Report on
Quantum homomorphic encryption for circuits of low T-gate complexity[1]

Mollimard Victor

01/03/2017

Introduction

New problems of privacy, security and anonymity appear in the delegation of computation in cloud computing. One way to solve some of these problems is to use homomorphic encryption: someone can compute on messages with access to only the ciphers of those messages. Historically, before having a full homomorphic scheme (i.e. every polynomials on messages can be computed), there were intermediary results with limitation on the polynomials that could be computed.

The results found in this paper are of a similar sort to those intermediary results except but in the quantum case: the paper presents the construction of three homomorphic schemes secure under modern cryptography definitions and in the idea equivalent to schemes limiting the number of multiplication gates in the classical setting. The three constructions are based on basic quantum building blocks for quantum homomorphic encryption and classical fully homomorphic encryption schemes.

1 Classical fully homomorphic encryption scheme

First, the constructions are based on a fully homomorphic encryption (FHE) scheme as introduced in [2] and constructed recently in [3] by using the following definitions taken from [4].

Definition 1. A homomorphic encryption scheme is a four-tuple of PPT algorithms $(HE.KeyGen, HE.Enc, HE.Eval, HE.Dec)$ such that:

$HE.KeyGen(\lambda)$: with λ a security parameter, returns three keys: the public key pk, the secret key sk and the evaluation key ek.

$HE.Enc(pk, m)$: with m a single bit message and pk the public key, outputs a cipher text c.

$HE.Dec(sk, c)$: with c a cipher and sk the secret key, returns a single bit message $m*$.

$HE.Eval(ek, f, c_1, \dots, c_l)$: with ek the evaluation key, $f; \{0,1\}^l \to \{0,1\}$ a circuit (a polynomial of l variables) and l ciphers $c_1, \dots, c_l$, outputs a cipher c_f.

Definition 2.($\mathscr{S}$-homomorphic) Consider a class of circuits $\mathscr{S}$ decomposed in sub-classes $\mathscr{S}_n$ of circuits of same size n. A scheme HE is $\mathscr{S}$-homomorphic (or homomorphic for the class $\mathscr{S}$) if for any sequences of circuits $(f_n \in \mathscr{S}_n)_{n\in\mathbb{N}}$ and respective inputs $(m_1, \dots, m_l)$ (l can depend on n) there is a negligible function η such that:

$$P_r[Dec(sk, Eval(ek, f_n, Enc(m_1), \dots Enc(m_l))) \neq f_n(m_1, \dots, m_l)] \leq \eta(n)$$

where (pk, sk, ek) are honestly generated keys with security parameter n.

The idea is for $Eval$ to effectively compute f_n on the messages with just their ciphers except in a negligible number of cases.

Definition 3.(Compactness) A homomorphic scheme HE is compact if there is a polynomial p such that the complexity of decrypting the output of $Eval$ is at most $p(n)$, n being the security parameter.

Definition 4.(Full homomorphic encryption) A scheme is fully homomorphic if it is compact and homomorphic for the class of all arithmetic circuit over $\mathbb{F}_2$.

A definition of quantum security can also be given:

Definition 5.(q-IND-CPA) A scheme HE is q-IND-CPA secure if for any quantum polynomial-time adversary $\mathcal{A}$ such that :

$$|P_r[\mathcal{A}(pk, ek, Enc(pk, 0)) = 1] - P_r[\mathcal{A}(pk, ek, Enc(pk, 1)) = 1]| \leq \eta(n)$$

where $\eta()$ is a negligible function, n a security parameter and (pk, sk, ek) honestly generated keys (with security parameter n).

2 Basic quantum building blocks and notations for quantum homomorphic encryption

The other building blocks necessary to construct the three scheme of the paper are quantum circuits and the quantum one-time pad. To introduce these, we will use a set of notation.

2.1 Notations

If a is a message, its encryption is denoted $\tilde{a}$. Register are quantum system storing information, they are denoted by calligraphic typeset like $\mathcal{X}, \mathcal{Y}$. The contents of a register is the set of positive semi-definite operators called density operators on $\mathcal{X}$. The set of density operators on $\mathcal{X}$ is $D(\mathcal{X})$.

If $\rho \in D(\mathcal{X} \otimes \mathcal{Y})$ (it is a state of the joint system), $Tr_{\mathcal{Y}}(\rho)$ is denoted by $\rho^{\mathcal{X}}$. $\mathcal{X}, \mathcal{Y}$ having same dimension is denoted by $\mathcal{X} \equiv \mathcal{Y}$.

The trace distance between two states ρ_1 and ρ_2 is $\Delta(\rho_1, \rho_2) = Tr\left(\sqrt{(\rho_1 - \rho_2)^\dagger(\rho_1 - \rho_2)}\right)$. For a random variable X, we note $\rho(X)$ its density matrix. A classical quantum state is of the form $\rho^{\mathcal{MA}} = \sum_x P_r[X = x] \left|x\right\rangle \left\langle x\right|^{\mathcal{M}} \otimes \rho_x^{\mathcal{A}}$.

A quantum channel $\Phi : D(\mathcal{A}) \to D(\mathcal{B})$ is a possible (physically realizable) mapping from register $\mathcal{A}$ to register $\mathcal{B}$. To simplify notation, we will write $\Phi(\rho^{\mathcal{AE}})$ and not $(\Phi \otimes I)(\rho^{\mathcal{AE}})$. We will use a conditional quantum channel: with input the classical-quantum state $\sum_x P_r[X = x] \left|x\right\rangle \left\langle x\right|^{\mathcal{M}} \otimes \rho_x^{\mathcal{A}}$ and for quantum channels $\Phi_x : D(\mathcal{A}) \to D(\mathcal{B})$, outputs:

$$Tr_M\left(\sum_x P_r[X = x] \left|x\right\rangle \left\langle x\right|^{\mathcal{M}} \otimes \Phi_x(\rho_x^{\mathcal{A}})\right)$$

Finally, a quantum measurement consists in a measurement in the computational basis except if otherwise specified. A quantum algorithm is a polynomial-time uniform family of quantum circuits implementing a family of quantum channels.

2.2 Quantum circuits

We consider the following gates corresponding to "easy" operations in the homomorphic characteristic of the future schemes:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},\ H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

The set of circuits generated by these gates is the Clifford group. Moreover, for the following, it is useful to remember that X and Z are Pauli gate.

We also consider the gate $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\frac{\pi}{4}} \end{bmatrix}$ corresponding to the "difficult" operation.

A layered quantum circuit consists of alternating layers each composed uniquely by either Clifford gates or T gates. The T-depth as defined in [5] is then the number of layers of T-gates.

2.3 Quantum one-time pad

The quantum one-time pad is define (in the way of [6]) for a single-qubit system ρ in register $\mathcal{R}$ and $a,\ b \in \{0,1\}$ secrets and consists in two functions namely the encryption and decryption:

$$QEnc_{a,b} = \begin{cases} \mathcal{R} \to \mathcal{R} \\ \rho \to X^a Z^b \rho Z^b X^a \end{cases} \quad \text{and} \quad QDec_{a,b} = \begin{cases} \mathcal{R} \to \mathcal{R} \\ \rho \to X^a Z^b \rho Z^b X^a \end{cases}$$

It is easy to see $QDec_{a,b} \circ DEnc_{a,b}$ is the identity. By choosing a, b at random someone having access to only $QEnc_{a,b}(\rho)$ cannot find ρ: indeed, for all ρ, $\frac{1}{4} \sum\limits_{a,b} X^a Z^b \rho Z^b X^a = \frac{\mathbb{I}_2}{2}$.

3 Definitions and properties of a quantum homomorphic encryption

Before building a quantum homomorphic encryption, the formal definitions and properties of such a scheme must be given. The definitions concerns the security, compactness, correctness and indivisibility or weaker versions of these properties. Two cases are also differentiate: the public-key case and the symmetric-key case.

3.1 Public-key setting

First, here is the definition of a quantum homomorphic encryption (QHE):
Definition 6. it is a four-tuple of quantum algorithms $(QHE.KeyGen, QHE.Enc, QHE.Eval, QHE.Dec)$ such that:

> $QHE.KeyGen(1^\lambda)$ with λ a security parameter, outputs three keys (pk, sk, ρ_{evk}): pk a classical public key, sk a classical secret key and $\rho_{evk} \in D(\mathcal{R}_{evk})$ a quantum evaluation key.
>
> $QHE.Enc_{pk}$ with pk the public key, is a function that maps a state of the message register $\mathcal{M}$ i.e. a message to a state of the cipher register $\mathcal{C}$ i.e. a cipher.
>
> $QHE.Eval^C$ with C a circuit defining a channel $\Phi_C : D(\mathcal{M}^{\otimes n}) \to D(\mathcal{M}^{\otimes m})$ is a function: $D(\mathcal{R}_{evk} \otimes \mathcal{C}^{\otimes n}) \to D(\mathcal{C}^{\otimes m})$. It consumes the evaluation key in the computation.
>
> $QHE.Dec_{sk}$ with sk the secret key, returns a state of the message register for a state of the cipher register given in input.

The following definition gives the q-IND-CPA security for QHE. First, consider the two following experiments: $\Xi^{cpa,0}_{QHE}$ consists in measuring the register $\mathcal{M}$ then encrypting $|0\rangle\langle 0|$, the results being in $\mathcal{C}$; $\Xi^{cpa,1}_{QHE}$ consists in encrypting the state of $\mathcal{M}$, the results being in $\mathcal{C}$.
The CPA indistinguishability experiment is now given with a adversary $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$. $\mathcal{A}_1$ uses a quantum channel from $D(\mathcal{R}_{evk})$ to $D(\mathcal{M} \otimes \mathcal{E})$ with access to pk where $\mathcal{E}$ is an arbitrary environment. $\mathcal{A}_2$ maps $D(\mathcal{C} \otimes \mathcal{E})$ to one bit.
The experiment $PubK^{cpa}_{\mathcal{A},QHE}(\kappa)$ is then given by the picture from the original paper[1]:

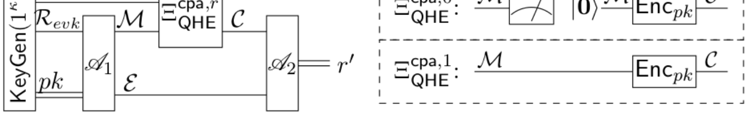

Figure 1: The quantum CPA indistinguishability experiment.

It consists in five steps:

1. Generate honestly (pk, sk, ρ_{evk}) from a security parameter κ.
2. $\mathcal{A}_1$ is then called and outputs in $\mathcal{M} \otimes \mathcal{E}$.
3. A random $r \in \{0,1\}$ is chosen and $\Xi_{QHE}^{cpa,r}$ is applied.
4. $\mathcal{A}_2$ is then called and outputs a bit r'
5. $\mathcal{A}$ wins if $r = r'$, in this case the result of the experiment is 1, otherwise it is 0.

Definition 7. A QHE is q-IND-CPA if for any quantum polynomial-time adversary $\mathcal{A}$, there is a negligible function η such that: $P_r[PubK_{\mathcal{A},QHE}^{cpa}(\kappa) = 1] \leq \frac{1}{2} + \eta(\kappa)$.

Another way to define security is to use the same type of experiment but where the adversary chooses two t-tuples of messages and the challenger returns the encryption of one the tuple. The adversary wins if it can find which tuple it is. A QHE is said q-IND-CPA-mult if there is no quantum polynomial-time algorithm that has a chance of winning being more than $\frac{1}{2} + \eta(\kappa)$ where η is a negligible function and κ the security parameter.

This two definitions of security are in fact equivalent, it is proven in the original paper[1] in appendix B.

The two following definitions gives the correctness and compactness properties for a class of circuits $\mathscr{S}$.

Definition 8.($\mathscr{S}$-homomorphic) Let $\mathscr{S} = \{\mathscr{S}_\kappa\}_{\kappa \in \mathbb{N}}$ be a class of quantum circuit. A QHE is $\mathscr{S}$-homomorphic if for any sequence of circuits $\{C_\kappa \in \mathscr{S}_\kappa\}_\kappa$ with induced channel $\Phi_{C_\kappa} : D(\mathcal{M}^{\otimes n(\kappa)}) \rightarrow D(\mathcal{M}^{\otimes m(\kappa)})$ and any input $\rho \in D(\mathcal{M}^{\otimes n(\kappa)} \otimes \mathcal{E})$, then the following trace distance is negligible:

$$\Delta \left(QHE.Dec_{sk}^{\otimes m(\kappa)} \left[QHE.Eval^{C_\kappa} \left(\rho_{evk}, QHE.Enc_{pk}^{\otimes n(\kappa)}(\rho) \right) \right], \Phi_{C_\kappa}(\rho) \right)$$

One way to understand this definition is that there is no difference between applying a circuit in $\mathscr{S}$ to messages in clear or to their ciphers (with $QHE.Eval$). However, it is not exactly correctness as there is no property for decrypting cipher of one message except if $\mathscr{S}$ contains the identity circuit. Just one use of $QHE.Eval$ is possible, the key ρ_{evk} being consumed in the operation.

In the same way, compactness can be defined for a class of circuits:

Definition 9. ($\mathscr{S}$-compactness) Let $\mathscr{S} = \{\mathscr{S}_\kappa\}_{\kappa \in \mathbb{N}}$ be a class of quantum circuits. A QHE is $\mathscr{S}$-compact if there is a polynomial p such that: for any sequence of circuits $\{C_\kappa \in \mathscr{S}_\kappa\}_\kappa$, the circuit complexity of applying $QHE.Dec$ to the output of $QHE.Eval^{C_\kappa}$ is at most $p(\kappa)$ (it is independent of C_κ).

If a QHE is $\mathscr{S}$-compact over some universal class, it is said compact.

One particularity of quantum space is that bit-by-bit work is not everything: entanglement prevents it (a system must in this case be considered in its totality). The definition must then consider this case. The definition of compactness is also adapted and a weaker version is proposed.

Definition 10. An indivisible QHE scheme is a QHE with $QHE.Eval$ and $QHE.Dec$ re-defined as:

> $QHE.Eval^C$ with C a quantum circuit: is a function $D(\mathcal{R}_{evk} \otimes \mathcal{C}^{\otimes n}) \rightarrow D(\mathcal{R}_{aux} \otimes \mathcal{C}'^{\otimes m})$. $\mathcal{R}_{aux}$ is a new register that can be entangled with $\mathcal{C}'$, decryption can then only be done globally.
>
> $QHE.Dec_{sk}$ with sk secret key: is a function $D(\mathcal{R}_{aux} \otimes \mathcal{C}'^{\otimes m}) \rightarrow D(\mathcal{M}^{\otimes m})$: it transform a cipher in a message with the help of $\mathcal{R}_{aux}$.

Definition 11. ($\mathscr{S}$-compactness for indivisible scheme) Let $\mathscr{S} = \{\mathscr{S}_\kappa\}_{\kappa \in \mathbb{N}}$ be a class of circuits. An indivisible QHE is $\mathscr{S}$-compact if there is a polynomial p such that for any sequence of circuits $\{C_\kappa \in \mathscr{S}_\kappa\}_\kappa$ with channel $\Phi_{C_\kappa} : \mathcal{M}^{\otimes n(\kappa)} \rightarrow \mathcal{M}^{\otimes m(\kappa)}$, the circuit complexity of applying $QHE.Dec^{\otimes m(\kappa)}$

to the output of $QHE.Eval^{C_\kappa}$ is at most $p(\kappa, m(\kappa))$ (it is independent of the complexity of C_κ).

Definition 12. (quasi-compactness) Let $\mathscr{S} = \{\mathscr{S}_\kappa\}_{\kappa\in\mathbb{N}}$ be the class of circuits over some universal gate set. Let $f : \mathscr{S} \to \mathbb{R}_{\geq 0}$ be some function. An indivisible QHE is f-quasi-compact if there is a polynomial p such that for any sequence of circuits $\{C_\kappa \in \mathscr{S}_\kappa\}_\kappa$ with channel $\Phi_{C_\kappa} : \mathcal{M}^{\otimes n(\kappa)} \to \mathcal{M}^{\otimes m(\kappa)}$, the circuit complexity of applying $QHE.Dec^{\otimes m(\kappa)}$ to the output of $QHE.Eval^{C_\kappa}$ is at most $f(C_\kappa)p(\kappa, m(\kappa))$.

That is to say the decoding can depend on some characteristic of the evaluated circuits (like the size of the difficult part in term of computation (for the future constructions, it is the T-gates)).

3.2 Symmetric-key setting

The definitions can also be given a symmetric-key setting. Here, only the definition of a quantum homomorphic encryption and one refinement of this definition will be given. The other definitions concerning security, correctness and compactness can also be adapted but the ideas are the same. The adapted definition can be found in the original paper[1].

Definition 13. A symmetric-key QHE is a QHE with $QHE.KeyGen$ and $QHE.Enc$ redefined as:

$QHE.KeyGen(1^\kappa)$ with κ a security parameter outputs a couple (sk, ρ_{evk}) with sk a classical secret encryption/decryption key and $\rho_{evk} \in D(\mathcal{R}_{evk})$ a quantum evaluation key.

$QHE.Enc_{sk}$ is still a function that given the register $\mathcal{M}$ returns a cipher in register $\mathcal{C}$ but now depends on sk (and not pk).

A refinement of this definition is to limit the number of encryption possible for a given key: it is a bounded symmetric-key QHE.

Definition 14. It is a symmetric-key QHE with $QHE.KeyGen$, $QHE.Enc$ and $QHE.Dec$ redefined as:

$QHE.KeyGen(1^\kappa, 1^n)$ returns the pair (sk, ρ_{evk}) (it now depends of one more parameter n).

$QHE.Enc_{sk,d}$ follows the same idea as previously but increase d at each call. If $d > n$, it outputs $\perp$ indicating an error.

$QHE.Dec_{sk,d}$ The decryption follows the same idea as previously but depends now of d.

4 Clifford scheme

The paper now explain how to create a QHE q-IND-CPA, compact and $\mathscr{S}$-homomorphic for the Clifford group from one classical FHE that is q-IND-CPA.

It is in fact a QHE for stabilizer circuits i.e. Clifford group, single-qubit preparation (like $|0\rangle$) and measurement. Here, the construction of the scheme will be given, and main arguments of proofs will be exposed but not the formal proofs given in the original paper[1]. This new scheme is called CL. It needs a FHE that will be call HE.

CL is based on one idea exposed in [7] consisting in: for all Clifford circuit C and all Pauli Q, there exists a Pauli Q' such that $QC = CQ'$; and on the one-time pad: applying a random Pauli operator is a perfectly secure symmetric-key quantum encryption scheme. So it is possible to applied a Clifford circuit to a cipher of the one-time pad.

A Clifford circuit C can then be applied to an encrypt data $Q|\psi\rangle$ to obtain $Q'(C|\psi\rangle)$. Decrypting consists then in removing Q' a Pauli operator i.e. applying one more time Q'. The problem is then to find Q'.

But if Q is known, $Q = X^{a_1}Z^{b_1} \otimes \cdots \otimes X^{a_n}Z^{b_n}$, then Q' can be described by $(a'_1, b'_1, \ldots, a'_n, b'_n)$ depending only on C and $(a_1, b_1, \ldots, a_n, b_n)$. This dependence can be given by a function $f^C : \mathbb{F}_2^n \to \mathbb{F}_2^n$ called here a key update rule. This function can be decomposed to the key update rule of each gate in the set X,Z,H,P,CNOT. Each of these fundamental key update rules is known and described in appendix C of the original paper[1]. The knowledge of just C and Q is thus sufficient to decode (it is sufficient to create the update key rule for C, Q then gives the input and the output is Q').

The idea for CL is then to code the data with the one-time pad and to use HE to code $(a_1, b_1, \dots, a_n, b_n)$. However, in this idea the decryption depends on the size of the circuit when the key update rule is created i.e. the compactness property is not respected. The challenge is to allow the execution of any Clifford circuit while keeping the compactness.

To do so, an hybrid of the quantum one-time pad and of a classical FHE is used and solves the challenge by performing key updates on encrypted quantum one-time pad in a way allowing to keep the compactness condition for any Clifford circuit. More precisely, to evaluate a Clifford circuit C consisting in a sequence of gates $c_1, \dots, c_G$, the gates are applied to the encrypted one-time pad and $f^{c_1} \circ \dots \circ f^{c_G}$ is homomorphically evaluated on the encrypted keys $a_1, b_1, \dots, a_n, b_n$ by keeping track of the functions for each bit of the quantum one-time pad key, $\{f_{a,i}, f_{b,i}\}_{i=1}^n$. Or each of the fundamental key update rules is linear thus each $f_{a,i}$ and $f_{b,i}$ are linear polynomials over $\mathbb{F}_2[a_1, b_1, \dots a_n, b_n]$ and are called key polynomials.

At the beginning of the evaluation, $f_{a,i} = a_i$ and $f_{b,i} = b_i$. They can be updated with the key updates rules corresponding to c_j the currently evaluated gate. To compute the new encrypted one-time pad keys once the circuit is complete, one homomorphically evaluate each key polynomials on the old encrypted one-time pad keys.

CL can now be defined with $\mathcal{M} = \mathbb{C}^{0,1}$, cipher being a quantum state in $\mathbb{C}^{0,1}$ and a classical string ($\mathcal{C} = \mathbb{C}^{C \times C} \otimes \mathcal{X}$ and $\mathcal{C}' = \mathbb{C}^{C' \times C'} \otimes \mathcal{X}$ where C is the output space of $HE.Enc$, C' is the output space of $HE.Eval$ and $\mathcal{X}$ is):

$CL.KeyGen(1^\kappa)$. For a key generation, use $HE.KeyGen(1^\kappa)$ to obtain (pk, sk, evk). Create ρ_{evk} as the classical state $\rho(evk)$.

$CL.Enc_{pk} : D(\mathcal{M}) \to D(\mathcal{C})$ defined as:

$$CL.Enc_{pk}(\rho^{\mathcal{M}}) = \sum_{a,b \in \{0,1\}} \frac{1}{4} \rho \left(HE.Enc_{pk}(a), HE.Enc_{pk}(b)\right) \otimes QEnc_{a,b}(\rho^{\mathcal{M}})$$

where $QEnc_{a,b}$ is the encryption function of quantum one-time pad.

$CL.Eval^C : D(\mathcal{R}_{evk} \otimes \mathcal{C}^{\otimes n}) \to D(\mathcal{C}'^{\otimes m})$. Suppose C is composed by $c_1, \dots, c_G$ and is a Clifford circuit. For each time a gate c_j initializes a fresh qubit, a new $CL.Enc_{pk}(|0\rangle \langle 0|)$ is append to the system. Call $\rho \in D(\mathcal{X}_1 \otimes \dots \otimes \mathcal{X}_m)$ the composite system consisting of the input quantum system and the initialized qubits.

1. for all $i \in [n]$, initialize $f_{a,i}$ and $f_{b,i}$ as a_i and b_i.
2. for $j = 1 \dots G$ such that c_j is a gate or a measurement:
   (a) Apply gate c_j to the state i.e. $\rho \leftarrow c_j \rho c_j^{-1}$.
   (b) Update $f_{a,i}, f_{b,i}$ as explained previously if c_j is applied to the wire i (if it is a CNOT, update for the two wire concerned).
3. update the classical encryption with $c_i = (HE.Eval_{evk}^{f_{a,i}}(\tilde{a}_i), HE.Eval_{evk}^{f_{b,i}}(\tilde{b}_i))$.
4. output $(c_1, \dots, c_m, \rho)$

$CL.Dec_{sk} : D(\mathcal{C}') \to D(\mathcal{M})$. For $\tilde{a}, \tilde{b} \in C'$, decryption is given by the conditional quantum channel:

$$CL.Dec_{sk} : |\tilde{a}\rangle \langle \tilde{a}| \otimes |\tilde{b}\rangle \langle \tilde{b}| \otimes \rho^{\mathcal{X}} \to QDec_{HE.Dec_{sk}(\tilde{a}), HE.Dec_{sk}(\tilde{b})}(\rho^{\mathcal{X}})$$

which can be done by decrypting first the classical register to obtain $a = HE.Dec_{sk}(\tilde{a})$ and $b = HE.Dec_{sk}(\tilde{b})$, applying $QDec_{a,b}$ then tracing out $\mathbb{C}^{C' \times C'}$.

CL is $\mathscr{S}$-homomorphic for the Clifford group, compact and q-IND-CPA (if HE is q-IND-CPA).

The main argument for being $\mathscr{S}$-homomorphic is that HE is homomorphic and the key update rule were construct with keeping this homomorphic characteristic. The decrypted values of ciphers are then correct giving then the property.

The argument behind the compactness is that the decryption of one qubit of the output of $CL.Eval$ is the decryption of two bits (a and b) and two operations (applying X^a and Z^b). Or the decryption of a and b by $HE.Dec$ is in polynomial-time in the security parameter by compactness of HE.

The idea behind the security is a two parts proof: having the cipher of a and b give a negligible advantage and without the two ciphers, the quantum CPA indistinguishability experiment is independent of r for the perspective of the adversary (assuring there is no advantage in the decryption). The first part is assure by the security of HE: there is no difference for the adversary if (a, b) or $(0, 0)$ is used.

5 Quantum homomorphic schemes with T-gates

CL can now be used as a stepping stone to construct scheme that can deal with difficult computational part: the T-gates. Two schemes will be presented hereafter their formal definitions and the proofs of their properties are in the section 6&7 of the original paper[1].

5.1 EPR: T-gate computation with entanglement

The idea is exactly the same as for CL with the addition that T-gates generate a problem: $TX^aZ^b = X^aZ^{a\oplus b}P^aT$. An undesirable P error is picked in the process. From [8], this error can be correct by applying ZP. Security holds if the evaluation algorithm does not know if the correction is applied or not. This can be done with a gadget (derived from a method of [9] and [10]).

Here, the idea is to delay the correction by exploiting entanglement for the evaluation of T-gate on encrypted data. However, using this method key update cannot be done in similar way as previously for T-gate: as the value of the corresponding register is unknown, the key update is view as a symbolic computation with an extra variable added.

For the first T-gate evaluation ($t = 1$), the evaluation does not have the knowledge to evaluate $f_1 = f_{a,i}$ (i is the wire upon which the gate is performed) in order to perform the correction. It is possible to compute a classical cipher $\tilde{f_1}$ that decrypts as $f_1(a_1, b_1, \ldots, a_n, b_n)$. For a T-gate, the output part of the auxiliary system contain both $\tilde{f_1}$ and $\mathcal{R}_1$. As a part of the decryption, compute f_1 as the $HE.Dec(\tilde{f_1})$ and apply P^{f_1} to $\mathcal{R}_1$ to obtain k_1 by measuring in the Hadamard basis. For the procedure, k_1 is unknown (it is an unknown part of the encryption key). The $Eval$ algorithm continues for values of t up to R (the number of T-gates) each time adding one unknown variable.

Each T-gate adds to the complexity of the decryption procedure, since for each T-gate, a possible P-correction and a measurement on an auxiliary qubit must be performed. In addition, the key-polynomials and the f_t cannot be evaluated until the variables k_t have been measured, thus the evaluation takes place in the decryption phase, increasing the dependence on R to $O(R^2)$.

Now, some properties can be given for this scheme called EPR which is q-IND-CPA (if HE is q-IND-CPA), $\mathscr{S}$-homomorphic for the class of all quantum circuits and R^2-quasi-compact. The idea to prove the security of this scheme is exactly the same as for CL. The $\mathscr{S}$-homomorphic characteristic comes from the homomorphic characteristic of HE and its conservation by the gadget used to compute the T-gates. The R^2-quasi-compactness comes from the decryption phase (R^2 is the only part that only depends on the circuit, there are other parts but they are mixing variables not depending on the circuit).

5.2 AUX: T-gate computing using auxiliary states

The problem is still the P correction that is introduced by computation of the T-gates but here a more pro-active approach is use to resolve it. The idea is to use auxiliary registers generated during the key generation and containing parts of the original encryption key. This is use to correct the P-error of a straightforward application of a T-gate on the cipher.

More precisely, this register contains hidden version of P corrections that are useful for the evaluation of the T-gate. In general, the exact auxiliary state is not in a register but obtains by combining some of them (it allows to not know in advance the key as they can be obtained by combination). However, this method is costly: it introduces new unknowns (in term of new variables as well as "cross-terms") that need to be corrected in any future T-gate. Thus, the size of the evaluation key grows as polynomial whose degree is exponential in T-depth. Only a constant T-depth can then be tolerated by this scheme.

This new scheme called AUX is a symmetric-key encryption because the auxiliary qubits depend on the one-time pad encryption keys. It is also bounded in the number of qubits that can be encrypted by n(in the same way as a classical one-time pad that picks a fixed-length encryption key ahead of time).

The idea behind the construction of the auxiliary registers is that auxiliary states can be combined allowing the construction of keys later without knowing their need at the beginning. But the number of auxiliary state grows super-exponential in the T-depth (forcing it to be constant to have a computable solution).

The proofs of the properties for AUX are technical in the sense that they are decomposed in intermediary results some being computations of boundaries (like the number of auxiliary state required). Nevertheless, the difficulties behind compactness and correctness is the exact number of auxiliary registers required and the degree of key-polynomials at a given layer.

Security is proven in two parts: firstly an adversary that interacts with $AUX.KeyGen$ cannot do much better than one that interacts with a alter version where every classical encryption is an encryption of 0. Then that using this alter version, an adversary cannot win with probability superior to $\frac{1}{2}$.

Reporting

First and foremost, a sum up of the contribution of this paper are the transposition of modern homomorphic encryption definitions to the quantum universe, a compact and secure homomorphic encryption scheme for the Clifford group, and homomorphic encryption schemes for Clifford group union T-gates circuits similar to classical homomorphic schemes with restriction for the multiplication (gates) that came before a full homomorphic encryption scheme.

The principal limitation of this work is the fact it has been done only for T-gates and not for other "difficult" gates. In the classical case this was not possible as there is only two fundamental gates + and ×. However in quantum theory, the addition gate is link to the Clifford group. In the same way, × should be link to a group of "difficult" gates and if one can see how this work could be adapted for other T-gates of the form $T = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{bmatrix}$ for $\theta \in \pi\mathbb{Q}$, it is far harder for a triangular matrix.

One research project proposed by the paper concerns circuit privacy i.e. can you adapt this scheme such that a user evaluating a circuit C on his inputs learn nothing more than the value of C on these inputs. The difficulty of such a project is clear in the fact that everything done here with update key use the knowledge of C. Another clear research project proposed by the paper is to make a full quantum homomorphic encryption scheme.

A research project not proposed by the article could be to increase the life expectancy of the evaluation key: allowing to use it for more than one evaluation.

References

[1] A. Broadbent and S. Jeffery. Quantum homomorphic encryption for circuits of low T-gate complexity. *Advances in Cryptology – CRYPTO 2015*

[2] R. Rivest, . Adleman, and M. Dertouzos. On data banks and privacy homomorphisms. In *Foundations of Secure Computation*, pages 169-177, 1978

[3] C. Gentry. Fully homomorphic encryption using ideal lattices. In *Proceedings of the 41st annual ACM symposium on Theory of Computing (STOC09)*, pages 169-178, 2009.

[4] BV11 Z. Brakerski and V. Vaikuntanathan. Efficient fully homomorphic encryption from (standard) LWE. In *Proceedings of the 52nd Annual IEEE Symposium on Foundation s of Computer Science (FOCS 2011)*, pages 97106, 2011. Full version available at Cryptology ePrint Archive, Report 2011/344.

[5] M. Amy, D. Maslov, M. Mosca, and M. Roetteler. A meet-in-the-middle algorithm for fast synthesis of depth-optimal quantum circuits. *Computer-Aided Design of Integrated Circuits and Systems, IEEE Transactions on*, 32(6):818830, June 2013.

[6] A. Ambainis, M. Mosca, A. Tapp, and R. De Wolf. Private quantum channels. In *Proceedings of the 41st Annual IEEE Symposium on Foundations of Computer Science (FOCS00)*, pages 547553, 2000.

[7] D. Gottesman. The Heisenberg representation of quantum computers. In *Group 22: Proceedings of the XXII International Colloquium on Group Theoretical Methods in Physics*, pages 3243, 1998.

[8] A. Childs. Secure assisted quantum computation. *Quantum Information and Computation*, 5:456466, 2005.

[9] 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. *Nature communications*, 5, 2014.

[10] A. Broadbent. Delegating private quantum computations.arXiv:1506.01328[quant-ph], to appear in *Canadian Journal of Physics*, 2015.