On Statistically-Secure Quantum Homomorphic Encryption

Ching-Yi Lai* and Kai-Min Chung

Institute of Information Science, Academia Sinica, Taipei 11529, Taiwan

Abstract. Homomorphic encryption (HE) is an encryption scheme that allows computations to be evaluated on encrypted inputs without knowledge of their raw messages. Recently the first quantum fully homomorphic encryption (FHE) was proposed by Dulek *et al.* with privacy inherited from classical FHE and thus is computationally secure. On the other hand, Ouyang *et al.* constructed a quantum HE scheme for Clifford circuits with information-theoretic security (IT-security). It is desired to see whether an information-theoretically-secure (IT-secure) quantum FHE exists. If not, what other nontrivial class of quantum circuits can be homomorphically evaluated with IT-security? We answer the first question in the negative. As for the second one, we propose an IT-secure quantum HE scheme that supports the homomorphic evaluation of a class of quantum circuits, called IQP^+, which is an enlarged class of the instantaneous quantum polynomial-time (IQP) circuits. Our HE scheme is based on a class of concatenated quantum stabilizer codes, whose logical X and Z operators act nontrivially on different sets of qubits.

Keywords: Homomorphic encryption, quantum cryptography, information-theoretic security, stabilizer codes, IQP circuits, postselection

1 Introduction

In this work, we investigate the possibility of statistically-secure (or information-theoretically-secure, and IT-secure for short) symmetric-key homomorphic encryptions in the quantum setting. Encryption schemes are typically considered as a computational primitive, since an IT-secure symmetric key encryption scheme can only securely encrypt messages of length at most the length of the secret key by Shannon's impossibility result [44]. However, when homomorphic operations can be done over encrypted data, even encrypting a bounded number of messages can be interesting. In the classical case, it is in fact possible to construct an IT-secure symmetric-key encryption with homomorphism over the XOR operation. Nonetheless, it is also not hard to show that IT-secure fully homomorphic encryptions do not exist (e.g., see [24] for a simple argument).

Quantum mechanics endows us with additional computing power to fulfill quantum cryptography primitives with functionalities beyond classical cryptography, such as the well-known BB84 quantum key distribution protocol [8], which

* e-mail: cylai0616@iis.sinica.edu.tw

is an IT-secure key distribution impossible for classical primitives. Recently this secure delegation of computation on encrypted data has been considered in quantum cryptography [17, 20, 24, 35, 36, 38, 40, 43, 49]. Quantum computation is possible if a *universal* set of quantum gates can be performed. That is, any unitary operator can be approximated to an arbitrary accuracy by a quantum circuit consisting of gates from the set according to the Solovay-Kitaev theorem [33, 39], provided the abilities of preparing simple ancilla states and performing basic single-qubit measurements. A homomorphic encryption scheme that supports quantum computation is called a *quantum* homomorphic encryption (QHE) scheme. Likewise, a QHE that supports the homomorphic evaluation of any quantum computation is called a quantum *fully* homomorphic encryption (QFHE). In order to achieve QFHE, an encrypted universal set of gates need to be implemented efficiently. Using quantum one-time pad [2], a quantum homomorphic encryption for a nontrivial class of *Clifford circuits* (defined in Sec. 2) was proposed in [17]. A Clifford circuit is composed of Hadamard (H), phase (P), and controlled-NOT (CNOT) gates. Homomorphic evaluation of a Clifford circuit can be performed directly on the encrypted states. In addition, the pads (classical bits) should be updated accordingly, which are done by classical FHE protocols (e.g., [9, 22, 29, 50]), assuming that their computational hardness assumptions remain true for quantum computation. It is known that the Clifford gates together with the $\pi/8$ gate (T) are universal for quantum computation. However, when a T gate is applied, the corresponding pads cannot be updated efficiently without violating the requirement of *compactness*, i.e., the complexity of decryption algorithm does not depend on the size of the delegated quantum circuit (see Definition 5). To achieve universality, a gadget for implementing a T gate was proposed in [24] and thus fulfills the first QFHE. Since a classical FHE scheme is required in the protocol, this QFHE scheme has computational security, inherited from the classical FHE scheme. Now given the power of quantum mechanics, an interesting question is:

Is there a QFHE scheme with information-theoretic security (IT-security)?

The possibility was first investigated by Ouyang *et al.* [40] and they showed that IT-secure quantum homomorphic encryption can be performed for Clifford circuits. Furthermore, their scheme can handle a small number of T gates, at the cost of exponential blow-up in the ciphertext size. On the other hand, there is a negative result for QFHE with perfect security [51], which still leaves open whether QFHE can be done with (imperfect) IT-security. More questions: Is there a QFHE that admits the evaluation of universal quantum computation? If not, what class of quantum computation can be supported? In particular, is QHE for classical computation possible? We show that the answers are both not:

Theorem 1. *There is no QFHE with IT-security. There is no QHE that is homomorphic for classical circuits with IT-security.*

The same result was also independently observed in [38]. We prove the impossibility of IT-secure QFHE by a reduction to the nonexistence of IT-secure

quantum private information retrieval (QPIR) protocol with one database [21]. Actually, it also rules out the existence of IT-secure HE for classical computation, even with quantum encryption. (See Sec. 3 for more details.) Evaluation of universal quantum computation on encrypted quantum states is not possible even with constant privacy error, unless the requirement of compactness is relaxed. The next question to ask is:

> Can we have IT-secure homomorphic evaluation for any nontrivial class of quantum circuits other than the Clifford circuits?

The answer is yes. The QHE scheme in [40] is based on quantum stabilizer codes, more precisely, the class of Calderbank-Shor-Steane (CSS) codes [19, 48]. Quantum stabilizer codes are used to protect quantum states against noise decoherence in the setting of fault-tolerant quantum computation (FTQC) [23] and they have also been used to achieve different notions of security in the literature (e.g., [5, 7, 15, 16, 47]). (See Sec. 4.1 for a brief introduction of stabilizer codes.) If a CSS code is built from a classical doubly-even dual-containing code [23] (e.g., the Steane code [48], quantum Reed-Muller codes, and quantum quadratic-residue codes [34]), the Clifford gates $\{H, P, \text{CNOT}\}$ can be *transversally* implemented, i.e., applying a physical gate bitwise on each qubit. Functionalities and security of the QHE scheme [40] follows directly from this transversality. Therefore, if we replace the CSS codes used in the QHE scheme in [40] by codes with a different transversal gate set, we obtain a QHE scheme that is homomorphic for a set of circuits different from the Clifford circuits. For example, the triorthogonal codes [10] have transversal CNOT, T, and control-control-phase gates. It is known that transversal gates alone cannot be universal for quantum error-correcting codes [25, 52]. As a consequence this method does not apply to homomorphic evaluation of universal quantum computation. More discussion about transversal computation can be found in [38], where they also proved that no additive quantum error-correcting code can have a transversal Toffoli gate.

We would like to search for other QHE schemes different from this type so that a nontrivial class of homomorphic quantum computation is possible. We show how to do it for the class of *instantaneous quantum polynomial-time* (IQP) circuits [45]. Roughly speaking, an IQP circuit is composed of gates that are diagonalized in the computational basis with input state $|+\rangle \otimes \cdots \otimes |+\rangle$ and its output is the measurement outcomes in the $\{|+\rangle, |-\rangle\}$ basis (see Definition 3). It can be seen that no quantum codes have transversal IQP circuits. In fact, we will propose a QHE scheme IQPP in Sec. 5 for IQP^+ circuits, which have additional CNOT, X, Y gates and measurements in the computational basis and allows arbitrary input quantum states in the xy-plain (see Definition 4). More precisely, the idea is that secret information is encrypted in the relative phase φ of a qubit $(|0\rangle + e^{i\varphi}|1\rangle)/\sqrt{2}$. Note that the Hadamard gate is not allowed in this scheme as we pointed out in the previous section that an IT-secure QFHE scheme does not exist.

Theorem 2. *(Informal) The scheme IQPP is an IT-secure QHE scheme for IQP^+ circuits.*

The notion of IQP computation with commuting quantum circuits was proposed in [45], which is not universal for quantum computation. It is known that the class of IQP with *postselection* is equivalent to the class PP [12]. (A postselected circuit is a quantum circuit with some specified measurement outcomes.) Moreover, IQP computations are difficult to be simulated by classical computers [12–14] unless the polynomial hierarchy collapses to the third level. Recently an important goal of experimental quantum physics is to demonstrate a successful quantum computation that cannot be achieved by a classical computer. However, this task becomes difficult as the number of qubits involved in a quantum system grows. For example, currently it is hard to implement Shor's factoring algorithm [46]. Instead, nonuniversal circuits, such as IQP, are physically more feasible so that quantum supremacy could be demonstrated [13, 26, 28, 42]. The IQP^+ circuits are a larger set than the IQP circuits and hence are also unlikely to be simulated by classical circuits. It would be interesting to see what additional power the class of IQP^+ circuits can provide. In contrast, a Clifford circuit with input states in the computational basis can be classically simulated according to the Gottesman-Knill theorem [31].

The security of our scheme IQPP is derived similarly to that in [40]. In [40], each qubit is first noisily encoded into a corrupted quantum codeword (see Subsec. 4.5) and then the qubits of the codeword are randomly permuted with several appended qubits in the maximally-mixed state (see Subsec. 4.6). When the permutation is hidden from the server, the encrypted qubit is secret. This is also a manner we have in IQPP. Now we want to find different logical gates that can be homomorphically evaluated while maintaining the privacy. Notice that in the setting of fault-tolerant quantum computation, several techniques are provided to achieve universal quantum computation. For the class of codes with transversal Clifford gates, a magic state gadget is used to implement a T gate [11], which requires the preparation of a magic ancillary state, a CNOT, a measurement, and possibly a correction operator conditioned on the measurement outcome. Another method is to choose two codes that allow two different transversal gate sets, whose union is universal. Then a code deformation can be performed between these two codes [4, 41]. For example, the Steane code can be deformed into a triorthogonal Reed-Muller code. Instead of code deformation, one can perform logical teleportation between any two codes [18]. We would like to apply these techniques from FTQC to perform the homomorphic evaluation of non-Clifford gates. Unfortunately, all the mentioned techniques require a logical measurement on the encrypted data and need to apply a correction operation conditioned on the logical measurement outcome. Since the server cannot learn the logical measurement outcome, these methods cannot be applied to our task. The feature of noninteraction between the client and server during evaluation is a strong constraint in QHE for that the client cannot interpret the measurement outcomes for the server.

Motivated by the implementation of T gate in [32], we observed that the implementation of a gate diagonal in the computational basis (call it a *diagonal gate*) can be done with only a subset of qubits involved (see Fig. 4). When a

quantum operator acts nontrivially on a subset of qubits, this subset is called the *support* of the quantum operator. If the support of a diagonal gate is known to the server, the diagonal gate can be implemented correctly. However, revealing these locations will induce an attack of logical Z measurement. For example, in Fig. 4, only three qubits are involved in the implementation, but these locations correspond to the support of logical Z of the Steane code (see Subsec. 4.2). Fortunately, the input qubits of IQP^+ circuits lie in the xy-plain so that this logical Z measurement is not harmful to the privacy. Another issue is that for some codes, the logical Z and X operators have the same support, such as the Steane code, so that a logical X attack exists simultaneously, precluding the encryption of any quantum information. We show that this can be avoid by constructing quantum codes whose logical X and Z operators have different supports. Finally our scheme IQPP is based on a code family constructed from the concatenation of the Steane code and a $[[6, 2]]$ code $\mathcal{Q}_6$ (see Subsec. 4.3). Details of functionalities of IQPP are provided in Sec. 5.

In a world that postselection is possible, the IQP circuits are universal, and so are the IQP^+ circuits. However, our QHE scheme IQPP is still not a QFHE with postselection since the compactness would be broken from the number of Hadamard gadgets (Fig. 2) required in the evaluation of a circuit. It would be interesting to find one IT-secure QFHE for postselected circuits or to prove its nonexistence.

This paper is organized as follows. Preliminaries are given in the next section, including basics of quantum information processing and definitions of IQP and IQP^+. In Sec. 3 we define QHE and its properties and then prove the impossibility of IT-secure QFHE. In Sec. 4 we detail each component of our QHE scheme IQPP. The complete scheme of IQPP is given in Sec. 5. We briefly discuss why the Hadamard gate is not available for IQPP in Appendix A.

2 Preliminaries

2.1 Quantum Information Processing

We give notation and briefly introduce basics of quantum mechanics here. Let $L(\mathcal{H})$ denote the space of linear operators on a complex Hilbert space $\mathcal{H}$. A quantum system is described by a *density operator* $\rho \in L(\mathcal{H})$ that is positive semidefinite and with trace one $\mathrm{tr}(\rho) = 1$. Let $D(\mathcal{H}) = \{\rho \in L(\mathcal{H}) : \rho \geq 0, \mathrm{tr}(\rho) = 1\}$ be the set of density operators on a $\mathcal{H}$. When $\rho \in D(\mathcal{H})$ is of rank one, it is called a *pure* quantum state and we can write $\rho = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathcal{H}$, where $\langle\psi| = |\psi\rangle^\dagger$ is the conjugate transpose of $|\psi\rangle$. If ρ is not pure, it is called a *mixed* state and can be expressed as a convex combination of pure quantum states. The distance between two quantum states ρ and σ is

$$\frac{1}{2}||\rho - \sigma||_{\mathrm{tr}},$$

where $||X||_{\mathrm{tr}} = \mathrm{tr}\left(\sqrt{X^\dagger X}\right)$ is the trace norm of an operator X.

Associated with an m-qubit quantum system is a complex Hilbert space $\mathbb{C}^{2^m}$ with a computational basis $\{|v\rangle : v \in \{0,1\}^m\}$. Let $\{|0\rangle, |1\rangle\}$ be an ordered basis for pure single-qubit states in $\mathbb{C}^2$. The Pauli matrices

$$\sigma_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ \sigma_1 = X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},\ \sigma_3 = Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix},\ \sigma_2 = Y = iXZ$$

form a basis of $L(\mathbb{C}^2)$. Then any single-qubit density operator $\rho \in D(\mathbb{C}^2)$ admits a Bloch sphere representation

$$\rho = \frac{I + r_1 X + r_2 Y + r_3 Z}{2} \triangleq \frac{I + \boldsymbol{r} \cdot \boldsymbol{\sigma}}{2}, \tag{1}$$

where $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ and $\boldsymbol{r} = (r_1, r_2, r_3) \in \mathbb{R}^3$ is called the Bloch vector of ρ such that $r_1^2 + r_2^2 + r_3^2 \leq 1$. If ρ is pure, we have $r_1^2 + r_2^2 + r_3^2 = 1$.

The evolution of a quantum state $\rho \in D(\mathcal{H})$ is described by a *quantum operation* $\mathcal{E} : D(\mathcal{H}) \to D(\mathcal{H}')$ for some Hilbert spaces $\mathcal{H}$ and $\mathcal{H}'$. In particular, if the evolution is a unitary U, we have the evolved state $\mathcal{E}(\rho) = U\rho U^\dagger$. A quantum operation of several single-qubit Pauli operators on n different qubits simultaneously can be realized as an n-fold Pauli operator. Denote the n-fold Pauli group by

$$\mathcal{G}_n = \{i^c E_1 \otimes \cdots \otimes E_n : c \in \{0,1,2,3\}, E_j \in \{I, X, Y, Z\}\}.$$

All elements in $\mathcal{G}_n$ are unitary with eigenvalues ± 1 and they either commute or anticommute with each other. An n-fold Pauli operator admits a binary representation that is irrelevant to its phase. For two binary n-tuples $u, v \in \{0,1\}^n$, define

$$Z^u X^v = \bigotimes_{j=1}^{n} Z^{u_j} X^{v_j}.$$

where $u = u_1 \cdots u_n$ and $v = v_1 \cdots v_n$. Thus any $g \in \mathcal{G}_n$ can be expressed as $g = i^c Z^u X^v$ for some $c \in \{0,1,2,3\}$ and $u, v \in \{0,1\}^n$.

The set of unitary operators in $L(\mathbb{C}^{2^n})$ that preserve the n-fold Pauli group $\mathcal{G}_n$ by conjugation is the *Clifford group*, which is generated by the Hadamard (H), phase (P) and controlled-NOT (CNOT) gates:

$$H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix},\ P = \begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix},$$
$$\text{CNOT} = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes X.$$

The gates H, P, and CNOT are called *Clifford gates*. It is known that circuits composed of only Clifford gates are not universal; the Clifford gates together with any gate outside the Clifford group will do. For example, a candidate is the $\pi/8$ gate

$$T = e^{i\pi/8} \begin{bmatrix} e^{-i\pi/8} & 0 \\ 0 & e^{i\pi/8} \end{bmatrix}.$$

These gates that involve only a few qubits are called elementary gates. Then a quantum circuit is composed of a sequence of elementary gates and possibly some quantum measurements. It is known that quantum measurements can be deferred to the end of a quantum circuit [39] and we will assume it is always the case in this paper. Also we consider only measurements in the Z basis $(|0\rangle, |1\rangle)$ and measurements in the X basis $(|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}})$. We denote by $C(\rho)$ the output of a quantum circuit C with input quantum state ρ by treating C as a quantum operation.

Finally we may use the notation X_j to denote the operator

$$X_j = I^{\otimes j-1} \otimes X \otimes I^{\otimes n-j},$$

where n is the total number of qubits of the underlying system and can be inferred from the context. Similarly for Z_j, H_j, T_j, and so on. Also the tensor product notation may be omitted sometimes. For example, we may write

$$X \otimes Y \otimes Z \otimes Z = XYZ^{\otimes 2} = X_1Y_2Z_3Z_4 = Z^{0111}X^{1100}.$$

In particular, we denote by C_iX_j, a CNOT gate with control qubit i and target qubit j; that is, X_j is applied to qubit j if qubit i is in the state $|1\rangle$.

2.2 Instantaneous Quantum Polynomial-time Computation

IQP circuits are proposed in [12, 45].

Definition 3. *An IQP circuit on N qubits is a quantum circuit consisting of quantum gates diagonal in the Z basis $(|0\rangle, |1\rangle)$. The input state is $|+\rangle^{\otimes N}$ and the output is the measurement outcomes on a specified subset of qubits in the X basis $(|+\rangle, |-\rangle)$.*

Let

$$R(\theta) = \begin{bmatrix} e^{-i\theta/2} & 0 \\ 0 & e^{i\theta/2} \end{bmatrix} = e^{-i\frac{\theta}{2}Z}$$

be the rotation about $\hat{z}$ axis by an arbitrary angle θ. In general, the quantum gates on an IQP circuit can be generated by $R(\theta)$ and controlled-rotation $CR(\theta)$, where

$$CR(\theta) \triangleq |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes R(\theta).$$

It is obvious that IQP circuits are not universal. Observe that the controlled-Z gate $CZ = |0\rangle\langle 0| \otimes I + |1\rangle\langle 1| \otimes Z$ is in IQP and a CNOT can be implemented by a CZ and two H gates. Thus universality can be achieved by including the Hadamard gate with the IQP circuits. However, H does not commute with gates in IQP. Instead, it is proved that IQP circuits with *postselection* is universal [12]. It has been shown that a Hadamard gate can be implemented by the gadget in Fig. 1 [1]. If the measurement outcome is $|+\rangle$ and no Pauli X correction is needed, this gadget has only one CZ as shown in Fig. 2, which is in IQP. In practical, a postselected circuit is implemented by repeating the circuit several times until the specified measurement outcomes are obtained.

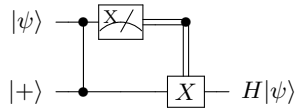

Fig. 1. The Hadamard gadget. The X-meter is a measurement in the X basis. Conditioned on the measurement outcome, a Pauli X correction is applied if necessary.

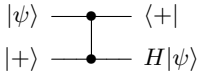

Fig. 2. The postselected Hadamard gadget. A postselection of the measurement outcome $|+\rangle$ is denoted by $\langle+|$.

Finally, we define another class of nonuniversal quantum circuits that is larger than IQP.

Definition 4. *An IQP$^+$ circuit is composed of X, Y,* CNOT*, $R(\theta)$, $CR(\theta)$ gates for any θ and possibly some measurements in the X or Z basis at the end, and the input state is a product state of qubits in $D_{xy}(\mathbb{C}^2)$, where*

$$D_{xy}(\mathbb{C}^2) \triangleq \{\rho \in D(\mathbb{C}^2) : \rho = \frac{I + v_x X + v_y Y}{2}, v_x^2 + v_y^2 \leq 1\}.$$

Note that an IQP circuit does not allow X, Y, and CNOT gates and measurements in the Z basis. If ρ is a product state of N qubits in $D_{xy}(\mathbb{C}^2)$, we simply say that $\rho \in D_{xy}(\mathbb{C}^2)^{\otimes N}$. We will provide an IT-secure QHE scheme IQPP that admits the evaluation of IQP$^+$ circuits in Sec. 5.

3 Impossibility of Information-Theoretically Secure Quantum Fully Homomorphic Encryption

In this section we formally define QHE schemes and their properties. Then we employ a lower bound for *quantum random access codes* [3] and show that the existence of an information-theoretically secure QFHE would contradict this lower bound.

Definition 5. *A private-key quantum homomorphic encryption scheme F is defined by the following four algorithms:*

- *(Key generation) $\mathsf{F.KeyGen}$: $1^\kappa \to sk$. The algorithm takes an input of a security parameter κ and outputs a classical private key sk.*
- *(Encryption) $\mathsf{F.Encrypt}_{sk}$: $D(\mathcal{M}) \to D(\mathcal{C})$, where $\mathcal{M}$ is the textspace and $\mathcal{C}$ is the cipherspace. The algorithm takes sk and a quantum state $\rho = \bigotimes_j \rho_j \in D(\mathcal{M})$ as input and outputs a quantum state $\tilde{\rho} = \bigotimes_j \tilde{\rho}_j \in D(\mathcal{C})$, where ρ_j are over the same state space and $\tilde{\rho}_j$ is the encrypted ρ_j using the key sk.*

– *(Evaluation)* $\mathsf{F.Eval}$*:* $\mathfrak{C}_\kappa \times D(\mathcal{C}) \to D(\mathcal{C}')$*, where* $\mathfrak{C}_\kappa$ *is a set of admissible quantum circuits for* F *and the security parameter* κ*. The algorithm takes* $C \in \mathfrak{C}_\kappa$ *and* $\tilde{\rho} \in D(\mathcal{C})$ *as input and outputs* $\sigma \in D(\mathcal{C}')$*.*
– *(Decryption)* $\mathsf{F.Decrypt}_{sk}$*:* $D(\mathcal{C}') \to D(\mathcal{M})$*. The algorithm takes* sk *and* $\sigma \in D(\mathcal{C}')$ *as input and outputs a quantum state* $\hat{\sigma} \in D(\mathcal{M})$*.*

(Correctness) F *is homomorphic for* $\mathfrak{C} = \cup_\kappa \mathfrak{C}_\kappa$ *if there exists a negligible function* η *of* κ *such that for* $sk \leftarrow \mathsf{F.KeyGen}(1^\kappa)$*,* $C \in \mathfrak{C}_\kappa$*, and input* $\rho \in D(\mathcal{M})$*, we have*

$$\left\| \mathbb{E}\left\{ \mathsf{F.Decrypt}_{sk}(\mathsf{F.Eval}(C, \mathsf{F.Encrypt}_{sk}(\rho))) \right\} - \mathbb{E}\left\{ C(\rho) \right\} \right\|_{\mathrm{tr}} \leq \eta(\kappa),$$

where the expectation $\mathbb{E}$ *is taken over all possible measurement outcomes.*
(Compactness) F *is compact if there exists a polynomial* p *in* κ *such that for any* $C \in \mathfrak{C}_\kappa$*, the circuit complexity of applying* $\mathsf{F.Decrypt}$ *to the output of* $\mathsf{F.Eval}_C$ *is at most* $p(\kappa)$*.*

We use a notion of expectation in the definition of correctness. This is because that quantum circuits may have measurements at the end and the measurement outcomes are random. Even though the outcomes are classical variables, they still fit in the language of quantum mechanics. That is, a classical string corresponds to a density operator diagonalized in the Z basis.

The compactness requirement simply says that the decryption complexity does not depend on the circuit for evaluation. This forbids the trivial case that the server does nothing but return the input state to the client so that the client simply evaluates the circuit in decryption.

Definition 6. *A quantum homomorphic encryption scheme* F *is information-theoretically secure if for any two quantum states* $\rho, \rho' \in D(\mathcal{M})$ *and a security parameter* κ*, there exists a negligible function* ϵ *of* κ *such that*

$$\left\| \mathbb{E}_{sk}\left\{ \mathsf{F.Encrypt}_{sk}(\rho) \right\} - \mathbb{E}_{sk}\left\{ \mathsf{F.Encrypt}_{sk}(\rho') \right\} \right\|_{\mathrm{tr}} \leq \epsilon(\kappa).$$

This definition says that two encrypted quantum states of an IT-secure QHE are statistically indistinguishable.

Definition 7. *A quantum homomorphic encryption scheme* F *is fully homomorphic if it is compact and homomorphic for all quantum circuits generated by a universal set of gates.*

Ouyang *et al.* introduced an IT-secure QHE scheme that is homomorphic for the Clifford circuits [40]. It is desired to investigate the existence of a QFHE that is IT-secure. Unfortunately, we answer this problem in the negative. We show this by a reduction to the nonexistence of IT-secure *quantum private information retrieval* (QPIR) protocol [21] with one database.

Next we briefly introduce the notion of quantum random access codes [3]. An (n, m, p) random access code is a function that encodes an n-bit string $x \in \{0,1\}^n$ in an m-qubit quantum state $\rho_x \in \mathbb{C}^{2^m}$ and for any $1 \leq i \leq n$, there exists

measurement $\mathcal{O}_i$ with outcome 0 or 1 such that $\Pr\{\mathcal{O}_i(\rho_x) = x_i\} \geq p$. It holds that

$$m \geq (1 - H(p))n, \tag{2}$$

where $H(p) = -p \log p - (1-p)\log(1-p)$ is the binary entropy function. Nayak [37] argued that this is also a communication lower bound for the problem of IT-secure QPIR [21] with one database. In an QPIR problem with a single server, Alice (the server) has a database of n-bit string x and Bob wishes to learn the ith entry x_i with probability $p > 1/2$ by exchanging m qubits without revealing the index i to Alice. Such a protocol is called an (n, m, p) QPIR protocol. Equation (2) holds here since an (n, m, p) QPIR protocol would define an (n, m, p) quantum random access code. (See also [6] for an extension of this result.)

Now we prove the impossibility of IT-secure QFHE as follows.

Theorem 8. *There is no QFHE with IT-security.*

Proof. Assume there is an IT-secure QFHE scheme F. Suppose Alice holds a database $x \in \{0,1\}^n$ and Bob wants to retrieve information x_i from Alice by using F without revealing i. Let C_x be a quantum circuit that takes an input $i \in \{1, 2, \ldots, n\}$ and outputs x_i. (We may consider classical circuits as a special case of quantum circuits.)

First Bob chooses an index i^* of $\log n$ bits in mind. Using the QFHE algorithm F, he generates the cipher state $\mathsf{F.Encrypt}_{sk}(i^*)$, which is of $O(\mathrm{poly}(\kappa) \cdot \log n)$ qubits for some random private key $sk \leftarrow \mathsf{F.KeyGen}(1^\kappa)$, and then sends it to Alice. After computing $\mathsf{F.Eval}(C_x, \mathsf{F.Encrypt}_{sk}(i^*))$, Alice obtains $\mathsf{F.Encrypt}_{sk}(x_{\widehat{i}})$ for some $\widehat{i} \in \{1, \ldots, n\}$, which is of $O(\mathrm{poly}(\kappa) \cdot \log n)$ qubits. Then she sends it back to Bob, who then decrypts it and obtains $x_{\widehat{i}}$.

Since the QFHE scheme F is IT-secure by assumption, Alice cannot learn Bob's choice of i^*. If she honestly computes the homomorphic evaluation, Bob would learn $x_{\widehat{i}} = x_{i^*}$. Thus we have an $(n, m = O(\mathrm{poly}(\kappa) \cdot \log n), p = 1)$ QPIR protocol with information-theoretic security inherited from the QFHE F.

Now if the security parameter κ is chosen such that

$$O(\mathrm{poly}(\kappa) \cdot \log n) < n,$$

which contradicts the Nayak lower bound (2) that at least $\Omega(n)$ qubits are required in communication. Therefore, an IT-secure QFHE cannot exist. □

Observe that in the proof of Theorem 8, Alice needs to homomorphically evaluates only a classical selection function, which is impossible for any IT-secure QHE schemes. Thus we have the following corollary.

Corollary 9. *There is no QHE that is homomorphic for classical circuits with IT-security.*

4 Homomorphic Computation on Stabilizer Codes

We begin with a brief introduction of stabilizer codes and then discuss each function block that will be used in our scheme IQPP in the following subsections. The complete scheme of IQPP will be presented in Sec. 5.

4.1 Stabilizer Codes

Suppose $\mathcal{S}$ is an Abelian subgroup of the n-fold Pauli group $\mathcal{G}_n$ with independent generators $g_1, \ldots, g_{n-k}$ and $-I^{\otimes n} \notin \mathcal{S}$. Then $\mathcal{S}$ defines an $[[n, k]]$ quantum *stabilizer code*

$$\mathcal{Q}(\mathcal{S}) = \{|\psi\rangle \in \mathbb{C}^{2^n} : g|\psi\rangle = |\psi\rangle, \forall g \in \mathcal{S}\},$$

which is a subspace of $\mathbb{C}^{2^n}$ of dimension 2^k [30, 39]. The vectors in $\mathcal{Q}(\mathcal{S})$ are called *codewords* of $\mathcal{Q}(\mathcal{S})$. The elements in $\mathcal{S}$ are called the *stabilizers* of $\mathcal{Q}(\mathcal{S})$. The vector space $\mathcal{Q}(\mathcal{S})$ is isomorphic to the state space of k logical qubits. In this section, a logical operator U on the jth logical qubit will be denoted by $\bar{U}_j$ and a logical qubit will be denoted by $|\bar{\psi}\rangle$.

Quantum Calderbank-Shor-Steane (CSS) codes [19,48] are a class of stabilizer codes with stabilizer generators of the form Z^v or X^u for $v, u \in \{0, 1\}^n$. Herein we construct a family of concatenated CSS codes and propose a QHE scheme IQPP that admits the evaluation of IQP^+ circuits. In particular, our codes are obtained by concatenating multiple layers of the $[[7, 1]]$ *Steane* code [48] with a $[[6, 2]]$ CSS code $\mathcal{Q}_6$ at the top-level.

4.2 Steane Code

Consider the initial state

$$|\psi\rangle|+\rangle|+\rangle|+\rangle|0\rangle|0\rangle|0\rangle \in \mathbb{C}^{2^7},$$

where $|\psi\rangle \in \mathbb{C}^2$ is an arbitrary information qubit, and $|0\rangle$ and $|+\rangle$ are ancillas. This initial state has six independent stabilizer generators X_2, X_3, X_4, Z_5, Z_6, and Z_7 and its logical Pauli operators are X_1 and Z_1 that modify the information qubit $|\psi\rangle$. An encoding circuit of the Steane code is shown in Fig. 3. After encoding, we have

$$\begin{aligned}
|\bar{0}\rangle =& |0000000\rangle + |1100011\rangle + |1010101\rangle + |1001110\rangle \\
&+ |0110110\rangle + |0101101\rangle + |0011011\rangle + |1111000\rangle \\
|\bar{1}\rangle =& |1111111\rangle + |0011100\rangle + |0101010\rangle + |0110001\rangle \\
&+ |1001001\rangle + |1010010\rangle + |1100100\rangle + |0000111\rangle.
\end{aligned}$$

Thus the logical Pauli operators are

$$\bar{X} = X^{\otimes 7}, \bar{Z} = Z^{\otimes 7}.$$

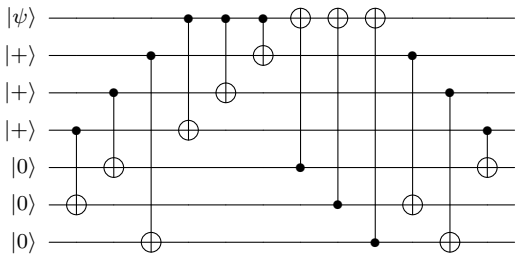

Fig. 3. An encoding circuit of the $[[7, 1]]$ Steane code.

The corresponding stabilizer generators are

$$g_1 = X_1X_2X_6X_7,\ g_4 = Z_1Z_2Z_6Z_7,$$
$$g_2 = X_1X_3X_5X_7,\ g_5 = Z_1Z_3Z_5Z_7,$$
$$g_3 = X_1X_4X_5X_6,\ g_6 = Z_1Z_4Z_5Z_6.$$

Clifford gates can be transversally implemented in the Steane code as mentioned previously [23]. The logical measurement in the Z basis is by a classical decoding of the bitwise single-qubit measurement outcomes in the Z basis, and similar for the logical measurement in the X basis.

Next we describe how the logical $R(\theta)$ and $CR(\theta)$ gates are implemented in this paper.

Proposition 10. *The logical $R(\theta)$ gate in the Steane code can be implemented by*

$$\bar{R}(\theta) = (C_2X_3)(C_3X_7)R_7(\theta)(C_3X_7)(C_2X_3). \tag{3}$$

Proof. For $c = c_1 \cdots c_7 \in \{0, 1\}^7$, let $a_c = c_2c_3c_7$ and $b_c = c_1c_4c_5c_6$. Observe that

$$(C_2X_3)(C_3X_7)R_7(\theta)(C_3X_7)(C_2X_3)|c\rangle = \begin{cases} e^{-i\theta/2}|c\rangle, \text{ if wt}\,(a_c) \equiv 0 \mod 2; \\ e^{i\theta/2}|c\rangle, \quad \text{otherwise,} \end{cases}$$

where wt (a) is the number of nonzero bits of a. Consequently,

$$(C_2X_3)(C_3X_7)R_7(\theta)(C_3X_7)(C_2X_3)|\overline{0}\rangle = e^{-i\theta/2}|\overline{0}\rangle,$$
$$(C_2X_3)(C_3X_7)R_7(\theta)(C_3X_7)(C_2X_3)|\overline{1}\rangle = e^{i\theta/2}|\overline{1}\rangle.$$

Thus $\bar{R}(\theta) = (C_2X_3)(C_3X_7)R_7(\theta)(C_3X_7)(C_2X_3)$ as desired. □

The circuit in Fig. 4 is used to implement the logical $R(\theta)$ gate, which generalizes the implementation of the logical T gate in [32]. Similarly, the circuit in Fig. 5 is used to implement the logical $CR(\theta)$ gate.

Proposition 11. *The logical $CR(\theta)$ gate between two codewords (qubits numbered from 1 to 14) of the Steane code can be implemented by*

$$\overline{C_1R_2}(\theta) = (C_2X_3)(C_9X_{10})(C_3X_7)(C_{10}X_{14})C_7R_{14}(\theta)(C_{10}X_{14})(C_3X_7)(C_9X_{10})(C_2X_3). \tag{4}$$

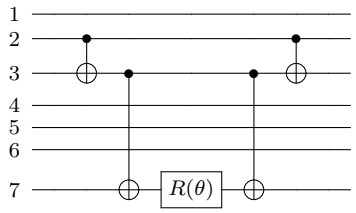

Fig. 4. The circuit implementation of the logical $R(\theta)$ gate in the Steane code.

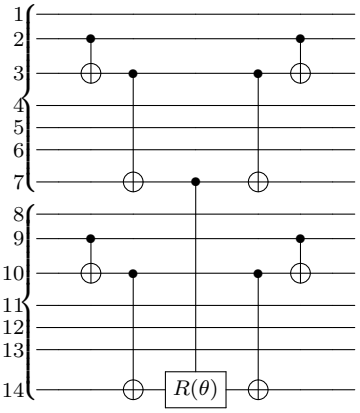

Fig. 5. The circuit implementation of the logical $CR(\theta)$ gate between two codewords of the Steane code.

4.3 [[6, 2]] CSS Code $\mathcal{Q}_6$

A [[6,2]] quantum code encodes two information qubits in six physical qubits. Suppose we have the following 6-qubit initial state

$$|\Psi\rangle = |\psi_1\rangle|\psi_2\rangle|+\rangle|+\rangle|0\rangle|0\rangle \in \mathbb{C}^{2^6}, \tag{5}$$

where $|\psi_1\rangle$ and $|\psi_2\rangle$ are two arbitrary information qubits in $\mathbb{C}^2$ and the ancilla states $(|+\rangle, |0\rangle)$ are chosen appropriately. The stabilizer generators of $|\Psi\rangle$ are X_3, X_4, Z_5, and Z_6, and its logical Pauli operators are X_1, Z_1 and X_2, Z_2.

Consider a Clifford unitary encoding operator U_6 as shown in Fig. 6 such that

$$\begin{array}{ll}
U_6 X_1 U_6^\dagger = XIIIXX & U_6 Z_1 U_6^\dagger = ZZIIII, \\
U_6 X_2 U_6^\dagger = XXIIII & U_6 Z_2 U_6^\dagger = IZZZII, \\
U_6 X_3 U_6^\dagger = XXXIXI & U_6 Z_3 U_6^\dagger = IIZIII, \\
U_6 X_4 U_6^\dagger = XXIXIX & U_6 Z_4 U_6^\dagger = IIIZII, \\
U_6 Z_5 U_6^\dagger = ZZZIZI & U_6 X_5 U_6^\dagger = IIIIXI, \\
U_6 Z_6 U_6^\dagger = ZZIZIZ & U_6 X_6 U_6^\dagger = IIIIIX.
\end{array} \tag{6}$$

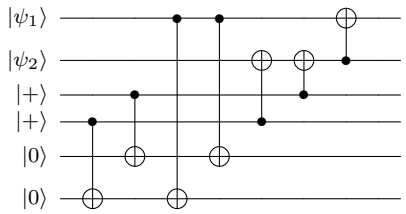

Fig. 6. The encoding circuit of the $[[6,2]]$ CSS code $\mathcal{Q}_6$.

Our $[[6,2]]$ code $\mathcal{Q}_6$ is defined by the four stabilizer generators

$$g_1 = U_6 X_3 U_6^\dagger, g_2 = U_6 X_4 U_6^\dagger, g_3 = U_6 Z_5 U_6^\dagger, g_4 = U_6 Z_6 U_6^\dagger,$$

and the logical Pauli operators are $\bar{X}_1 = U_6 X_1 U_6^\dagger$, $\bar{X}_2 = U_6 X_2 U_6^\dagger$, $\bar{Z}_1 = U_6 Z_1 U_6^\dagger$, and $\bar{Z}_2 = U_6 Z_2 U_6^\dagger$. The codewords of $\mathcal{Q}_6$ in the computational basis are

$$|\overline{00}\rangle = \frac{1}{2}\left(|000000\rangle + |111010\rangle + |110101\rangle + |001111\rangle\right), \tag{7}$$

$$|\overline{10}\rangle = \frac{1}{2}\left(|100011\rangle + |011001\rangle + |010110\rangle + |101100\rangle\right), \tag{8}$$

$$|\overline{01}\rangle = \frac{1}{2}\left(|110000\rangle + |001010\rangle + |000101\rangle + |111111\rangle\right), \tag{9}$$

$$|\overline{11}\rangle = \frac{1}{2}\left(|010011\rangle + |101001\rangle + |100110\rangle + |011100\rangle\right), \tag{10}$$

which are derived by $|\overline{00}\rangle = \frac{1}{2}\left(\sum_{i,j=0}^{1} g_1^i g_2^j |000000\rangle\right)$, $|\overline{10}\rangle = \bar{X}_1|\overline{00}\rangle$, $|\overline{01}\rangle = \bar{X}_2|\overline{00}\rangle$, and $|\overline{11}\rangle = \bar{X}_1\bar{X}_2|\overline{00}\rangle$.

Note that in IQPP, we will implement logical operations on the first logical qubit of $\mathcal{Q}_6$, while the state of the second logical qubit is not concerned. (More precisely, the second logical qubit is chosen to be the maximally-mixed state $\frac{1}{2}I$ for a security issue.) In particular, $\mathcal{Q}_6$ is chosen so that the supports of $\bar{X}_1$ and $\bar{Z}_1$ are different.

A transversal CNOT between two codewords implements a logical CNOT from the control codeword to the target codeword since $\mathcal{Q}_6$ is a CSS code [23]. Again, the logical measurement in the Z (or X) basis is by a classical decoding of the bitwise single-qubit measurement outcomes in the Z (or X) basis.

The logical $R_1(\theta)$ and $CR(\theta)$ between the first logical qubits of two codewords are shown in Figs. 7 and 8, respectively.

Proposition 12. *The logical $R(\theta)$ gate on the first logical qubit of a codeword of $\mathcal{Q}_6$ can be implemented by*

$$\bar{R}_1(\theta) = (C_1 X_2) R_2(\theta) (C_1 X_2). \tag{11}$$

Proof. Let $a \in \{0,1\}^2, b \in \{0,1\}^4$ and their concatenation be denoted by $ab \in \{0,1\}^6$. Observe that

$$(C_1X_2)R_2(\theta)(C_1X_2)|ab\rangle = \begin{cases} e^{-i\theta/2}|ab\rangle, \text{ if wt}\,(a) \equiv 0 \mod 2; \\ e^{i\theta/2}|ab\rangle, \text{ otherwise,} \end{cases}$$

where, again, wt (a) is the number of nonzero bits of a. Consequently,

$$(C_1X_2)R_2(\theta)(C_1X_2)|\overline{0v}\rangle = e^{-i\theta/2}|\overline{0v}\rangle,$$
$$(C_1X_2)R_2(\theta)(C_1X_2)|\overline{1v}\rangle = e^{i\theta/2}|\overline{1v}\rangle,$$

for $v \in \{0,1\}$. Thus $\bar{R}_1(\theta) = (C_1X_2)R_2(\theta)(C_1X_2)$ as desired. □

Similarly, we have the following proposition for $CR(\theta)$ gate of $\mathcal{Q}$.

Proposition 13. *The logical $CR(\theta)$ gate between two codewords (qubits numbered from 1 to 12) of $\mathcal{Q}_6$ can be implemented by*

$$\overline{C_1R_2}(\theta) = (C_1X_2)(C_7X_8)C_2R_8(\theta)(C_7X_8)(C_1X_2). \tag{12}$$

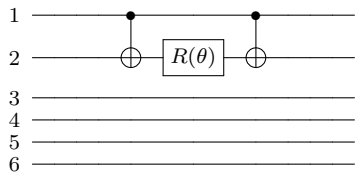

Fig. 7. The circuit that implements $\bar{R}_1(\theta)$ for the $[[6,2]]$ code $\mathcal{Q}_6$. Note that only the first two qubits are involved.

Other possible logical operations, such as the Hadamard gate, the logical CNOT gates within a codeword, are postponed to Appendix A, since they cannot be implemented without leaking any information about the encrypted message qubit in IQPP.

4.4 Concatenated Quantum Codes

To achieve security asymptotically, we need an infinite code family. A useful method to construct a large code is by concatenating small codes. Suppose an upper-layer $[[n_u, k]]$ quantum code $\mathcal{Q}(\mathcal{S}_u)$ with stabilizer group $\mathcal{S}_u$ is concatenated with a bottom-layer $[[n_b, 1]]$ quantum code $\mathcal{Q}(\mathcal{S}_b)$ with stabilizer group $\mathcal{S}_b$. The concatenated quantum code $\mathcal{Q}$ has parameters $[[n_un_b, k]]$ [27] and its codewords are codewords of $\mathcal{Q}(\mathcal{S}_u)$ built on logical qubits of $\mathcal{Q}(\mathcal{S}_b)$. The stabilizers of $\mathcal{Q}$ has two types. The first type is obtained by replacing the Pauli components of the stabilizers of $\mathcal{S}_u$ with the logical operators of $\mathcal{Q}(\mathcal{S}_b)$. The second type are the

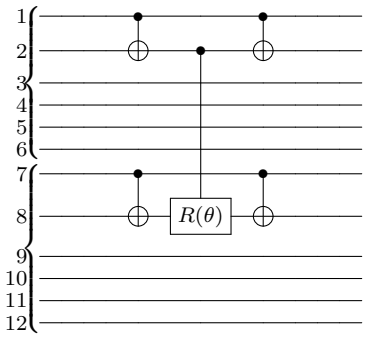

Fig. 8. The circuit that implements a logical $CR(\theta)$ gate between the first logical qubits of two codewords of the $[[6, 2]]$ code $\mathcal{Q}_6$.

stabilizers of $\mathcal{S}_b$ acting on one of the n_u codeword blocks of n_b qubits. Similarly, the logical operators of $\mathcal{Q}$ are the logical operators of $\mathcal{Q}(\mathcal{S}_u)$ with components being replaced by the logical operators of $\mathcal{Q}(\mathcal{S}_b)$.

If we concatenate the $[[6, 2]]$ code $\mathcal{Q}_6$ (top-level) with l layers of the Steane code (bottom level), we obtain a $[[6 \cdot 7^l, 2]]$ code $\mathcal{Q}_6^{(l)}$. The logical operators on the first information qubit of $\mathcal{Q}_6^{(l)}$ are

$$\begin{aligned} \bar{X}_1^{(l)} &= X^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} X^{\otimes 7^l} X^{\otimes 7^l}, \\ \bar{Z}_1^{(l)} &= Z^{\otimes 7^l} Z^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l}, \end{aligned} \tag{13}$$

and

$$\bar{Y}_1^{(l)} = (-1)^l Y^{\otimes 7^l} Z^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} X^{\otimes 7^l} X^{\otimes 7^l}. \tag{14}$$

Let $U_6^{(l)}$ denote the Clifford encoder of $\mathcal{Q}_6^{(l)}$ and let $\mathcal{D}_6^{(l)}$ be an efficient decoder (a general quantum operation) of $\mathcal{Q}_6^{(l)}$.

The logical CNOT gate between two codewords is also transversally implemented. Now a rotation about $\hat{z}$ is implemented as in Proposition 13, with the gates being replaced by the logical gates of a lower-layer code, recursively. For example, the $R(\theta)$ gate in Fig. 7 is implemented by the circuit in Fig. 4 in an l-layer concatenated version. Let $\bar{R}^{(l)}(\theta)$ denote the rotation of the first logical qubit of $\mathcal{Q}_6^{(l)}$ about $\hat{z}$. Let $\overline{CR}^{(l)}(\theta)$ denote the $CR(\theta)$ between two codewords of $\mathcal{Q}_6^{(l)}$.

4.5 Noisy Encoding

Recall that by definition, the eigenvalues of the stabilizer generators of a clean codeword are all $+1$'s. In a task of homomorphic encryption, it is assumed that there are no communication errors on the physical qubits. To some extent, using

clean codewords may reveal information about the encrypted qubits. Thus random noises are introduced to modified these eigenvalues. This is done by padding the ancillas in (5): $|+\rangle$ is replaced by $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ with probability 0.5 and remains unchanged with probability 0.5; similarly for $|0\rangle$. That is,

$$|+\rangle\langle+| \rightarrow \frac{1}{2}(|+\rangle\langle+| + |-\rangle\langle-|) = \frac{1}{2}I$$
$$|0\rangle\langle 0| \rightarrow \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|) = \frac{1}{2}I.$$

This is similar to performing quantum one-time padding [2] on the ancillas before encoding. As a result, the density operator of the initial state (5) becomes

$$|\psi\rangle\langle\psi| \otimes (\frac{1}{2}I)^{\otimes 5}$$

and the encoded state is

$$U_6 \left(|\psi_1\rangle\langle\psi_1| \otimes (\frac{1}{2}I)^{\otimes 5} \right) U_6^\dagger \tag{15}$$

Equivalently, the codeword is corrupted by a random Pauli $U_6 Z_3^{a_3} Z_4^{a_4} X_5^{a_5} X_6^{a_6} U_6^\dagger$ for $a_j \in \{0, 1\}$. Since only the ancilla states are modified, these errors are correctable and the information qubit can be perfectly recovered. This is called *noisy encoding**. Note that the second logical qubit is also put in the maximally-mixed state $\frac{1}{2}I$ for security. In general, the noisily-encoded state of $\rho = \frac{I+v_1X+v_2Y+v_3Y}{2}$ by $U_6^{(l)}$ is

$$\begin{aligned} U_6^{(l)} \left(\rho \otimes (\frac{1}{2}I)^{\otimes(6\cdot 7^l-1)} \right) U_6^{(l)\dagger} =& \frac{1}{2} \Big(I^{\otimes(6\cdot 7^l)} + v_1 X^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} X^{\otimes 7^l} X^{\otimes 7^l} \\ &+ v_2 Y^{\otimes 7^l} Z^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} X^{\otimes 7^l} X^{\otimes 7^l} \\ &+ v_3 Z^{\otimes 7^l} Z^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} \Big) \end{aligned} \tag{16}$$

according to (13) and (14). As we mentioned before that the noisy encoding is recoverable, we have

$$\mathcal{D}_6^{(l)} \left(U_6^{(l)} \left(\rho \otimes (\frac{1}{2}I)^{\otimes(6\cdot 7^l-1)} \right) U_6^{(l)\dagger} \right) = \rho.$$

4.6 Permutation on the Qubits

The information-theoretic security of the homomorphic encryption in [40] comes from the random qubit-permutation on the noisily-encoded quantum codeword (15) with additional maximally-mixed states ($\frac{1}{2}I$)'s. A similar manner will appear in our scheme. The permutation operator will be introduced here.

* This is called *random encoding* in [40], but we want to avoid the possible confusion with *randomized encoding*.

Let S_m denote the symmetric group of permutations on $\{1, 2, \ldots, m\}$. A permutation that exchanges two elements $x, y \in \{1, 2, \ldots, m\}$ and keeps all the others fixed is called a *transposition* and is denoted by $\tau(x, y)$. It is known that every permutation can be decomposed as a product of transpositions.

Two qubits can be swapped by the circuit shown in Fig. 9. Let SWAP(i, j) denote the circuit that swaps the states of qubits i and j. It is obvious that performing SWAP(i, j) is equivalent to applying transition $\tau(i, j)$ on the qubit indices. Given a permutation $\pi = \prod_i \tau(a_i, b_i) \in S_a$, we can define a corresponding permutation operator on the m-qubit space by

$$\mathrm{Per}_\pi = \prod_i \mathrm{SWAP}(a_i, b_i) \in L(\mathbb{C}^{2^m}), \tag{17}$$

which can be implemented by a series of SWAPs.

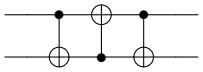

Fig. 9. The circuit for swapping two qubits: SWAP.

5 Quantum Homomorphic Encryption Scheme for IQP$^+$ Circuits

In this section we give our IT-secure QHE scheme IQPP that admits the evaluation of IQP$^+$ circuits.

Let IQP^+_N be the set of IQP$^+$ circuits with at most N input qubits. Suppose a client asks a server to compute a quantum circuit $C \in \mathrm{IQP}^+_N$ on an N-qubit input state $\rho = \bigotimes_{i=1}^N \rho_i \in D_{xy}(\mathbb{C}^2)^{\otimes N}$, where $\rho_i \in D_{xy}(\mathbb{C}^2)$.

Our symmetric-key QHE scheme IQPP is defined as follows.

QHE scheme IQPP
security parameter κ
variables N, l, m,
input $C \in \mathrm{IQP}^+_N$, and $\rho \in D_{xy}(\mathbb{C}^2)^{\otimes N}$

- (Key generation) $\mathsf{IQPP.KeyGen} : 1^N \times 1^l \times 1^m \to (S_{n/3+m})^N$, where $n \triangleq 6 \cdot 7^l$. A permutation $\pi \in S_{n/3+m}$ is uniformly chosen as the symmetric key and will be used N times.
- (Encryption) $\mathsf{IQPP.Encrypt}_\pi$: $D(\mathbb{C}^{2^N}) \to D(\mathbb{C}^{2^{N(n+m)}})$. Encryption is done by a noisy encoding $U_6^{(l)}$ followed by a random permutation on the last $n/3$ qubits with m maximally-entangled states.

$$\mathsf{IQPP.Encrypt}_\pi\left(\bigotimes_{i=1}^N \rho_i\right) = \bigotimes_{i=1}^N \left(I^{\otimes 2n/3} \otimes \mathrm{Per}_\pi\right) \mathcal{A}_m \left(U_6^{(l)} \left(\rho_i \otimes (\frac{1}{2}I)^{\otimes(n-1)}\right) U_6^{(l)\dagger}\right) \left(I^{\otimes 2n/3} \otimes \mathrm{Per}_\pi^\dagger\right),$$

where $\mathcal{A}_m : D(\mathcal{X}) \to D(\mathcal{X} \otimes \mathbb{C}^{2^m})$ is a quantum operation defined by

$$\mathcal{A}_m(\rho) = \rho \otimes (\frac{1}{2}I)^{\otimes m} \tag{18}$$

for $\rho \in D(\mathcal{X})$.

– (Evaluation) $\mathsf{IQPP.Eval} : \mathrm{IQP}_N^+ \times D(\mathcal{C}^{2^{N(n+m)}}) \to D(\mathcal{C}^{2^{N(n+m)}}) \times \{\perp, 0, 1\}^{N(n+m)}$. Let $R = \perp^{N(n+m)}$ be a register that records the measurement outcomes, where $\perp$ is the default state of an entry. Suppose $C \in \mathrm{IQP}_N^+$ is composed of the gates $c_1, \ldots, c_t$ in sequence and $\bar{\rho} = \mathsf{IQPP.Encrypt}_\pi \left(\bigotimes_{i=1}^N \rho_i \right) \in D(\mathbb{C}^{2^{N(n+m)}})$. The homomorphic operation of c_j are applied to $\bar{\rho}$ in sequence:
  - If $c_j = X_i$, apply $I^{\otimes(i-1)(n+m)} \otimes \left(\bar{X}_1^{(l)} \otimes X^{\otimes m} \right) \otimes I^{\otimes(N-i)(n+m)}$.
  - If $c_j = Y_i$, apply $I^{\otimes(i-1)(n+m)} \otimes \left(\bar{Y}_1^{(l)} \otimes X^{\otimes m} \right) \otimes I^{\otimes(N-i)(n+m)}$.
  - If $c_j = C_i X_k$, apply $\prod_{h=1}^{n+m} C_{(i-1)(n+m)+h} X_{(k-1)(n+m)+h}$.
  - If $c_j = R_i(\theta)$, apply $I^{\otimes(i-1)(n+m)} \otimes \left(\bar{R}^{(l)}(\theta) \otimes I^{\otimes m} \right) \otimes I^{\otimes(N-i)(n+m)}$.
  - If $c_j = C_i R_k(\theta)$, apply $I^{\otimes(i-1)(n+m)} \otimes \left(\overline{C_i R}_k^{(l)}(\theta) \otimes I^{\otimes m} \right) \otimes I^{\otimes(N-i)(n+m)}$.
  - If c_j is a measurement on qubit i in the X (or Z) basis, apply bitwise measurements in the X (or Z) basis on qubits $(i-1)(n+m)+1$ to $i(n+m)$ and update R with the measurement outcomes correspondingly.

  Let $(\Upsilon, R) = \mathsf{IQPP.Eval}(C, \bar{\rho})$, where $\Upsilon \in D(\mathbb{C}^{2^{N(n+m)}})$.

– (Decryption) $\mathsf{IQPP.Decrypt}_\pi$: $D(\mathcal{C}^{2^{N(n+m)}}) \times \{\perp, 0, 1\}^{N(n+m)} \to D(\mathcal{C}^{2^N}) \times \{\perp, 0, 1\}^N$. Decryption is done by the following steps.
  1. Apply $I^{\otimes 2n/3} \otimes P_{\pi^{-1}}$ on each block of $n+m$ qubits of Υ and throw out those qubits that are appended to the codewords of $\mathcal{Q}_6^{(l)}$. Let $\check{\Upsilon} \in D(\mathbb{C}^{2^{Nn}})$ be the residual state.
  2. Apply π^{-1} to each $n+m$ block of the register R and delete those dummy outcomes. Let $\check{R} \in \{\perp, 0, 1\}^{Nn}$ be the residual outcomes.
  3. Let $O = \perp^N$ be a register that records the decrypted measurement outcomes. For $j = 1$ to N, apply a classical decoding to $\check{R}_{(j-1)n+1} \cdots \check{R}_{jn}$ if there is a measurement on the jth line of the circuit C and then update O_j with the decoded outcome. Otherwise, apply $\mathcal{D}_6^{(l)}$ to qubits $(j-1)n+1$ to jn of $\check{\Upsilon}$ and throw out those ancillas. Let $\Phi \in D(\mathbb{C}^{2^N})$ be the final state. Then

$$(\Phi, O) \leftarrow \mathsf{IQPP.Decrypt}_\pi \left(\Upsilon, R \right).$$

To prove the information-theoretically security of IQPP, we need the following lemma, which results from noisy encoding and a randomly qubit-permutation with maximally-mixed states. The proof is similar to [40, Lemma 4]. This lemma says that security can be achieved by permuting only the last 1/3 qubits of a codeword of $\mathcal{Q}_6^{(l)}$ with sufficient maximally-mixed states.

Lemma 14. *Let N, m, l be positive integers and $n = 6 \cdot 7^l$. Suppose*

$$\tilde{\rho} = \frac{1}{(n/3+m)!} \sum_{\pi \in S_{n/3+m}} \mathit{IQPP.Encrypt}_\pi \left(\bigotimes_{i=1}^{N} \rho_i \right)$$

and

$$\tilde{\rho}' = \frac{1}{(n/3+m)!} \sum_{\pi \in S_{n/3+m}} \mathit{IQPP.Encrypt}_\pi \left(\bigotimes_{i=1}^{N} \rho_i' \right),$$

where $\rho_i, \rho_i' \in D_{xy}(\mathbb{C}^2)$. Then

$$\frac{1}{2}||\tilde{\rho} - \tilde{\rho}'||_{\mathrm{tr}} \leq 2\left(3^N - 1\right) \binom{\frac{n}{3}+m}{m}^{-1/2}. \tag{19}$$

Proof. We begin with some notation in this proof. Let $1_a 0_b \in \{0,1\}^{a+b}$ denote the binary string $\underbrace{1\cdots1}_{a}\underbrace{0\cdots0}_{b}$ and we may omit the subscript when it is one. Let $0_{a\times b}$ be the $a \times b$ all-zero matrix and $1_{a\times b}$ be the $a \times b$ all-one matrix Let $\{0,1,2,3\}^{a\times b}$ be the set of $a \times b$ matrices with entries in $\{0,1,2,3\}$. For $A = [A_{i,j}] \in \{0,1,2,3\}^{a\times b}$, define

$$\sigma_A = \otimes_{i=1}^{a} \otimes_{j=1}^{b} \sigma_{A_{i,j}}.$$

Thus $\rho = \frac{1}{2^{Nn}} \otimes_{i=1}^{N} \left((I + v_{i,1}X + v_{i,2}Y) \otimes I^{\otimes n-1}\right)$ can be expressed as

$$\rho = \frac{1}{2^{Nn}} \sum_{r \in \{0,1,2\}^{N\times 1}} a_r \sigma_{r[10_{n-1}]},$$

where $a_r = \prod_{i=1}^{n} v_{i,r_{i,1}} \in \mathbb{C}$ and $r[10_{n-1}] \in \{0,1,2\}^{N\times n}$. Note that $|a_r| \leq 1$. Similarly,

$$\rho' = \frac{1}{2^{Nn}} \sum_{r \in \{0,1,2\}^{N\times 1}} a_r' \sigma_{r[10_{n-1}]}.$$

Thus by (16),

$$(U_6^{(l)})^{\otimes N}(\rho - \rho')(U_6^{(l)\dagger})^{\otimes N} = \frac{1}{2^{Nn}} \sum_{r \in \{0,1,2\}^{N\times 1} \setminus 0_{N\times 1}} (a_r - a_r')\sigma_{[E_r 1_{N\times(n/3)}]}, \tag{20}$$

where $E_r \in \{0,1,2\}^{N\times(2n/3)}$ depends on the encoding of σ_r.

It is known that the trace distance of two quantum states is an upper bound on the difference of their probabilities of obtaining the same measurement outcome [39]:

$$\frac{1}{2}||\rho - \sigma||_{\mathrm{tr}} = \max_{M': M' \geq 0, M' \leq \mathrm{id}} \mathrm{tr}\left(M'(\rho - \sigma)\right).$$

Suppose $\frac{1}{2}||\tilde{\rho}-\tilde{\rho}'||_{\mathrm{tr}} = \mathrm{tr}\left(M(\tilde{\rho}-\tilde{\rho}')\right)$ for Hermitian positive operator $M \in L(\mathbb{C}^{2^{N(n+m)}})$. Then we have, by (18) and (20),

$$\begin{aligned}\frac{1}{2}||\tilde{\rho}-\tilde{\rho}'||_{\mathrm{tr}} =& \mathrm{tr}\left(M\left(\frac{1}{(n/3+m)!}\sum_{\pi\in S_{n/3+m}} \mathsf{IQPP.Encrypt}_{\pi}\left(\bigotimes_{i=1}^{N}\rho_i - \bigotimes_{i=1}^{N}\rho_i'\right)\right)\right)\\ =& \frac{1}{2^{N(n+m)}}\mathrm{tr}\left(\tilde{M}\left(\sum_{r\in\{0,1,2\}^{N\times 1}\setminus 0_{N\times 1}}(a_r-a_r')\sigma_{[E_r 1_{N\times\frac{n}{3}}0_{N\times m}]}\right)\right),\end{aligned} \tag{21}$$

where

$$\tilde{M} = \frac{1}{(n/3+m)!}\sum_{\pi\in S_{n/3+m}}\left(I^{\otimes 2n/3}\otimes \mathrm{Per}_{\pi}\right)^{\otimes N} M \left(I^{\otimes 2n/3}\otimes \mathrm{Per}_{\pi}^{\dagger}\right)^{\otimes N}.$$

For $A\in\{0,1,2,3\}^{N\times(n+m)}$, define

$$\hat{\sigma}_A = \sum_{\pi\in S_{n/3+m}}\left(I^{\otimes 2n/3}\otimes \mathrm{Per}_{\pi}\right)^{\otimes N}\sigma_A\left(I^{\otimes 2n/3}\otimes \mathrm{Per}_{\pi}^{\dagger}\right)^{\otimes N}.$$

Let $G_{N\times(n+m)}$ be a maximal subset of $\{0,1,2,3\}^{N\times(n+m)}$ such that for $A,B\in G_{N\times(n+m)}$, $\hat{\sigma}_A\neq\hat{\sigma}_B$. Then $\tilde{M}$ can be expressed as

$$\tilde{M} = \sum_{A\in G_{N\times(n+m)}} a_A\hat{\sigma}_A,$$

where $a_A\in\mathbb{C}$. (This is possible since M can be decomposed as a linear combination of σ_A.) The absolute values of $a_{[E_r 1_{N\times(n/3)}0_{N\times m}]}$ can be upper bounded as follows.

$$\begin{aligned}2^{N(n+m)} \geq& \mathrm{tr}\left(\tilde{M}^2\right) = \mathrm{tr}\left(\sum_{A,A'\in G_{N\times(n+m)}} a_A a_{A'}\hat{\sigma}_A\hat{\sigma}_{A'}\right) \overset{(a)}{=} \sum_{A\in G_{N\times(n+m)}}\mathrm{tr}\left(a_A^2\hat{\sigma}_A^2\right)\\ \geq& a^2_{[E_r 1_{N\times(n/3)}0_{N\times m}]}\mathrm{tr}\left(\hat{\sigma}^2_{[E_r 1_{N\times(n/3)}0_{N\times m}]}\right)\\ \overset{(b)}{=}& a^2_{[E_r 1_{N\times(n/3)}0_{N\times m}]}\cdot\left(\frac{n}{3}+m\right)!\left(\frac{n}{3}\right)!m!\cdot 2^{N(n+m)},\end{aligned}$$

where (a) and (b) are because that Pauli operators are orthogonal to each other with respect to the trace inner product. Thus

$$\left|a_{[E_r 1_{N\times(n/3)}0_{N\times m}]}\right| \leq \sqrt{\frac{1}{\left(\frac{n}{3}+m\right)!\left(\frac{n}{3}\right)!m!}}.$$

Now (21) becomes

$$\begin{aligned}
&\frac{1}{2}||\tilde{\rho}-\tilde{\rho}'||_{\mathrm{tr}} = \frac{1}{2^{N(n+m)}}\mathrm{tr}\left(\sum_{\substack{r\in\{0,1,2\}^{N\times 1}\setminus 0_{N\times 1}\\ A\in G_{N\times(n+m)}}} a_A(a_r-a'_r)\hat{\sigma}_A\sigma_{[E_r 1_{N\times(n/3)}0_{N\times m}]}\right)\\
\leq&\frac{1}{2^{N(n+m)}}\sum_{r\in\{0,1,2\}^{N\times 1}\setminus 0_{N\times 1}}\left|\mathrm{tr}\left(a_{[E_r 1_{N\times(n/3)}0_{N\times m}]}(a_r-a'_r)\hat{\sigma}_{[E_r 1_{N\times(n/3)}0_{N\times m}]}\sigma_{[E_r 1_{N\times(n/3)}0_{N\times m}]}\right)\right|,\\
\leq&\frac{1}{2^{N(n+m)}}\sum_{r\in\{0,1,2\}^{N\times 1}\setminus 0_{N\times 1}}|a_{[E_r 1_{N\times(n/3)}0_{N\times m}]}|\cdot|a_r-a'_r|\cdot\left|\mathrm{tr}\left(\hat{\sigma}_{[E_r 1_{N\times(n/3)}0_{N\times m}]}\sigma_{[E_r 1_{N\times(n/3)}0_{N\times m}]}\right)\right|\\
\leq&2\left(3^N-1\right)\binom{\frac{n}{3}+m}{m}^{-1/2}.
\end{aligned}$$

By Theorem 14, given an evaluation circuit on N qubits, a quantum code of large enough length $n = 6\cdot 7^l$ should be used in the scheme and each codeword should be permuted with sufficiently many m maximally-mixed states so that the trace distance of two encrypted states is small for security.

Theorem 15. *For a security parameter κ, let $N=\kappa$, $l=\left\lceil\frac{\ln 2\kappa}{\ln 7}\right\rceil$, and $m = 2\cdot 7^l$. Then IQPP is an IT-secure QHE scheme for IQP$^+$ circuits such that for $C\in IQP^+_\kappa$ and $\rho,\rho'\in D_{xy}(\mathbb{C}^2)^{\otimes\kappa}$:*

$$\left\|\mathbb{E}_\pi\left\{\mathit{IQPP.Encrypt}_\pi(\rho)\right\}-\mathbb{E}_\pi\left\{\mathit{IQPP.Encrypt}_\pi(\rho')\right\}\right\|_{\mathrm{tr}}\leq e^5\kappa e^{-\kappa\ln 3}.$$

Proof. – (Correctness) From the construction of IQPP, for $C\in \mathrm{IQP}^+_\kappa$ with input $\rho\in D_{xy}(\mathbb{C}^2)^{\otimes\kappa}$, it is clear that for any security parameter κ, and $\pi\leftarrow\mathsf{IQPP.KeyGen}(1^\kappa)$, we have

$$\left\|\mathbb{E}_\pi\left\{\mathsf{IQPP.Decrypt}_\pi(\mathsf{IQPP.Eval}(C,\mathsf{IQPP.Encrypt}_\pi(\rho)))\right\}-\mathbb{E}_\pi\left\{C(\rho)\right\}\right\|_{\mathrm{tr}}=0,$$

since there is no randomness except the measurement outcomes and the distribution of measurement outcomes remains the same after encryption. Thus IQPP is homomorphic for IQP$^+$.

– (Compactness) F is compact if there exists a polynomial p such that for any $C\in\mathfrak{C}^\kappa_{\mathsf{F}}$, the circuit complexity of applying $\mathsf{F.Decrypt}$ to the output of $\mathsf{F.Eval}_C$ is at most $p(\kappa)$.
Given a QHE task on IQP$^+$ circuits with κ input qubits, the decryption algorithm IQPP.Decrypt performs κ permutations and at most κ classical decoding, and at most κ quantum decoding. Each permutation takes at most $2\cdot 7^l+m=O(\kappa)$ CNOTs and consequently these permutations take a total of $O(\kappa^2)$ CNOTs. Since there are no physical errors, the errors introduced by noisy encoding are correctable errors. Thus each classical or quantum decoding takes $O(\mathrm{poly}(n))=O(\mathrm{poly}(\kappa))$ steps. Consequently the total complexity of performing IQPP.Decrypt is $O(\mathrm{poly}(\kappa))$, which is independent of the circuit size. Thus IQPP is compact.

– (Security) Recall the Stirling's approximation

$$\sqrt{2\pi n}n^n e^{-n} < n! < \sqrt{2\pi n}n^n e^{-n+1}.$$

We have

$$\binom{n/3+m}{m} \geq \frac{(n/3+m)^{n/3+m+1/2}}{e^2\sqrt{2\pi}(n/3)^{n/3+1/2}m^{m+1/2}} = \frac{\sqrt{3}}{e^2\sqrt{\pi n}}2^{2n/3}.$$

Then by Lemma 14,

$$\begin{aligned}
&\left\|\mathbb{E}_\pi\left\{\mathsf{IQPP.Encrypt}_\pi(\rho)\right\} - \mathbb{E}_\pi\left\{\mathsf{IQPP.Encrypt}_\pi(\rho')\right\}\right\|_{\mathrm{tr}} \\
\leq& 2e(3^N-1)(\pi n/3)^{1/4}2^{-n/3} \\
\leq& e^4 7^{l/4} e^{N\ln 3 - 2\cdot 7^l \ln 2} \\
\leq& e^5 \kappa e^{-\kappa \ln 3}.
\end{aligned}$$

Thus IQPP is IT-secure by Definition 6.

□

Acknowledgements

We thank Si-Hui Tan for introducing their work [40] to us. CYL would like to thank Todd B. Brun, Nai-Hui Chia, and Wei-Kai Lin for helpful discussions. KMC acknowledges helpful discussions with Salil P. Vadhan. KMC was partially supported by 2016 Academia Sinica Career Development Award under Grant no. 23-17 and the Ministry of Science and Technology, Taiwan under Grant no. MOST 103-2221- E-001-022-MY3.

References

1. Aliferis, P., Brito, F., Di Vincenzo, D.P., Preskill, J., Steffen, M., Terhal, B.M.: Fault-tolerant computing with biased-noise superconducting qubits: a case study. New J. Phys. 11(1), 013061 (Jan 2009)
2. Ambainis, A., Mosca, M., Tapp, A., Wolf, R.D.: Private quantum channels. In: Proceedings of the 41st Annual Symposium on Foundations of Computer Science. pp. 547–553 (2000)
3. Ambainis, A., Nayak, A., Ta-Shma, A., Vazirani, U.: Dense quantum coding and quantum finite automata. JACM 49(4), 496–511 (Jul 2002)
4. Anderson, J.T., Duclos-Cianci, G., Poulin, D.: Fault-tolerant conversion between the steane and reed-muller quantum codes. Phys. Rev. Lett. 113, 080501 (Aug 2014)
5. Barnum, H., Crepeau, C., Gottesman, D., Smith, A., Tapp, A.: Authentication of quantum messages. In: The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings. pp. 449–458 (2002)
6. Baumeler, Ä., Broadbent, A.: Quantum private information retrieval has linear communication complexity. Journal of Cryptology 28(1), 161–175 (2015)

7. Ben-Or, M., Crepeau, C., Gottesman, D., Hassidim, A., Smith, A.: Secure multiparty quantum computation with (only) a strict honest majority. In: 2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06). pp. 249–260 (Oct 2006)
8. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing. vol. 175, p. 8. New York (1984)
9. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: Proceedings of the 2011 IEEE 52Nd Annual Symposium on Foundations of Computer Science. pp. 97–106. FOCS '11, IEEE Computer Society, Washington, DC, USA (2011)
10. Bravyi, S., Haah, J.: Magic-state distillation with low overhead. Phys. Rev. A 86, 052329 (Nov 2012)
11. Bravyi, S., Kitaev, A.: Universal quantum computation with ideal clifford gates and noisy ancillas. Phys. Rev. A 71, 022316 (Feb 2005)
12. Bremner, M.J., Jozsa, R., Shepherd, D.J.: Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy. Proc. R. Soc. A 467(2126), 459–472 (2010)
13. Bremner, M.J., Montanaro, A., Shepherd, D.J.: Achieving quantum supremacy with sparse and noisy commuting quantum computations, Quantum 1, 8 (2017).
14. Bremner, M.J., Montanaro, A., Shepherd, D.J.: Average-case complexity versus approximate simulation of commuting quantum computations. Phys. Rev. Lett. 117, 080501 (Aug 2016)
15. Broadbent, A., Fitzsimons, J., Kashefi, E.: Universal blind quantum computation. In: Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on. pp. 517–526 (Oct 2009)
16. Broadbent, A., Gutoski, G., Stebila, D.: Quantum one-time programs. In: Canetti, R., Garay, J.A. (eds.) Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II. pp. 344–360. Springer Berlin Heidelberg, Berlin, Heidelberg (2013)
17. Broadbent, A., Jeffery, S.: Quantum homomorphic encryption for circuits of low T-gate complexity. In: Gennaro, R., Robshaw, M. (eds.) Advances in Cryptology – CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II. pp. 609–629. Springer Berlin Heidelberg, Berlin, Heidelberg (2015)
18. Brun, T.A., Zheng, Y.C., Hsu, K.C., Job, J., Lai, C.Y.: Teleportation-based fault-tolerant quantum computation in multi-qubit large block codes (2015), `http://arxiv.org/abs/1504.03913`
19. Calderbank, A.R., Shor, P.W.: Good quantum error-correcting codes exist. Phys. Rev. A 54(2), 1098–1105 (1996)
20. Childs, A.M.: Secure assisted quantum computation. Quant. Inf. Comp. 5(6), 456–466 (2005)
21. Chor, B., Kushilevitz, E., Goldreich, O., Sudan, M.: Private information retrieval. JACM 45(6), 965–981 (Nov 1998)
22. van Dijk, M., Gentry, C., Halevi, S., Vaikuntanathan, V.: Fully homomorphic encryption over the integers. In: Gilbert, H. (ed.) Advances in Cryptology – EUROCRYPT 2010: 29th Annual International Conference on the Theory and Applications of Cryptographic Techniques, French Riviera, May 30 – June 3, 2010. Proceedings. pp. 24–43. Springer Berlin Heidelberg, Berlin, Heidelberg (2010)
23. DiVincenzo, D.P., Shor, P.W.: Fault-tolerant error correction with efficient quantum codes. Phys. Rev. Lett. 77(15), 3260–3263 (1996)

24. Dulek, Y., Schaffner, C., Speelman, F.: Quantum homomorphic encryption for polynomial-sized circuits. In: Robshaw, M., Katz, J. (eds.) Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III. pp. 3–32. Springer Berlin Heidelberg, Berlin, Heidelberg (2016)
25. Eastin, B., Knill, E.: Restrictions on transversal encoded quantum gate sets. Phys. Rev. Lett. 102, 110502 (Mar 2009)
26. Fujii, K.: Noise threshold of quantum supremacy (2016), https://arxiv.org/abs/1610.03632
27. Gaitan, F.: Quantum error correction and fault tolerant quantum computing. CRC Press, Boca Raton, FL (2008)
28. Gao, X., Wang, S.T., Duan, L.M.: Quantum supremacy for simulating a translation-invariant Ising spin model. Phys. Rev. Lett. 118, 040502 (Jan 2017)
29. Gentry, C.: Fully homomorphic encryption using ideal lattices. In: Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing. pp. 169–178. STOC '09, ACM, New York, NY, USA (2009)
30. Gottesman, D.: Stabilizer codes and quantum error correction. Ph.D. thesis, California Institute of Technology, Pasadena, CA (1997)
31. Gottesman, D.: The Heisenberg Representation of Quantum Computers (1998), https://arxiv.org/abs/quant-ph/9807006v1
32. Jochym-O'Connor, T., Laflamme, R.: Using concatenated quantum codes for universal fault-tolerant quantum gates. Phys. Rev. Lett. 112, 010505 (Jan 2014)
33. Kitaev, A.Y.: Quantum computations: algorithms and error correction. RUSS. MATH. SURV. 52(6), 1191–1249 (1997)
34. Lai, C.Y., Lu, C.C.: A construction of quantum stabilizer codes based on syndrome assignment by classical parity-check matrices. IEEE Trans. Inf. Theory 57(3), 7163 – 7179 (2011)
35. Liang, M.: Symmetric quantum fully homomorphic encryption with perfect security. Quant. Inf. Proc. 12(12), 3675–3687 (2013)
36. Liang, M.: Quantum fully homomorphic encryption scheme based on universal quantum circuit. Quant. Inf. Proc. 14(8), 2749–2759 (2015)
37. Nayak, A.: Optimal lower bounds for quantum automata and random access codes. In: Foundations of Computer Science, 1999. 40th Annual Symposium on. pp. 369–376 (1999)
38. Newman, M., Shi, Y.: Limitations on Transversal Computation through Quantum Homomorphic Encryption (2017), http://arxiv.org/abs/1704.07798
39. Nielsen, M.A., Chuang, I.L.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge, UK (2000)
40. Ouyang, Y., Tan, S.H., Fitzsimons, J.: Quantum homomorphic encryption from quantum codes (2015), http://arxiv.org/abs/1508.00938
41. Paetznick, A., Reichardt, B.W.: Universal fault-tolerant quantum computation with only transversal gates and error correction. Phys. Rev. Lett. 111, 090505 (Aug 2013)
42. Qiang, X., Loke, T., Montanaro, A., Aungskunsiri, K., Zhou, X., OBrien, J.L., Wang, J.B., Matthews, J.C.F.: Efficient quantum walk on a quantum processor. Nat. Commun. 7(11511) (2016)
43. Rohde, P.P., Fitzsimons, J.F., Gilchrist, A.: Quantum walks with encrypted data. Phys. Rev. Lett. 109, 150501 (Oct 2012)
44. Shannon, C.: Communication theory of secrecy systems. Bell Systems Techn. Journal 28, 656–719 (1949)

45. Shepherd, D., Bremner, M.J.: Temporally unstructured quantum computation. Proc. R. Soc. A 465(2105), 1413–1439 (2009)
46. Shor, P.W.: Algorithms for quantum computation: discrete logarithm and factoring. In: Proceedings of the 35th Annual Symposium on the Theory of Computer Science. p. 124. IEEE Computer Society Press, Los Alamitos (1994)
47. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 85, 441–444 (Jul 2000)
48. Steane, A.M.: Multiple particle interference and quantum error correction. Proc. R. Soc. London A 452, 2551–2576 (1996)
49. Tan, S.H., Kettlewell, J.A., Ouyang, Y., Chen, L., Fitzsimons, J.F.: A quantum approach to homomorphic encryption (2014), `https://arxiv.org/abs/1411.5254`
50. Vaikuntanathan, V.: Computing blindfolded: New developments in fully homomorphic encryption. In: Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on. pp. 5–16 (Oct 2011)
51. Yu, L., Pérez-Delgado, C.A., Fitzsimons, J.F.: Limitations on information-theoretically-secure quantum homomorphic encryption. Phys. Rev. A 90, 050303 (Nov 2014)
52. Zeng, B., Cross, A., Chuang, I.: Transversality versus universality for additive quantum codes. IEEE Trans. Inf. Theory 57(9), 6272–6284 (Sept 2011)

A Logical Operations of $\mathcal{Q}_6$

A logical CNOT within a codeword of $\mathcal{Q}_6$ is more tricky. Let $\overline{C_1X_2}$ denote the logical CNOT from information qubit 1 to information qubit 2, and similar for $\overline{C_2X_1}$. We will say that $\overline{C_1X_2}$ and $\overline{C_2X_1}$ are logical *inner* CNOT gates.

Proposition 16. *(a) $\overline{C_1X_2}$ can be implemented by swapping qubits 1 and 2 within a codeword.*
(b) $\overline{C_2X_1}$ can be implemented by the circuit in Fig. 10.

Proof. (a) Consider the computation basis (7)-(10). If qubits 1 and 2 are swapped, $|\overline{00}\rangle$ and $|\overline{01}\rangle$ are unchanged, while $|\overline{10}\rangle$ and $|\overline{11}\rangle$ are swapped. This implements $\overline{C_1X_2}$.

(b) Consider the quantum circuit in Fig. 10. It can be checked that the parity of qubits $2, 3, 4$ is used to control the application logical X_1. □

Note that $\overline{C_2X_1}$ cannot be implemented in our QHE scheme since qubits 5 and 6 are hidden from the server. If one tries to apply a transversal CNOT on the permuted qubits, the information will be corrupted by the random states of the appended ancillas.

The transversal Hadamard gate implements the logical Hadamard on the first qubit up to some correction.

Lemma 17. *The logical Hadamard gate on the first logical qubit of the $[[6, 2]]$ code $\mathcal{Q}$ can be implemented by*

$$\bar{H}_1 = H^{\otimes 6}\overline{C_2X_1}\,\overline{C_1X_2}, \tag{22}$$

where $\overline{C_1X_2}$ and $\overline{C_2X_1}$ are demonstrated in Proposition 16.

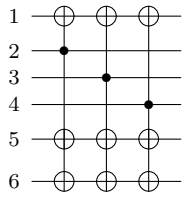

Fig. 10. The circuit for implementation of $\overline{C_2X_1}$ within a codeword of the $[[6,2]]$ code (the top six qubits).

Proof. First, the transversal Hadamard $H^{\otimes 6}$ preserves the code space, since the stabilizer group is unchanged under conjugation by $H^{\otimes 6}$:

$$\begin{aligned} H^{\otimes 6} g_1 H^{\otimes 6} =& g_3, \\ H^{\otimes 6} g_2 H^{\otimes 6} =& g_4. \end{aligned}$$

Thus $H^{\otimes 6}$ is a legitimate logical operation. Observe that

$$\begin{aligned} H^{\otimes 6} \bar{X}_1 H^{\otimes 6} =& g_3 g_4 \bar{Z}_1 \bar{Z}_2, \\ H^{\otimes 6} \bar{X}_2 H^{\otimes 6} =& \bar{Z}_1, \\ H^{\otimes 6} \bar{Z}_2 H^{\otimes 6} =& g_1 g_2 \bar{X}_1 \bar{X}_2. \end{aligned}$$

Consequently,

$$H^{\otimes 6} \equiv \bar{H}_1 \bar{H}_2 \overline{C_1X_2}\, \overline{C_2X_1}. \tag{23}$$

The logical circuit of implementing $H^{\otimes 6}$ is illustrated in Fig. 11. Therefore,

$$H^{\otimes 6} \overline{C_2X_1}\, \overline{C_1X_2} \equiv \bar{H}_1 \bar{H}_2,$$

which is the desired operation since we do not care about any operation on logical qubit 2.

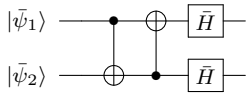

Fig. 11. The logical circuit for implementing the transversal Hadamard gate in (23) on a codeword of the $[[6,2]]$ code.

□

The transversal Hadamard gate implements the logical Hadamard gate on logical qubit 1 up to two logical inner CNOT gates. As mentioned above that $\overline{C_2X_1}$ cannot be implemented in our QHE scheme, neither can the logical H_1.