theory of computing*, STOC '13, pages 555–564, New York, NY, USA, 2013. ACM.

GKP+13b. Shafi Goldwasser, Yael Tauman Kalai, Raluca Ada Popa, Vinod Vaikuntanathan, and Nickolai Zeldovich. How to run turing machines on encrypted data. In *Advances in Cryptology–CRYPTO 2013*, pages 536–553. Springer, 2013.

GM84. Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *Journal of computer and system sciences*, 28(2):270–299, 1984.

GVW13. Sergey Gorbunov, Vinod Vaikuntanathan, and Hoeteck Wee. Attribute-based encryption for circuits. In *Proceedings of the Forty-fifth Annual ACM Symposium on Theory of Computing*, STOC '13, pages 545–554, New York, NY, USA, 2013. ACM.

OTF15. Yingkai Ouyang, Si-Hui Tan, and Joseph Fitzsimons. Quantum homomorphic encryption from quantum codes. *arXiv preprint arXiv:1508.00938*, 2015.

Pai99. Pascal Paillier. Public-key cryptosystems based on composite degree residuosity classes. In *Advances in cryptology – EUROCRYPT99*, pages 223–238. Springer, 1999.

RAD78. Ronald L Rivest, Len Adleman, and Michael L Dertouzos. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978.

RSA78. Ronald L Rivest, Adi Shamir, and Len Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.

Spe15. Florian Speelman. Instantaneous non-local computation of low T-depth quantum circuits. *arXiv preprint arXiv:1511.02839*, 2015.

SW14. Amit Sahai and Brent Waters. How to use indistinguishability obfuscation: Deniable encryption, and more. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing*, STOC '14, pages 475–484, New York, NY, USA, 2014. ACM.

SYY99. Tomas Sander, Adam Young, and Moti Yung. Non-interactive cryptocomputing for NC1. In *Foundations of Computer Science, 1999. 40th Annual Symposium on*, pages 554–566. IEEE, 1999.

VDGHV10. Marten Van Dijk, Craig Gentry, Shai Halevi, and Vinod Vaikuntanathan. Fully homomorphic encryption over the integers. In *Advances in cryptology–EUROCRYPT 2010*, pages 24–43. Springer, 2010.

YPDF14. 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.