On Statistically-Secure Quantum Homomorphic Encryption

Ching-Yi Lai[1,*] and Kai-Min Chung[1]

[1] Institute of Information Science, Academia Sinica, Taipei, Taiwan 11529

Homomorphic encryption is an encryption scheme that allows computations to be evaluated on encrypted inputs without knowledge of their raw messages. Recently Ouyang *et al.* constructed a quantum homomorphic encryption (QHE) scheme for Clifford circuits with statistical security (or information-theoretic security (IT-security)). It is desired to see whether an information-theoretically-secure (ITS) quantum FHE exists. If not, what other nontrivial class of quantum circuits can be homomorphically evaluated with IT-security? We provide a limitation for the first question that an ITS quantum FHE necessarily incurs exponential overhead. As for the second one, we propose two QHE schemes for an enlarged class of the instantaneous quantum polynomial-time (IQP) circuits called IQP^+. The first scheme TRIV follows directly from the one-time pad. The second scheme IQPP is constructed from a class of concatenated quantum stabilizer codes, whose logical X and Z operators act nontrivially on different sets of qubits.

I. INTRODUCTION

Homomorphic encryption is an encryption scheme that allows computation to be evaluated on encrypted inputs without knowledge of their raw messages. An encryption scheme is typically considered as a computational primitive, since an information-theoretically-secure (ITS for short) symmetric key encryption scheme can only securely encrypt messages of length at most the length of the secret key by Shannon's impossibility result [1, 2]. However, homomorphic encryptions can be interesting even with a bounded number of encrypted messages. Unfortunately, classical ITS *fully* homomorphic encryptions do not exist [3].

In this work we investigate the possibility of ITS symmetric-key homomorphic encryptions in the quantum setting. The quantum analogue of Shannon's impossibility result says that no quantum encryption scheme with information-theoretic security (IT-security) can encrypt a message much longer than the secret key [4–6]. In light of the negative result, we consider ITS symmetric-key quantum homomorphic encryption (QHE) with bounded-message security. Such a QHE scheme is called IT N_κ bounded-message secure (IT N_κ-BMS) for a security parameter κ (see Def. 3). We remark that security with respect to chosen-plaintext attacks (CPAs) where an adversary has access to an encryption oracle is usually considered in the computational setting [7, 8]; however, CPA security cannot hold in the information-theoretic setting due to Shannon's impossibility results.

If a QHE scheme supports homomorphic evaluation of arbitrary quantum computation, it is called a quantum *fully* homomorphic encryption (QFHE) scheme. For this, homomorphic evaluation of a universal set of gates need to be implemented efficiently. It is known that *Clifford* gates together with the T gate are universal for quantum computation. The Clifford gates are composed of Hadamard, phase, and controlled-NOT $\mathrm{CNOT} = |0\rangle\langle 0|\otimes I + |1\rangle\langle 1|\otimes X$. (Pauli matrices are denoted by I, X, Y, and Z.)

In the computational setting, there has been an exciting development of QHE, initiated by the seminal work of Broadbent and Jeffery [7], who constructed (computationally secure) QHE schemes for Clifford circuits with a small number of T gates. In a recent breakthrough, Dulek, Schaffner, and Speelman [8] constructed the first (leveled) QFHE. Very recently, Alagic, Dulek, Schaffner, and Speelman [9] showed how to further achieve verifiability for QFHE, which allows verification of correctness of homomorphically evaluated ciphertexts.

A natural question is: can we build a QFHE scheme with IT-security? The possibility was first investigated by Ouyang *et al.* [10] and they showed that ITS QHE can be performed for Clifford circuits. On the other hand, it has been shown by Yu *et al.* [11] that QFHE with perfect security must incur an exponential overhead. Herein, we extend the result to QFHE with imperfect IT-security by a reduction to the communication lower bound of *quantum private information retrieval* (QPIR) [12]. (Please see Theorem 5.) This limitation is also independently observed by Newman and Shi [13]. As a consequence, an ITS QFHE does not exist.

The next question is whether we can have ITS QHE for any nontrivial class of circuits other than the Clifford circuits. In [10] a class of Calderbank-Shor-Steane (CSS) codes [14, 15] with transversal Clifford gates are used to construct an ITS QHE scheme. Quantum codes are used in the setting of fault-tolerant quantum computation [16] and quantum cryptography (e.g., [17–21]). Therefore, if we replace those CSS codes by codes with a different transversal gate set, we obtain an ITS QHE scheme for another class of circuits. For example, the triorthogonal codes [22] have transversal CNOT, T, and control-control-phase gates. (However, it is known that transversal gates alone cannot be universal for quantum codes [23, 24]. See more discussion about transversal computation in [13].)

* cylai0616@iis.sinica.edu.tw

	TRIV	IQPP
secret key	k-wise independent hash functions with $k = O(N_\kappa)$	permutations in S_n with $n = O(N_\kappa)$
fresh ciphertext	1 qubit $O(\kappa)$ classical bits	$O(N_\kappa)$ qubits
evaluated ciphertext	1 qubit $O(N_\kappa \cdot \kappa)$ classical bits	$O(N_\kappa)$ qubits

TABLE I. Comparison of IT N_κ-BMS schemes TRIV and IQPP for security error level $2^{-\kappa}$.

In this paper we show how to do QHE for a class of quantum circuits, called IQP$^+$, which is an enlarged class of the instantaneous quantum polynomial-time (IQP) circuits [25] (with additional X, Y, CNOT gates, and measurements in the Z basis). Note that the encrypted messages to IQP$^+$are restricted to the those density operators without any single Pauli Z in the Pauli decomposition. See Def. 7 and the discussions there. We will discuss a trivial scheme TRIV for IQP and show that TRIV can be extended for IQP$^+$, using additional $O(N_\kappa^2)$ bits to track the effects of additional CNOTs in IQP$^+$(see Theorem 10). Then we present a more involved scheme IQPP for IQP$^+$, constructed from CSS codes (the formal result is given in Theorem 18). We compare the two schemes for IQP$^+$circuits in Table. I. For homomorphic evaluation, IQPP needs $O(N_\kappa)$ qubits per message qubit, while TRIV needs $O(N_\kappa \cdot \kappa)$ classical bits per message qubit.

The notion of IQP computation was proposed in [25], which is not universal for quantum computation. It is known that the class of IQP with *postselection* is equivalent to the class PP [27]. Moreover, IQP computations are difficult to simulate with classical computers [27–29] unless the polynomial hierarchy collapses to the third level. Currently it is hard to implement Shor's factoring algorithm [30]. Instead, nonuniversal circuits, such as IQP, are physically more feasible so that quantum supremacy could be demonstrated [29, 31–33]. 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 by the Gottesman-Knill theorem [34].

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. III we define QHE and its properties and then provide the limitation of IT-secure QFHE in Sec. IV. In Sec. V we discuss IQP$^+$circuits and propose the QHE scheme TRIV. The complicated QHE scheme IQPP is given in Sec. VI.

II. PRELIMINARIES

A. Quantum Information Processing

We give notation and briefly introduce basics of quantum mechanics here. A quantum system will be denoted by a capital letter and its corresponding Hilbert space will be denoted by the corresponding calligraphic letter.

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 Hilbert space of a joint quantum system AB is the tensor product of the corresponding Hilbert spaces $\mathcal{A} \otimes \mathcal{B}$. We use ρ_{MR} to denote a density operator for the joint of the message (M) and reference (R) systems.

The trace distance between two quantum states ρ and σ is

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

where $||X||_{\mathrm{tr}} = \frac{1}{2}\mathrm{tr}\sqrt{X^\dagger X}$ 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

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

where $\vec{\sigma} = (\sigma_1, \sigma_2, \sigma_3)$ and $\vec{r} = (r_1, r_2, r_3) \in \mathbb{R}^3$ 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 [35] 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

$$X \otimes Y \otimes Z \otimes Z = XYZ^{\otimes 2} = X_1 Y_2 Z_3 Z_4 = Z^{0111} X^{1100}.$$

In particular, we denote by $C_i X_j$, 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 $|1\rangle$.

III. DEFINITIONS

Definition 1. A private-key quantum homomorphic qubit-encryption scheme F is defined by the following algorithms:

1) (Key generation) $\mathsf{F.KeyGen}$: $1^\kappa \to \mathcal{H}_{\mathrm{sk}} \times D(\mathcal{H}_{\mathrm{evk}})$. The algorithm takes an input of a security parameter κ and outputs a *classical* private key sk (and possibly some quantum evaluation key $\rho_{\mathrm{evk}} \in D(\mathcal{H}_{\mathrm{evk}})$).

2) (Encryption) $\mathsf{F.Enc}_{sk}$: $D(\mathbb{C}^2) \to D(\mathcal{C})$. The algorithm takes sk and a single-qubit $\rho \in D(\mathbb{C}^2)$ as input and outputs a ciphertext $\tilde{\rho} \in D(\mathcal{C})$.

3) (Evaluation) $\mathsf{F.Eval}$: $D(\mathcal{H}_{\mathrm{evk}}) \times \mathfrak{C}_\kappa \times D(\mathcal{C}^{\otimes M_\kappa}) \to D(\mathcal{C}^{\otimes M_\kappa}) \times \mathcal{M}^{\otimes M_\kappa}$, where $\mathfrak{C}_\kappa$ is a set of admissible quantum circuits for F and the security parameter κ, M_κ is the maximum number of input qubits for $\mathfrak{C}_\kappa$, and $\mathcal{M}$ is the set of corresponding homomorphic measurement outcomes.

4) (Decryption) $\mathsf{F.Dec}_{sk}$: $D(\mathcal{C}) \times \mathcal{M} \to D(\mathbb{C}^2) \times \{0,1\}$. If the measurement outcome $\mu \in \mathcal{M}$ is trivial, the algorithm takes sk and $\sigma \in D(\mathcal{C})$ as input and outputs a single-qubit quantum state $\hat{\sigma} \in D(\mathbb{C}^2)$. Otherwise, the algorithm takes sk and μ as input and outputs a bit of measurement outcome.

- (Correctness) F is *homomorphic* for $\mathfrak{C} = \cup_\kappa \mathfrak{C}_\kappa$ if there exists a negligible function $\eta(\kappa)$ such that for $sk, \rho_{\mathrm{evk}} \leftarrow \mathsf{F.KeyGen}(1^\kappa)$, $C \in \mathfrak{C}_\kappa$ on M_κ qubits, and $\rho_{MR} \in D(\mathbb{C}^{2^{M_\kappa}} \otimes \mathcal{R})$,

$$\left\| \Phi^{sk,M_\kappa}_{\mathsf{F.Dec}} \otimes \mathbb{I}_R \left(\Phi^{\rho_{\mathrm{evk}},C}_{\mathsf{F.Eval}} \otimes \mathbb{I}_R \left(\Phi^{sk,M_\kappa}_{\mathsf{F.Enc}} \otimes \mathbb{I}_R(\rho_{MR}) \right) \right) - C \otimes \mathbb{I}_R(\rho_{MR}) \right\|_{\mathrm{tr}} \le \eta(\kappa),$$

where Φ denotes the corresponding quantum operation of the underlying algorithm and R is a reference system.

- (Compactness) F is *compact* for $\mathfrak{C} = \cup_\kappa \mathfrak{C}_\kappa$ if there exists a polynomial p in κ such that for any $C \in \mathfrak{C}_\kappa$, the circuit complexity of applying $\mathsf{F.Dec}$ to the output of $\mathsf{F.Eval}_C$ is at most $p(\kappa)$.

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

Definition 2. A QHE scheme F is *information-theoretically N_κ-bounded-message-secure* (IT N_κ-BMS) if there exists a negligible function $\epsilon(\kappa)$, such that for every security parameter κ and $\rho_{MR}, \rho'_{MR} \in D(\mathbb{C}^{2^{N_\kappa}} \otimes \mathcal{R})$ with $\mathrm{tr}_M(\rho_{MR}) = \mathrm{tr}_M(\rho'_{MR})$,

$$\left\| \Phi^{sk,N_\kappa}_{\mathsf{F.Enc}} \otimes \mathbb{I}_R(\rho_{MR}) - \Phi^{sk,N_\kappa}_{\mathsf{F.Enc}} \otimes \mathbb{I}_R(\rho'_{MR}) \right\|_{\mathrm{tr}} \le \epsilon(\kappa), \tag{2}$$

where Φ denotes the corresponding quantum operation of the underlying algorithm.

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

Below is a weaker definition of IT N_κ-BMS with no reference system involved.

Definition 3. A QHE scheme F is *weak information-theoretically N_κ-bounded-message-secure* (weak IT N_κ-BMS) if there exists a negligible function $\epsilon(\kappa)$, such that for every security parameter κ and $\rho, \rho' \in D(\mathbb{C}^{2^{N_\kappa}})$,

$$\left\| \Phi^{sk,N_\kappa}_{\mathsf{F.Enc}}(\rho) - \Phi^{sk,N_\kappa}_{\mathsf{F.Enc}}(\rho') \right\|_{\mathrm{tr}} \le \epsilon(\kappa). \tag{3}$$

It is clear that Def. 2 implies Def. 3 by choosing a trivial reference system. By [6, Theorem 8], we have the following theorem.

Theorem 4. If F is a weak IT N_κ-BMS encryption scheme with security error at most $\epsilon(\kappa)$, then F is IT N_κ-BMS with security error at most $2^{2N_\kappa+1}\epsilon(\kappa)$.

IV. LIMITATION

The negative result for ITS QFHE is proved by a reduction to the communication lower bound of quantum private information retrieval (QPIR) with one server. In an (n,m) QPIR problem, Alice (the server) has a data string x of n bits and Bob wishes to learn the ith entry x_i. They create an initial state ρ_{ABR} with $\mathrm{tr}_R \rho_{ABR} = |x\rangle_A\langle x| \otimes |i\rangle_B\langle i|$

and after a two-party protocol $\mathcal{P}$ they end up with the final state $\rho'_{ABR} = \mathcal{P}(\rho_{ABR})$ by exchanging m qubits. We say that $\mathcal{P}$ has *correctness error* δ if for any ρ_{ABR} with $\mathrm{tr}_R \rho_{ABR} = |x\rangle_A\langle x| \otimes |i\rangle_B\langle i|$, there exists a measurement $\mathcal{M}$ such that

$$\Pr\left\{\mathcal{M}\left(\mathrm{tr}_{AR}(\rho'_{ARB})\right) = x_i\right\} \geq 1-\delta.$$

We say that $\mathcal{P}$ has *security error* ϵ if for any ρ_{ABR}, there exists a quantum operation $\mathcal{E}_{AR}$ such that

$$\|\mathrm{tr}_B\left(\mathcal{E}_{AR} \otimes \mathbb{I}_B(\rho_{ARB})\right) - \mathrm{tr}_B(\rho'_{ARB})\|_{\mathrm{tr}} \leq \epsilon.$$

Nayak [36, 37] proved that $m \geq (1 - H(1-\delta))n$ for $\epsilon = 0$, where $H(p)$ is the binary entropy function. This was extended to the case of $\epsilon > 0$ in [38]:

$$m \geq \left(1 - H\left(1 - \delta - 2\sqrt{\epsilon(1-\epsilon)}\right)\right) n. \tag{4}$$

We show that the existence of an ITS QFHE would contradict this communication lower bound.

Theorem 5. There is no IT N_κ-BMS QFHE for $N_\kappa = \omega(\log\kappa)$ with correctness error $\eta(\kappa) = 0.0001$ and security error $\epsilon(\kappa) = 0.0001$. Moreover, there is no IT N_κ-BMS QHE on classical circuits for $N_\kappa = \omega(\log\kappa)$ with correctness error $\eta(\kappa) = 0.0001$ and security error $\epsilon(\kappa) = 0.0001$.

Proof. Assume there is an IT N_κ-BMS QFHE scheme F for $N_\kappa = \omega(\log\kappa)$ with correctness error $\eta(\kappa) = 0.0001$ in Def. 1 and security error $\epsilon(\kappa) = 0.0001$ in Def. 3. We show that it leads to a QPIR protocol that violates the communication lower bound Eq. (4).

Suppose that F encrypts one qubit into a ciphertext of at most $p(\kappa)$ qubits and κ is sufficiently large such that

$$H\left(1 - \eta(\kappa) - 2\sqrt{\epsilon(\kappa)(1-\epsilon(\kappa))}\right) < 0.2.$$

Let $n = 100p^2(\kappa)$, which satisfies $\log n \leq N_\kappa$.

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 $C_x \in \mathfrak{C}_\kappa$ be a quantum circuit that takes an input $i \in \{1, 2, \ldots, n\}$ and outputs x_i.

The QPIR protocol is as follows. Suppose Bob wants to query an index i^* of $\log n$ bits. Using the QFHE algorithm F, he generates a key set $sk, \rho_{\mathrm{evk}} \leftarrow \mathsf{F.KeyGen}(1^\kappa)$ and then produces the cipher state $\mathsf{F.Enc}_{sk}^{\otimes \log n}(|i^*\rangle)$, which is of $p(\kappa)\log n$ qubits. Then he sends it to Alice, together with ρ_{evk}. After computing

$$\rho \triangleq \mathsf{F.Eval}(\rho_{\mathrm{evk}}, C_x, \mathsf{F.Enc}_{sk}^{\otimes \log n}(|i^*\rangle)),$$

Alice sends ρ back to Bob. By the security of IT N_κ-BMS F, Bob does not reveal his desired objective to Alice. If Alice honestly does the homomorphic evaluation, Bob would learn x_{i^*} with probability at least $1 - \eta(\kappa)$. Thus we have an $\left(n = 100p^2(\kappa), p(\kappa)(1 + \log n)\right)$ QPIR protocol with correctness error $\eta(\kappa)$ and security error $\epsilon(\kappa)$. Note that only $p(\kappa)(1 + \log n) = p(\kappa)(1 + \log 10 + 2\log p(\kappa))$ qubits are required in communication, which contradicts the communication lower bound (4) that at least $0.8n = 80p^2(\kappa)$ qubits are required.

Observe that in this proof Alice only needs to homomorphically evaluate a classical selection function. Thus the impossibility proof also rules our ITS QHE schemes for all classical circuits. $\square$

V. IQP$^+$CIRCUITS

IQP circuits are proposed in [25, 27]. We call a gate diagonal in the computational basis $(|0\rangle, |1\rangle)$ a *diagonal gate*.

Definition 6. An IQP circuit is a quantum circuit consisting of diagonal gates. The input state is the product state of some qubits in $|+\rangle$ and the output is the measurement outcomes on a specified subset of the qubits in the X basis $(|+\rangle, |-\rangle)$.

Definition 7. An IQP$^+$circuit on N qubits is composed of diagonal gates, X, Y, CNOT, and possibly some measurements in the X or Z basis at the end. The input is a product state of some qubits in

$$D_{xy}(\mathbb{C}^2) \triangleq \{\rho = \frac{I + v_x X + v_y Y}{2}, v_x^2 + v_y^2 \leq 1\}. \tag{5}$$

Note that it is always possible to shift the X, Y and $CNOT$ gates to the end of the circuit (before the measurements), since they preserve the diagonal gates by conjugation. Thus we may consider an IQP$^+$circuit as an IQP circuit followed by classical post-processing with only NOT and CNOT gates.

Remark 8. For the homomorphic encryption of IQP (IQP$^+$) circuits, we define a more general input space:

$$D_{xy}(\mathbb{C}^{2^N} \otimes \mathcal{R}) \triangleq \{\rho_{MR} \in D(\mathbb{C}^{2^N} \otimes \mathcal{R}) : \rho_{MR} = \sum_i \alpha_i A_{i,1} \otimes \cdots \otimes A_{i,N} \otimes B_i,\ A_{i,j} \in \{I, X, Y\}, B_i \in D(\mathcal{R})\}, \quad (6)$$

where $\mathcal{R}$ is a reference system.

In other words, $D_{xy}(\mathbb{C}^{2^N} \otimes \mathcal{R})$ is a collection of density operators that do not have any single Z operator in the message part of their Pauli decompositions. Similarly to Theorem 4, we have the following corollary. Then it suffices to prove that a QHE scheme for IQP (IQP$^+$) is weak IT N_κ-BMS.

Corollary 9. If F is a weak IT N_κ-BMS encryption scheme for input space $D_{xy}(\mathbb{C}^{N_\kappa})$ with security error at most $\epsilon(\kappa)$, then F is IT N_κ-BMS for input space $D_{xy}(\mathbb{C}^{N_\kappa} \otimes \mathcal{R})$ with security error at most $2^{2N_\kappa+1}\epsilon(\kappa)$.

A. Trivial QHE for IQP and IQP$^+$

Observe that an input qubit of a IQP or IQP$^+$circuit lies in the xy-plane, i.e., $|\psi\rangle = |0\rangle + e^{i\theta}|1\rangle$, which can be protected by a Z one-time pad. The symmetric-key QHE scheme TRIV is as follows.

QHE scheme for IQP circuits: TRIV

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 $C \in \text{IQP}_N$ on an N-qubit input state in $D_{xy}(\mathbb{C}^{2^N})$.

1) $\mathsf{TRIV.KeyGen}$: $1^\kappa \to h : \{0,1\}^\kappa \to \{0,1\}$, where h is uniformly drawn from a family of κ-independent hash functions H_κ (no evaluation key here).

2) $\mathsf{TRIV.Enc}$: $\mathsf{H}_\kappa \times D(\mathbb{C}^2) \to \{0,1\}^\kappa \times D(\mathbb{C}^2)$. Encryption is done by applying a Z one-time pad:
$$\mathsf{TRIV.Enc}_h(\rho) = \left(r, Z^{h(r)}\rho Z^{h(r)}\right)$$
for $\rho \in D(\mathbb{C}^2)$, where r is a random string of κ bits (encryption randomness). For an N-qubit input state, each qubit is encrypted respectively.

3) $\mathsf{TRIV.Eval}$: $\text{IQP}_N \times \{0,1\}^{N\times\kappa} \times D(\mathbb{C}^{2^N}) \to \{0,1\}^{N\times\kappa} \times D(\mathbb{C}^{2^N}) \times \{\perp,0,1\}^N$. Evaluation is trivial for diagonal gates since they commute with the encryption. Measurements in the X basis are also trivial and the outcomes are protected by the Z one-time pads.

4) $\mathsf{TRIV.Dec}_h$: $\{0,1\}^\kappa \times D(\mathbb{C}^2) \times \{\perp,0,1\} \to D(\mathbb{C}^2) \times \{\perp,0,1\}$. For $r \in \{0,1\}^\kappa$, $\sigma \in D(\mathbb{C}^2)$, and $\mu \in \{\perp,0,1\}$, if $\mu = \perp$, $\mathsf{TRIV.Dec}_h\left((r,\sigma,\mu)\right) = Z^{h(r)}\sigma Z^{h(r)}$; otherwise, $\mathsf{TRIV.Dec}_h\left((r,\sigma,\mu)\right) = h(r) \oplus \mu$.

We remark that TRIV can be adapted for IQP$^+$circuits. Since CNOT does not commute with Z and a Z on the target qubit of a CNOT will propagate to the control qubit through the CNOT, the Z pads will change correspondingly. Thus we use an additional binary $N \times N$ matrix to record the propagation of Z pads so that they can be correctly updated. Steps 3) and 4) are modified as follows.

QHE scheme for IQP$^+$circuits: TRIV

3') $\mathsf{TRIV.Eval}$: $\text{IQP}_N^+ \times \{0,1\}^{N\times\kappa} \times D(\mathcal{C}^{2^N}) \times \{0,1\}^{N\times N} \to \{0,1\}^{N\times\kappa} \times D(\mathcal{C}^{2^N}) \times \{\perp,0,1\}^N \times \{0,1\}^{N\times N}$. Evaluation is straightforward for the gates in IQP$^+$. Let W be the $N \times N$ binary identity matrix. If a CNOT with control qubit i and target qubit j is performed, $W_{i,k}$ is replaced by $W_{i,k} + W_{j,k}$ for $k = 1, \ldots, N$.

4') $\mathsf{TRIV.Dec}_h$: $[N_\kappa] \times \{0,1\}^N \times \{0,1\}^{N\times\kappa} \times D(\mathcal{C}^2) \times \{\perp, 0, 1\} \to D(\mathcal{C}^2) \times \{\perp, 0, 1\}$. For $a \in [N]$, $(W_{a1,}, \ldots, W_{a,N}) \in \{0,1\}^N$, $R = \begin{bmatrix} r_1 \\ \vdots \\ r_N \end{bmatrix} \in \{0,1\}^{N\times\kappa}$, $\sigma \in D(\mathbb{C}^2)$, and $\mu \in \{\perp, 0, 1\}$, compute

$$b = \sum_{j=1}^{N} W_{a,j} h(r_j) \mod 2.$$

If $\mu = \perp$, $\mathsf{TRIV.Dec}_h\left((a, W, R, \sigma, \mu)\right) = Z^b \sigma Z^b$; otherwise, $\mathsf{TRIV.Dec}_h\left((a, W, R, \sigma, \mu)\right) = b \oplus \mu$.

Therefore, we have the following theorem.

Theorem 10. For any polynomial N_κ in a security parameter κ, there exists an IT N_κ-BMS QHE scheme for IQP$^+$circuits with respect to the input space $D_{xy}(\mathbb{C}^{2^{N_\kappa}} \otimes \mathcal{R})$, where $\mathcal{R}$ is a reference system.

Proof. Note that TRIV has perfect correctness. Compactness is also straightforward. We prove the security as follows.

Let $R = \begin{bmatrix} r_1 \\ \vdots \\ r_{N_\kappa} \end{bmatrix} \in \{0,1\}^{N_\kappa\times\kappa}$. For $\rho_{AR}, \rho'_{AR} \in D_{xy}(\mathbb{C}^{2^{N_\kappa}} \otimes \mathcal{R})$,

$$\left\| \Phi^{h,N_\kappa}_{\mathsf{TRIV.Enc}} \otimes \mathbb{I}_R \left(\rho_{AR}\right) - \Phi^{h,N_\kappa}_{\mathsf{TRIV.Enc}} \otimes \mathbb{I}_R (\rho'_A R) \right\|_{\mathrm{tr}} \tag{7}$$

$$= \left\| \frac{1}{2^{kN_\kappa}|\mathsf{H}|} \sum_{h\in\mathsf{H}} \sum_{R\in\{0,1\}^{N_\kappa\times\kappa}} |R\rangle\langle R| \otimes Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \left(\rho_{AR}\right) Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \right.$$
$$\left. - \frac{1}{2^{kN_\kappa}|\mathsf{H}|} \sum_{h\in\mathsf{H}} \sum_{R\in\{0,1\}^{N_\kappa\times\kappa}} |R\rangle\langle R| \otimes Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \left(\rho'_{AR}\right) Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \right\|_{\mathrm{tr}}$$

$$\leq \left\| \frac{1}{2^{kN_\kappa}|\mathsf{H}|} \sum_{h\in\mathsf{H}} \sum_{\substack{R\in\{0,1\}^{N_\kappa\times\kappa} \\ r_j:\text{distinct}}} |R\rangle\langle R| \otimes Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \left(\rho_{AR}\right) Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \right.$$
$$\left. - \frac{1}{2^{kN_\kappa}|\mathsf{H}|} \sum_{h\in\mathsf{H}} \sum_{\substack{R\in\{0,1\}^{N_\kappa\times\kappa} \\ r_j:\text{distinct}}} |R\rangle\langle R| \otimes Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \left(\rho'_{AR}\right) Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \right\|_{\mathrm{tr}} \tag{8}$$
$$+ \left\| \frac{1}{2^{kN_\kappa}|\mathsf{H}|} \sum_{h\in\mathsf{H}} \sum_{\substack{R\in\{0,1\}^{N_\kappa\times\kappa} \\ r_j:\text{ not distinct}}} |R\rangle\langle R| \otimes Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \left(\rho_{AR}\right) Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \right.$$
$$\left. - \frac{1}{2^{kN_\kappa}|\mathsf{H}|} \sum_{h\in\mathsf{H}} \sum_{\substack{R\in\{0,1\}^{N_\kappa\times\kappa} \\ r_j:\text{not distinct}}} |R\rangle\langle R| \otimes Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \left(\rho'_{AR}\right) Z^{h(r_1)\cdots h(r_{N_\kappa})} \otimes \mathbb{I}_R \right\|_{\mathrm{tr}}. \tag{9}$$

Since h is a uniformly chosen N_κ-independent hash function, $h(r_1)h(r_2)\cdots h(r_{N_\kappa})$ is uniformly distributed over $\{0,1\}^{N_\kappa}$ for distinct $r_1, r_2, \ldots, r_{N_\kappa}$. Consequently, the trace norm (8) is zero since Z one-time pads have perfect correctness. Now we consider the trace norm (9). Since $\Pr\{r_i = r_j\} = 2^{-\kappa}$, by union bound,

$$\Pr\{r_j \text{ not distinct}\} \leq \binom{N_\kappa}{2} 2^{-\kappa}.$$

Thus

$$\left\|\Phi^{sk,N_\kappa}_{\mathsf{F.Enc}} \otimes \mathbb{I}_R(\rho_{MR}) - \Phi^{sk,N_\kappa}_{\mathsf{F.Enc}} \otimes \mathbb{I}_R(\rho'_{MR})\right\|_{\mathrm{tr}} \leq N_\kappa^2 2^{-\kappa} \tag{10}$$

for $\rho_{MR}, \rho'_{MR} \in D_{xy}(\mathbb{C}^{2^{N_\kappa}} \otimes \mathcal{R})$. □

VI. HOMOMORPHIC ENCRYPTION FOR IQP$^+$FROM 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 [35, 40]. Quantum Calderbank-Shor-Steane (CSS) codes [14, 15] 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 [15] with a $[[6,2]]$ CSS code $\mathcal{Q}_6$ at the top-level.

Motivated by the implementation of logical T in the Steane code [39], we observed that the implementation of a diagonal gate can be done by involving only a subset of qubits in a stabilizer code, called *support*. If the parity of the support qubits is known, the diagonal gate can be implemented correctly. However, revealing this support will induce an attack of logical Z measurement. Fortunately, this is not harmful since the input qubits of an IQP$^+$circuit lie in the xy-plane. Another issue is that for some stabilizer codes, the logical Z and X have the same support, such as the Steane code, so that a logical X attack exists simultaneously, precluding the encryption of any quantum information. Thus $\mathcal{Q}_6$ is chosen so that the supports of $\bar{X}_1$ and $\bar{Z}_1$ are different. So the main idea of IQPP is to hide the locations of the fifth and sixth qubits by randomly permuting them with additional maximally-mixed states (MMSs).

To get an infinite family of codes, we concatenate $\mathcal{Q}_6$ (top-level) with l layers of the Steane code to obtain a $[[6\cdot 7^l, 2]]$ code $\mathcal{Q}_6^{(l)}$, since the Clifford gates can be transversally implemented in the Steane code [16]. For security, each ancilla is initialized in MMS and the resulting encoding procedure is called *noisy encoding*.

In the following subsections we will explain these ideas in detail and then we present our QHE scheme IQPP for IQP$^+$circuits in Sec. VI F.

A. Steane Code

The $[[7,1,3]]$ Steane code is defined by the following stabilizer generators

$$\begin{aligned}
g_1 &= X_1X_2X_6X_7, \;\; g_4 = Z_1Z_2Z_6Z_7,\\
g_2 &= X_1X_3X_5X_7, \;\; g_5 = Z_1Z_3Z_5Z_7,\\
g_3 &= X_1X_4X_5X_6, \;\; g_6 = Z_1Z_4Z_5Z_6.
\end{aligned}$$

Its logical Pauli operators are $\bar{X} = X^{\otimes 7}$, $\bar{Z} = Z^{\otimes 7}$.

Clifford gates can be transversally implemented in the Steane code [16]. 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. 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. Let

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

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

Proposition 11. The logical $R(\theta)$ gate in the Steane code can be implemented by

$$\bar{R}(\theta) = (C_2X_3)(C_3X_7)R_7(\theta)(C_3X_7)(C_2X_3). \tag{11}$$

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

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

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

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

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. 1 is used to implement the logical $R(\theta)$ gate, which generalizes the implementation of the logical T gate in [39]. Similarly, the circuit in Fig. 2 is used to implement the logical $CR(\theta)$ gate.

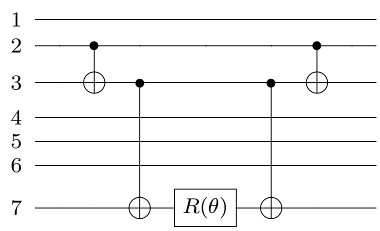

FIG. 1. The circuit implementation of the logical $R(\theta)$ gate in the Steane code.

Proposition 12. The logical $CR(\theta)$ gate between two codewords (qubits numbered from 1 to 14) of the Steane code can be implemented by

$$\overline{C_1R_2}(\theta) = (C_2X_3)(C_9X_{10})(C_3X_7)(C_{10}X_{14})C_7R_{14}(\theta)(C_{10}X_{14})(C_3X_7)(C_9X_{10})(C_2X_3). \tag{12}$$

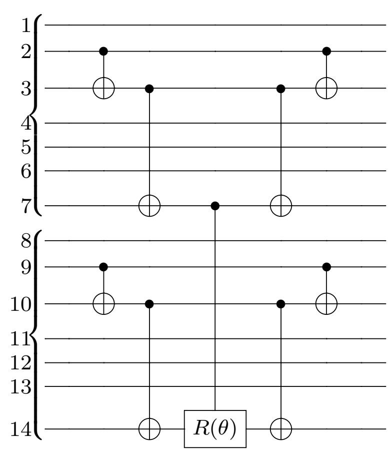

FIG. 2. The circuit implementation of the logical $CR(\theta)$ gate between two codewords of the Steane code.

Remark 13. A logical diagonal gate involving more codewords of the Steane code can be implemented similarly by decoding first the parity of each codeword, performing the diagonal gate, and then reversing the decoding.

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

Consider a Clifford unitary encoding operator U_6 such that

$$\begin{array}{ll} U_6X_1U_6^\dagger = XIIIXX & U_6Z_1U_6^\dagger = ZZIIII, \\ U_6X_2U_6^\dagger = XXIIII & U_6Z_2U_6^\dagger = IZZZII, \\ U_6X_3U_6^\dagger = XXXIXI & U_6Z_3U_6^\dagger = IIZIII, \\ U_6X_4U_6^\dagger = XXIXIX & U_6Z_4U_6^\dagger = IIIZII, \\ U_6Z_5U_6^\dagger = ZZZIZI & U_6X_5U_6^\dagger = IIIIXI, \\ U_6Z_6U_6^\dagger = ZZIZIZ & U_6X_6U_6^\dagger = IIIIIX. \end{array} \tag{13}$$

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

$$g_1 = U_6X_3U_6^\dagger, g_2 = U_6X_4U_6^\dagger, g_3 = U_6Z_5U_6^\dagger, g_4 = U_6Z_6U_6^\dagger,$$

and the logical Pauli operators are $\bar{X}_1 = U_6X_1U_6^\dagger$, $\bar{X}_2 = U_6X_2U_6^\dagger$, $\bar{Z}_1 = U_6Z_1U_6^\dagger$, and $\bar{Z}_2 = U_6Z_2U_6^\dagger$.

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 important. (More precisely, the second logical qubit is chosen to be the maximally-mixed state $\frac{1}{2}I$ for security.) 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 [16]. 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. 3 and 4, respectively.

Proposition 14. The logical $R(\theta)$ gate on the first logical qubit of a codeword of $\mathcal{Q}_6$ can be implemented by

$$\bar{R}_1(\theta) = (C_1X_2)R_2(\theta)(C_1X_2). \tag{14}$$

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,

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

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

$$\overline{C_1R_2}(\theta) = (C_1X_2)(C_7X_8)C_2R_8(\theta)(C_7X_8)(C_1X_2). \tag{15}$$

Remark 16. A logical diagonal gate involving more codewords of $\mathcal{Q}_6$ can be implemented similarly by decoding first the parity of each codeword, performing the diagonal gate, and then reversing the decoding.

C. 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 $[[n_un_b,k]]$ [41] and its codewords are codewords of $\mathcal{Q}(\mathcal{S}_u)$ built on logical qubits of $\mathcal{Q}(\mathcal{S}_b)$.

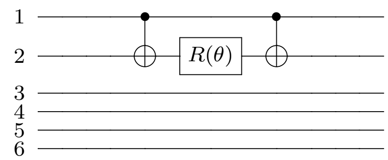

FIG. 3. The circuit that implements $\bar{R}_1(\theta)$ for the $[[6,2]]$ code $\mathcal{Q}_6$. Note that only the first two qubits are involved.

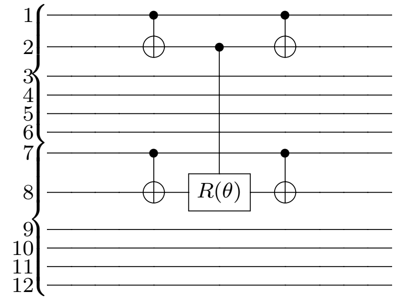

FIG. 4. The circuit that implements a logical $CR(\theta)$ gate between the first logical qubits of two codewords of the $[[6,2]]$ code $\mathcal{Q}_6$.

One can find a set of stabilizer generators of $\mathcal{Q}$ of the following 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 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

$$\begin{aligned} \bar{X}_1^{(l)} &= X^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} X^{\otimes 7^l} X^{\otimes 7^l}, \\ \bar{Z}_1^{(l)} &= Z^{\otimes 7^l} Z^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l}, \\ \bar{Y}_1^{(l)} &= (-1)^l Y^{\otimes 7^l} Z^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} X^{\otimes 7^l} X^{\otimes 7^l}. \end{aligned} \tag{16}$$

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 15, with the gates being replaced by the logical gates of a lower-layer code, recursively. For example, the $R(\theta)$ gate in Fig. 3 is implemented by the circuit in Fig. 1 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 $\mathcal{Q}_6^{(l)}$.

D. 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 modify these eigenvalues. This is done by padding ancillas in the maximally-mixed states. This is similar to applying quantum one-time pad [4] to the ancillas before encoding. As a result, the density operator of the initial state becomes $|\psi\rangle\langle\psi| \otimes (\frac{1}{2}I)^{\otimes 5}$ and the encoded state is

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

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*[26]. 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 $\rho = \frac{I+v_1X+v_2Y+v_3Z}{2}$ by $U_6^{(l)}$ is

$$U_6^{(l)}\left(\rho\otimes(\frac{1}{2}I)^{\otimes(6\cdot 7^l-1)}\right)U_6^{(l)\dagger} = \frac{1}{2}\left(I^{\otimes(6\cdot 7^l)} + v_1 X^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} X^{\otimes 7^l} X^{\otimes 7^l} \right.$$
$$+ v_2 Y^{\otimes 7^l} Z^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} X^{\otimes 7^l} X^{\otimes 7^l}$$
$$\left. + v_3 Z^{\otimes 7^l} Z^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l} I^{\otimes 7^l}\right) \tag{17}$$

according to (16). As we mentioned before, the noisy encoding is recoverable, and we have

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

E. Permutation on the Qubits

The information-theoretic security of the homomorphic encryption in [10] comes from the random qubit-permutation on the noisily-encoded quantum codeword (17) with additional maximally-mixed states $(\frac{1}{2}I)$'s. Our scheme will have a similar feature. The permutation operator will be introduced here.

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.

Let $\mathrm{SWAP}(i,j)$ denote the circuit that swaps the states of qubits i and j. It is obvious that performing $\mathrm{SWAP}(i,j)$ is equivalent to applying transposition $\tau(i,j)$ 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

$$\mathrm{Per}_\pi = \prod_i \mathrm{SWAP}(a_i,b_i) \in L(\mathbb{C}^{2^m}), \tag{18}$$

which can be implemented by a series of SWAPs.

F. QHE for IQP$^+$Circuits: IQPP

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 $\rho \in D_{xy}(\mathbb{C}^{2^N})$.

Our symmetric-key QHE scheme IQPP is as follows.

QHE scheme for IQP$^+$circuits: IQPP

---

security parameter κ
input $C \in \mathrm{IQP}_N^+$ on N qubits, and $\rho \in D_{xy}(\mathbb{C}^{2^N})$

1) $\mathsf{IQPP.KeyGen}: 1^\kappa \to S_{2m}$, where $m = 2\cdot 7^l$ and $l = \log(5N_\kappa)/\log 7$. A permutation $\pi \in S_{2m}$ is uniformly chosen as the symmetric key.

2) $\mathsf{IQPP.Enc}_\pi$: $D(\mathbb{C}^2) \to D(\mathbb{C}^{2^{4m}})$. Encryption is done by a noisy encoding of $U_6^{(l)}$ followed by a random permutation π on the last m qubits with additional m MMSs.

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

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

$$\mathcal{A}_m(\rho) = \rho \otimes (\frac{1}{2}I)^{\otimes m}. \tag{19}$$

For an N-qubit input state, each qubit is encrypted respectively.

3) $\mathsf{IQPP.Eval}$: $\mathrm{IQP}_N^+ \times D(\mathbb{C}^{2^{4mN}}) \to D(\mathbb{C}^{2^{4mN}}) \times \{\perp, 0, 1\}^{4mN}$. $\{\perp, 0, 1\}^{4mN}$ is the set of measurement outcomes. The homomorphic operation of a diagonal gate is similar to Prop. 14 and Remark 16, but with $\mathcal{Q}_6^{(l)}$ logical operations. A transversal CNOT between two codewords clearly implements an encrypted CNOT [16]. Encrypted X (Y) is simply the tensor product of the logical X (Y) of $\mathcal{Q}_6^{(l)}$ with additional $X^{\otimes m}$ $(Y^{\otimes m})$, i.e., they are bitwise implemented on the permuted qubits. Finally, encrypted measurements in the Z (X) basis are simply bitwise measurements in the Z (X) basis on the corresponding qubits.

4) $\mathsf{IQPP.Dec}_\pi$: $D(\mathbb{C}^{2^{4m}}) \times \{\perp, 0, 1\}^{4m} \to D(\mathbb{C}^2) \times \{\perp, 0, 1\}$. Decryption is done by first applying the inverse permutations on the quantum state and the measurement outcomes, and throwing out the garbage qubits and outcomes. Then apply $\mathcal{D}_6^{(l)}$ to the quantum codewords or apply a classical decoding to the measurement outcomes if an encrypted measurement is performed.

To prove the IT-security of IQPP, we need the following lemma, which results from noisy encoding and a random qubit-permutation with MMSs. The proof is similar to [10, 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 MMSs.

Lemma 17. Let $N, l \in \mathbb{Z}^+$ and $m = 2{\cdot}7^l$. Suppose $\tilde{\rho} = \frac{1}{(2m)!}\sum_{\pi \in S_{2m}} \mathsf{IQPP.Enc}_\pi(\rho)$ and $\tilde{\rho}' = \frac{1}{(2m)!}\sum_{\pi \in S_{2m}} \mathsf{IQPP.Enc}_\pi(\rho')$, where $\rho, \rho' \in D_{xy}(\mathbb{C}^{2^N})$. Then

$$\frac{1}{2}||\tilde{\rho} - \tilde{\rho}'||_{\mathrm{tr}} \le 2\left(3^N - 1\right)\binom{2m}{m}^{-1/2}. \tag{20}$$

Proof. We begin with some notation in this proof. Let

$$1_a0_b \in \{0,1\}^{a+b} \triangleq \underbrace{1\cdots1}_{a}\underbrace{0\cdots0}_{b}.$$

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

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

Thus ρ can be expressed as

$$\rho = \frac{1}{2^{3mN}} \sum_{r \in \{0,1,2\}^{N\times 1}} a_r \sigma_{r[10_{3m-1}]},$$

where $a_r \in \mathbb{C}$ with $|a_r| \le 1$ and $r[10_{3m-1}] \in \{0,1,2\}^{N\times 3m}$. Similarly,

$$\rho' = \frac{1}{2^{3mN}} \sum_{r \in \{0,1,2\}^{N\times 1}} a'_r \sigma_{r[10_{3m-1}]}.$$

Thus by (17),

$$(U_6^{(l)})^{\otimes N}(\rho - \rho')(U_6^{(l)\dagger})^{\otimes N} = \frac{1}{2^{3mN}} \sum_{r \in \{0,1,2\}^{N\times 1}\setminus 0_{N\times 1}} (a_r - a'_r)\sigma_{[E_r 1_{N\times m}]}, \tag{21}$$

where $E_r \in \{0,1,2\}^{N\times(2m)}$ 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 [35]:

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

Suppose $\frac{1}{2}||\tilde{\rho}-\tilde{\rho}'||_{\mathrm{tr}} = \mathrm{tr}M(\tilde{\rho}-\tilde{\rho}')$ for Hermitian positive operator $M \in L(\mathbb{C}^{2^{N(4m)}})$. Then we have, by (19) and (21),

$$\begin{aligned}\frac{1}{2}||\tilde{\rho}-\tilde{\rho}'||_{\mathrm{tr}} =& \mathrm{tr}M\left(\frac{1}{(2m)!}\sum_{\pi\in S_{2m}} \mathsf{IQPP.Enc}_{\pi}\left(\rho-\rho'\right)\right)\\ =&\frac{1}{2^{N(4m)}}\mathrm{tr}\tilde{M}\left(\sum_{r\in\{0,1,2\}^{N\times 1}\backslash 0_{N\times 1}} (a_r-a_r')\sigma_{[E_r 1_{N\times m} 0_{N\times m}]}\right),\end{aligned} \tag{22}$$

where

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

For $A\in\{0,1,2,3\}^{N\times(4m)}$, define

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

Let $G_{N\times(4m)}$ be a maximal subset of $\{0,1,2,3\}^{N\times(4m)}$ such that for $A,B\in G_{N\times(4m)}$, $\hat{\sigma}_A\neq\hat{\sigma}_B$ whenever $A\neq B$. Then $\tilde{M}$ can be expressed as

$$\tilde{M} = \sum_{A\in G_{N\times(4m)}} a_A\hat{\sigma}_A,$$

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 $a_{[E_r 1_{N\times m} 0_{N\times m}]}$ can be upper bounded as follows.

$$\begin{aligned}2^{N(4m)} \geq& \mathrm{tr}\tilde{M}^2 = \mathrm{tr}\sum_{A,A'\in G_{N\times(4m)}} a_A a_{A'}\hat{\sigma}_A\hat{\sigma}_{A'} \overset{(a)}{=} \sum_{A\in G_{N\times(4m)}} \mathrm{tr} a_A^2\hat{\sigma}_A^2\\ \geq& a^2_{[E_r 1_{N\times m} 0_{N\times m}]}\mathrm{tr}\hat{\sigma}^2_{[E_r 1_{N\times m} 0_{N\times m}]}\\ \overset{(b)}{=}& a^2_{[E_r 1_{N\times m} 0_{N\times m}]}\cdot(2m)!m!m!\cdot 2^{N(4m)},\end{aligned}$$

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

$$\left|a_{[E_r 1_{N\times m} 0_{N\times m}]}\right| \leq \sqrt{\frac{1}{(2m)!m!m!}}.$$

Now (22) becomes

$$\begin{aligned}
\frac{1}{2}||\tilde{\rho}-\tilde{\rho}'||_{\mathrm{tr}} =& \frac{1}{2^{N(4m)}}\mathrm{tr}\sum_{\substack{r\in\{0,1,2\}^{N\times 1}\backslash 0_{N\times 1}\\ A\in G_{N\times(4m)}}} a_A(a_r-a_r')\hat{\sigma}_A\sigma_{[E_r 1_{N\times m}0_{N\times m}]}\\
\leq& \frac{1}{2^{N(4m)}}\sum_{r\in\{0,1,2\}^{N\times 1}\backslash 0_{N\times 1}} \left|\mathrm{tr}a_{[E_r 1_{N\times m}0_{N\times m}]}(a_r-a_r')\hat{\sigma}_{[E_r 1_{N\times m}0_{N\times m}]}\sigma_{[E_r 1_{N\times m}0_{N\times m}]}\right|,\\
\leq& \frac{1}{2^{N(4m)}}\sum_{r\in\{0,1,2\}^{N\times 1}\backslash 0_{N\times 1}} \left|a_{[E_r 1_{N\times m}0_{N\times m}]}\right|\cdot|a_r-a_r'|\cdot\left|\mathrm{tr}\hat{\sigma}_{[E_r 1_{N\times m}0_{N\times m}]}\sigma_{[E_r 1_{N\times m}0_{N\times m}]}\right|\\
\leq& 2\left(3^N-1\right)\binom{2m}{m}^{-1/2}.
\end{aligned}$$

□

By Lemma 17, given an evaluation circuit on N qubits, a quantum code of large enough length $3m = 6\cdot 7^l$ 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 18. For any polynomial N_κ in a security parameter κ, there exists an IT N_κ-BMS QHE scheme for IQP$^+$circuits with respect to the input space $D_{xy}(\mathbb{C}^{2^{N_\kappa}}\otimes\mathcal{R})$ with a reference system.

Proof. Consider the QHE scheme IQPP.

- (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

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

  For $\rho,\rho'\in D_{xy}(\mathbb{C}^{2^{N_\kappa}})$, by Lemma 17,

$$\begin{aligned}
\|\mathbb{E}_\pi\{\mathsf{IQPP.Enc}_\pi(\rho)\}-\mathbb{E}_\pi\{\mathsf{IQPP.Enc}_\pi(\rho')\}\|_{\mathrm{tr}} \leq& 2e(3^{N_\kappa}-1)(\pi m)^{1/4}2^{-m}\\
\leq& e^5 N_\kappa^{-1/4}2^{-8N_\kappa}.
\end{aligned}$$

  By Corollary 9, IQPP is IT N_κ-BMS with security error at most $e^4N_\kappa^{-1/4}2^{-6N_\kappa}$ with respect to the message space with a reference system $D_{xy}(\mathbb{C}^{2^{N_\kappa}}\otimes\mathcal{R})$.

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

$$\|\mathbb{E}_\pi\{\mathsf{IQPP.Dec}_\pi(\mathsf{IQPP.Eval}(C,\mathsf{IQPP.Enc}_\pi(\rho)))\}-\mathbb{E}_\pi\{C(\rho)\}\|_{\mathrm{tr}}=0,$$

  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 $C\in\mathfrak{C}_{\mathsf{F}}^{N_\kappa}$, the circuit complexity of applying $\mathsf{F.Dec}$ to the output of $\mathsf{F.Eval}_C$ is at most $p(N_\kappa)$.

  Given a QHE task on IQP$^+$circuits with N_κ input qubits, the decryption algorithm $\mathsf{IQPP.Dec}$ performs N_κ permutations and at most N_κ classical decoding operations, and at most N_κ quantum decoding operations. Each permutation takes at most $2\cdot 7^l+m=O(N_\kappa)$ CNOTs and consequently these permutations take a total of $O(N_\kappa^2)$ CNOTs. Since there are no physical errors, the errors introduced by noisy encoding are correctable errors. Thus each classical or quantum decoding takes $O(\mathrm{poly}(n))=O(\mathrm{poly}(N_\kappa))$ steps. Consequently the total complexity of performing $\mathsf{IQPP.Dec}$ is $O(\mathrm{poly}(N_\kappa))$, which is independent of the circuit size. Thus IQPP is compact.

□

ACKNOWLEDGEMENTS

We thank Si-Hui Tan for introducing their work [10] to us. We are grateful to anonymous referees for their comments and the suggestion of the trivial scheme. 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.

[1] C. Shannon, "Communication theory of secrecy systems," *Bell Systems Techn. Journal*, vol. 28, pp. 656–719, 1949.

[2] Y. Dodis, *Shannon Impossibility, Revisited*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012, pp. 100–110.

[3] E. Kushilevitz and R. Ostrovsky, "Replication is NOT needed: SINGLE database, computationally-private information retrieval," in *38th Annual Symposium on Foundations of Computer Science, FOCS '97, Miami Beach, Florida, USA, October 19-22, 1997*, 1997, pp. 364–373.

[4] A. Ambainis, M. Mosca, A. Tapp, and R. D. Wolf, "Private quantum channels," in *Proceedings of the 41st Annual Symposium on Foundations of Computer Science*, 2000, pp. 547–553.

[5] S. P. Desrosiers and F. Dupuis, "Quantum entropic security and approximate quantum encryption," *IEEE Transactions on Information Theory*, vol. 56, no. 7, pp. 3455–3464, July 2010.

[6] C.-Y. Lai and K.-M. Chung, "Generalized Quantum Shannon Impossibility for Quantum Encryption," 2018. arXiv:1801.03656

[7] A. Broadbent and S. Jeffery, "Quantum homomorphic encryption for circuits of low T-gate complexity," in *Advances in Cryptology – CRYPTO 2015: 35th Annual Cryptology Conference, Santa Barbara, CA, USA, August 16-20, 2015, Proceedings, Part II*, R. Gennaro and M. Robshaw, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 609–629.

[8] Y. Dulek, C. Schaffner, and F. Speelman, "Quantum homomorphic encryption for polynomial-sized circuits," in *Advances in Cryptology – CRYPTO 2016: 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part III*, M. Robshaw and J. Katz, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 3–32.

[9] G. Alagic, Y. Dulek, C. Schaffner, and F. Speelman, *Quantum Fully Homomorphic Encryption With Verification*, 2017, 7th International Conference on Quantum Cryptography.

[10] Y. Ouyang, S.-H. Tan, and J. Fitzsimons, *Quantum homomorphic encryption from quantum codes*, 2015. arXiv:1508.00938

[11] L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, "Limitations on information-theoretically-secure quantum homomorphic encryption," *Phys. Rev. A*, vol. 90, p. 050303, Nov 2014.

[12] B. Chor, E. Kushilevitz, O. Goldreich, and M. Sudan, "Private information retrieval," *JACM*, vol. 45, no. 6, pp. 965–981, Nov. 1998.

[13] M. Newman and Y. Shi, *Limitations on Transversal Computation through Quantum Homomorphic Encryption*, 2017. arXiv:1704.07798

[14] A. R. Calderbank and P. W. Shor, "Good quantum error-correcting codes exist," *Phys. Rev. A*, vol. 54, no. 2, pp. 1098–1105, 1996.

[15] A. M. Steane, "Multiple particle interference and quantum error correction," *Proc. R. Soc. London A*, vol. 452, pp. 2551–2576, 1996.

[16] D. P. DiVincenzo and P. W. Shor, "Fault-tolerant error correction with efficient quantum codes," *Phys. Rev. Lett.*, vol. 77, no. 15, pp. 3260–3263, 1996.

[17] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Phys. Rev. Lett.*, vol. 85, pp. 441–444, Jul 2000.

[18] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of quantum messages," in *The 43rd Annual IEEE Symposium on Foundations of Computer Science, 2002. Proceedings.*, 2002, pp. 449–458.

[19] M. Ben-Or, C. Crepeau, D. Gottesman, A. Hassidim, and A. Smith, "Secure multiparty quantum computation with (only) a strict honest majority," in *2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06)*, Oct 2006, pp. 249–260.

[20] A. Broadbent, J. Fitzsimons, and E. Kashefi, "Universal blind quantum computation," in *Foundations of Computer Science, 2009. FOCS '09. 50th Annual IEEE Symposium on*, Oct 2009, pp. 517–526.

[21] A. Broadbent, G. Gutoski, and D. Stebila, "Quantum one-time programs," in *Advances in Cryptology – CRYPTO 2013: 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, R. Canetti and J. A. Garay, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 344–360.

[22] S. Bravyi and J. Haah, "Magic-state distillation with low overhead," *Phys. Rev. A*, vol. 86, p. 052329, Nov 2012.

[23] B. Eastin and E. Knill, "Restrictions on transversal encoded quantum gate sets," *Phys. Rev. Lett.*, vol. 102, p. 110502, Mar 2009.

[24] B. Zeng, A. Cross, and I. Chuang, "Transversality versus universality for additive quantum codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 9, pp. 6272–6284, Sept 2011.

[25] D. Shepherd and M. J. Bremner, "Temporally unstructured quantum computation," *Proc. R. Soc. A*, vol. 465, no. 2105, pp. 1413–1439, 2009.

[26] We acknowledge anonymous referees of an earlier version of this paper for the suggestion of the trivial scheme TRIV.

[27] M. J. Bremner, R. Jozsa, and D. J. Shepherd, "Classical simulation of commuting quantum computations implies collapse of the polynomial hierarchy," *Proc. R. Soc. A*, vol. 467, no. 2126, pp. 459–472, 2010.

[28] M. J. Bremner, A. Montanaro, and D. J. Shepherd, "Average-case complexity versus approximate simulation of commuting quantum computations," *Phys. Rev. Lett.*, vol. 117, p. 080501, Aug 2016.

[29] ——, "Achieving quantum supremacy with sparse and noisy commuting quantum computations," *Quantum*, vol. 1, p. 8, Apr. 2017.

[30] P. W. Shor, "Algorithms for quantum computation: discrete logarithm and factoring," in *Proceedings of the 35th Annual Symposium on the Theory of Computer Science*. Los Alamitos: IEEE Computer Society Press, 1994, p. 124.

[31] X. Qiang, T. Loke, A. Montanaro, K. Aungskunsiri, X. Zhou, J. L. OBrien, J. B. Wang, and J. C. F. Matthews, "Efficient quantum walk on a quantum processor," *Nat. Commun.*, vol. 7, no. 11511, 2016.

[32] K. Fujii, *Noise threshold of quantum supremacy*, 2016. arXiv:1610.03632 [quant-ph]

[33] X. Gao, S.-T. Wang, and L.-M. Duan, "Quantum supremacy for simulating a translation-invariant Ising spin model," *Phys. Rev. Lett.*, vol. 118, p. 040502, Jan 2017.

[34] D. Gottesman, "The Heisenberg representation of quantum computers," in *Group theoretical methods in physics. Proceedings, 22nd International Colloquium, Group22, ICGTMP'98, Hobart, Australia, July 13-17, 1998*, 1998, pp. 32–43.

[35] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. Cambridge, UK: Cambridge University Press, 2000.

[36] A. Nayak, "Optimal lower bounds for quantum automata and random access codes," in *Foundations of Computer Science, 1999. 40th Annual Symposium on*, 1999, pp. 369–376.

[37] A. Ambainis, A. Nayak, A. Ta-Shma, and U. Vazirani, "Dense quantum coding and quantum finite automata," *JACM*, vol. 49, no. 4, pp. 496–511, Jul. 2002.

[38] Ä. Baumeler and A. Broadbent, "Quantum private information retrieval has linear communication complexity," *Journal of Cryptology*, vol. 28, no. 1, pp. 161–175, 2015.

[39] T. Jochym-O'Connor and R. Laflamme, "Using concatenated quantum codes for universal fault-tolerant quantum gates," *Phys. Rev. Lett.*, vol. 112, p. 010505, Jan 2014.

[40] D. Gottesman, "Stabilizer codes and quantum error correction," Ph.D. dissertation, California Institute of Technology, Pasadena, CA, 1997.

[41] F. Gaitan, *Quantum error correction and fault tolerant quantum computing*. Boca Raton, FL: CRC Press, 2008.