A quantum approach to fully homomorphic encryption

Si-Hui Tan,1 Joshua A. Kettlewell,1 Yingkai Ouyang,1 Lin Chen,1 and Joseph F. Fitzsimons1,2 *

1Singapore University of Technology and Design, 20 Dover Drive, Singapore 138682
2Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543

(Dated: December 1, 2014)

Encryption schemes often derive their power from the properties of the underlying algebra on the symbols used. Inspired by group theoretic tools, we use the centralizer of the group of unitary operations to present a private-key quantum homomorphic encryption scheme that hides arbitrary quantum computations. A particular instance of our encoding hides information at least proportional to $m/\log m$ bits when $m$ bits are encrypted. This highlights the potential of our protocol to hide a non-trivial amount of information, and is suggestive of a large class of encodings that might yield better security.

The discovery that quantum systems could be harnessed to process data in a fundamentally new way has led to the burgeoning field of quantum information processing. This approach to computation holds the promise of more efficient algorithms for a variety of tasks including integer factorization [1], search [2] and quantum simulation [3]. However, quantum information processing has also found applications in the area of cryptography, which has been a focus of the field since the discovery of secure quantum key distribution protocols by Bennett and Brassard [4] and Ekert [5]. The information theoretic security of these protocols stands in stark contrast to the reliance of classical key agreement protocols on assumptions of computational hardness, and indeed a major goal of quantum cryptography research is to replicate and extend the functionality present in existing classical schemes while providing stronger, information theoretic, security guarantees.

In the world of classical cryptography, a central topic in recent years has been the study of homomorphic encryption [6–8]. Homomorphic encryption is a form of encryption which allows data processing to be performed on encrypted data without access to the encryption key. In general, a homomorphic encryption system is composed of four components: a key generation algorithm, an encryption algorithm that encrypts the data using the generated key, a decryption algorithm that decrypts the data using the key, and an evaluation algorithm which is used to process the data without decryption. Thus homomorphic encryption allows for secret data to be processed by third parties without allowing them access to the plaintext. After decryption, the plaintext output reveals the processed data. A scheme is termed fully homomorphic if it allows for arbitrary processing of the encrypted data. Although the idea for homomorphic encryption has existed for some time [6], it was not until 2009 that a fully homomorphic encryption scheme was discovered by Gentry [7]. Gentry’s scheme is only computationally secure, relying on the assumed hardness of certain worst-case problems over ideal lattices, and the sparse subset sum problem, although the condition requiring ideal lattices was later dropped [8].

Recent successes in quantum cryptography in finding information theoretically secure protocols for blind computation [9–14] and verifiable computing [15–18], problems closely linked to homomorphic encryption, have motivated the question of whether quantum mechanics allows for information theoretically secure fully-homomorphic encryption schemes. Indeed, a number of attempts have been made to find a quantum analogue of homomorphic encryption [19–22], however these attempts have inevitably run into a barrier. It is now known that it is not possible to achieve perfect information theoretic security while enabling arbitrary processing of encrypted data, unless the size of the encoding is allowed to grow exponentially [23]. As a result, such schemes have required interaction between parties to enable deterministic computation. These requirements parallel those of blind quantum computation which hides both the data and the computation being done on it. The question then remains as to whether information theoretically secure homomorphic encryption is possible without expanding the definition to include interactive protocols. A first step in the direction of non-interactive quantum protocols was presented in [24] for a restricted model of quantum computation known as the BosonSampling model [25] which is non-universal. Furthermore, the scheme ensures only that the encoded information and the accessible information differ by an amount proportional to $\log_2 m$ bits when $m$ bits are encrypted, which is a relatively weak security guarantee. An information-theoretically secure scheme that allows for arbitrary processing of encrypted data is not known to date, and is the focus of the present paper.

In this paper, we present what we believe to be the first known private-key homomorphic encryption protocol that supports universal classical or quantum computation while providing information theoretic security guarantees. The protocol we present ensures a gap between the information accessible to an adversary and actual information encoded that grows as $m/\log_2 m$ bits when $m$ bits are encrypted. This is a significantly stronger security guarantee than that offered by the scheme presented in [24], which offers only limited com-
putation on encrypted data. We present our results in three parts. First we present a general approach to homomorphic encryption stemming from the group theoretic structure of quantum operations. We then present a family of operations which allow universal computation on encrypted data for a broad class of encryption schemes satisfying certain symmetry constraints. Finally we present a concrete encoding satisfying these constraints and show that it limits the accessible information as described above.

**Group theoretic approach** — We approach the problem of creating a homomorphic encryption scheme via the most naive route: we try to construct a set of encryption operations which commute with the operations used to implement computation on the encrypted data. However, this approach immediately encounters a barrier when applied to the case of universal computation. In such a case the computation operations form a group, either the unitary group in the case of quantum computation or the symmetric group in the case of classical reversible computation, which does not usually commute with other operations. Indeed, any irreducible representation of these groups only commutes with operators proportional to the identity, precluding non-trivial encryption. However, for reducible representations of these groups, there can exist non-trivial operators which commute with the entire group. This provides a natural route to constructing a homomorphic encryption scheme which allows the evaluation of operators chosen from some group $G$ on encrypted data, by choosing a representation of the group with a non-trivial centralizer. In the case where the group has a trivial center, this means that the operations used to perform the computation must form a subgroup of a larger group from which the centralizer elements are drawn. While it is not immediately obvious that encryption operations chosen from the centralizer of some reducible representation of $G$ should actually be able to hide information, the BosonSampling scheme presented in [24] provides an example of such an encoding where a non-trivial amount of information is hidden.

**Representation of computation** — We now construct a specific reducible representation of the unitary group, by providing a set of logic gates which generate it. This representation of $U(n^m)$ is a subgroup of the group of unitary transformations of all $nm$ particles, in which it has a centralizer with a large number of independent elements. Later we will present an explicit encryption scheme built from elements of the centralizer of this subgroup, however we note that the gates we present now are compatible with any choice of encryption operators from the centralizer of this subgroup and not only with the specific scheme we explore in this paper.

In order to construct a reducible representation of the unitary group, we draw inspiration from the multi-rail qudit encoding prevalent in quantum optics [26]. Let us consider $nm$ bosonic particles, each with $d$ internal states, partitioned into sets of $n$ particles. Each set is used to represent a logical qudit of $n$ levels. We consider a plaintext of $m$ distinct $n$-dits, each one of which is encoded in a unique set of $n$ particles. The state of the particle at site position $x$ is given by $|a\rangle_x = \hat{a}^\dagger_{x,\alpha} |\text{vac}\rangle$, where the creation and annihilation operators satisfy $[\hat{a}_{x,\alpha}, \hat{a}^\dagger_{y,\beta}] = \delta_{\alpha,\beta} \delta_{x,y}$, and $\alpha$ labels the internal state of the particle for $0 \leq \alpha \leq d-1$. The internal states of the bosonic particles give them some degree of distinguishability [27]—a feature which will be utilized for the evaluation.

For the evaluation, a qudit is a state in $\mathbb{C}^n$ and the plaintext is represented on an $m$-qudit state in the tensor product space $(\mathbb{C}^n)^\otimes m$. A local gate acting on a single qudit lies in $U(n)$ and as there is more than one particle used to represent the qudit, we are working in a reducible representation of this group, a necessity as discussed earlier. The computational basis of the qudit is formed by the state of the $n$ particles with their respective sites labeled by the tuples $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$,

$$|\alpha_\mathbf{x}\rangle = |\alpha_1\rangle_{x_1} |\alpha_2\rangle_{x_2} \ldots |\alpha_n\rangle_{x_n},$$

where $0 \leq \alpha_1, \ldots, \alpha_n \leq d-1$. Each qudit acts as an $n$-dimensional oscillator and there are $d$ types of bosons for each site. We shall use the boson realization of the $U(n)$ algebra [28–30] to describe the generators of local qudit gates for realizing computation on the encrypted data. The operators

$$\hat{C}_{x,y} := \sum_{\alpha=0}^{d-1} \hat{a}^\dagger_{x,\alpha} \hat{a}_{y,\alpha},$$

for $1 \leq x, y \leq n$, form the set of generators for $U(n)$. One can verify that the following commutator relations are satisfied for $\{\hat{C}_{x,y}\}$: $[\hat{C}_{x,y}, \hat{C}_{w,v}] = \delta_{y,w} \hat{C}_{x,v} - \delta_{x,v} \hat{C}_{w,y}$.

To produce any $m$-qudit quantum gate which lies in $U(n^m)$, we need an imprimitive 2-qudit gate together with the set of single qudit gates. A two-qudit gate is primitive if it maps separable states to separable states, and imprimitive otherwise. The following theorem from [31] establishes that the addition of any imprimitive gate suffices to generate a representation of $U(n^m)$.

**Theorem 1**: The collection of all single-qudit gates and any imprimitive two-qudit gate is universal.

Let $S(\alpha, \beta)_{x,y}$ be a representation of the unitary SWAP operator that swaps two particles at positions $x$ and $y$ given by

$$S(\alpha, \beta)_{x,y} = \frac{1}{2} \sum_{\alpha, \beta=0}^{d-1} |s(\alpha, \beta)\rangle_{x,y} \langle s(\alpha, \beta)|$$

$$- \frac{1}{2} \sum_{\alpha, \beta=0}^{d-1} |a(\alpha, \beta)\rangle_{x,y} \langle a(\alpha, \beta)|$$
where \( |s(\alpha, \beta)\rangle_{x,y} = \frac{1}{\sqrt{2}} (|\alpha, \beta\rangle + |\beta, \alpha\rangle)_{x,y} \), and the subscripts label the sites.

For the particles of two qudits at \( x \) and \( y \) given by \( |\alpha\rangle_x |\beta\rangle_y \), we define the following 2-qudit gate to be the SWAP gate:

\[
N(\alpha, \beta)_{x,y}^{(n)} = \frac{1}{\sqrt{2}} \left( I + i \bigotimes_{k=1}^{n} S(\alpha_k, \beta_k)_{x_k, y_k} \right).
\]

We now show that this gate is an imprimitive 2-qudit gate (see Fig. 1).

**Lemma 1:** \( N(\alpha, \beta)_{x,y}^{(n)} \) is an imprimitive 2-qudit gate.

Proof: Consider the action of \( N(\alpha, \beta)_{x,y}^{(n)} \) on the separable state \( |\alpha\rangle_x |\beta\rangle_y \):

\[
N(\alpha, \beta)_{x,y}^{(n)} |\alpha\rangle_x |\beta\rangle_y = \frac{1}{\sqrt{2}} \left( |\alpha\rangle_x |\beta\rangle_y + i |\beta\rangle_x |\alpha\rangle_y \right).
\]

The resulting state is not separable unless \( |\beta\rangle = |\alpha\rangle \). As such, \( N(\alpha, \beta)_{x,y}^{(n)} \) is an imprimitive gate.

It follows from Theorem 1 and Lemma 1 that the collection of \( N(\alpha, \beta)_{x,y}^{(n)} \) and all single qudit gates, implemented as in [32], is universal. We now present an encryption scheme for which the encryption and decryption procedures commute with all local qudit gates and with \( N(\alpha, \beta)_{x,y}^{(n)} \).

**Encoding scheme** — For the encryption operation, a unitary operator, \( \mathcal{E} \), which only acts on the internal state of the constituent particles, is applied on each of the \( m \) partitions. Any \( \mathcal{E} \) which acts symmetrically on the particles in each set will commute with the representation of \( U(n^m) \) described above. However, here we focus on one particular choice of encoding. For our encoding, we set the number of particles per qudit to be the same as the number of internal states per particle, i.e., \( n = d \). A schematic of this encoding scheme is shown in Fig. 2.

First, we define the logical basis of the qudits to be

\[
|\alpha\rangle_L = \bigotimes_{\ell=0}^{d-1} |\alpha + \ell (\text{mod } d)\rangle_x
\]

for \( \alpha = 0, \ldots, d - 1 \), where the subscript \( L \) has been used to distinguish the logical state of the qudit from those of the individual particles. Note that this basis can be generated from \( |0\rangle_L \) via a repeated application of \( \hat{L} = \hat{s} \otimes \hat{d} \), where \( \hat{s} \) is a cyclic shift operation on the internal state of each particle such that \( \hat{s}|\alpha\rangle_x = |\alpha + 1 (\text{mod } d)\rangle_x \). The generators of the encoding are, for \( k = 1, \ldots, \lfloor \frac{d}{2} \rfloor \),

\[
\hat{\Delta}_k = \frac{\hat{L}^k + \hat{L}^{-k}}{2}, \quad \hat{\Delta}_{k+\lfloor \frac{d}{2} \rfloor} = -\frac{\hat{L}^k - \hat{L}^{-k}}{2i},
\]

and \( \hat{\Delta}_0 = \frac{I}{2} \). Let \( |a_{\ell}\rangle_L = F |\ell\rangle_L \), where \( F \) is the quantum Fourier transform given by \( F = \sum_{j,k=0}^{d-1} \frac{1}{\sqrt{d}} \exp\left(\frac{2\pi i j k}{d}\right) |j\rangle_L \langle k|_L \). It is easy to verify that \( \{|a_{\ell}\rangle_L\} \) are the eigenvectors of \( \hat{\Delta}_k \) with eigenvalues \( c_{\ell}(k) = \cos\left(\frac{2\pi \ell k}{d}\right) \), and of \( \hat{\Delta}_{k+\lfloor \frac{d}{2} \rfloor} \) with eigenvalues \( s_{\ell}(k) = \sin\left(\frac{2\pi \ell k}{d}\right) \). To simplify our calculations, we choose to express our generators in the following basis instead:

\[
\tilde{\hat{H}}_\ell = \frac{1}{d} \left( v_\ell \hat{\Delta} - \eta_{\ell} \hat{\Delta}_{\lfloor \frac{d}{2} \rfloor} \right),
\]

where \( v_\ell = 2 \left( c_{\ell}(0), c_{\ell}(\lfloor \frac{d}{2} \rfloor), s_{\ell}(1), \ldots, s_{\ell}(\lfloor \frac{d}{2} \rfloor) \right)^T \),

\( \hat{\Delta} = (\hat{\Delta}_0, \ldots, \hat{\Delta}_{\lfloor \frac{d}{2} \rfloor})^T \) and \( \eta_{\ell} = \frac{1+i(-1)^d}{2} \cos(\ell \pi) \).

Data represented using the logical basis can be encrypted by choosing a key, \( \kappa = (\kappa_1, \ldots, \kappa_{d-1}) \), where each \( \kappa_\ell \) is an integer chosen uniformly at random from \( \{0, \ldots, d\} \), and applying the corresponding random unitary operation on each qudit:

\[
\mathcal{E} = \exp\left( \sum_{\ell=0}^{d-1} i \phi_{\ell} \tilde{\hat{H}}_\ell \right),
\]

where the angle \( \phi_{\ell} := \frac{2\pi}{d+\tau_{\kappa_\ell}} \). It is convenient to think of \( \mathcal{E} \) as a product of integer powers of \( \mathcal{E}_\ell := \exp(i \tilde{\hat{H}}_{\ell} \frac{2\pi}{d+\tau_{\kappa_\ell}}) \), so that \( \mathcal{E} = \mathcal{E}_1^{\kappa_1} \cdots \mathcal{E}_{d-1}^{\kappa_{d-1}} \).

After the encoding, computation can still be performed on the qudits using the operations described in the previous section. However, for an adversary that does
not have access to $\kappa$, the information encoded is obscured. Once the evaluation is completed, the qudits can be decrypted by applying $E^\dagger$ on every qudit to yield the processed plaintext. Surprisingly, with this simple encryption-decryption process, any quantum computation done on the encrypted state yields the same result when decrypted, as if it was done on the unencrypted state: it is a fully homomorphic private-key quantum cryptosystem.

To prove that our scheme works, we have to show that (1) $E$ commutes with a local qudit gate in $U(n)$, and that (2) $E \otimes E$ commutes with the 2-qudit $N(\alpha, \beta)_{xy}^{(n)}$ gate.

**Lemma 2:** $E$ commutes with any local qudit gate.

Proof: The encoding operation acts only on the internal states of each particle, whereas the generators of the $U(n)$ transform all internal states in the same way. As such the former must commute with the latter. More formally, we first show that $\hat{s} \otimes \hat{s}$ commutes with $\hat{C}_{x,y}$:

\[
(\hat{s} \otimes \hat{s}) \hat{C}_{x,y} = \sum_{\alpha=0}^{d-1} \hat{a}_{x,\alpha+1} \delta_{y,\alpha+1} \hat{a}_{y,\alpha+1} (\hat{s} \otimes \hat{s}) = \hat{C}_{x,y} (\hat{s} \otimes \hat{s})
\]

where we have used the fact that the set of $\alpha$’s is a group under addition modulo $d$. Since $\hat{C}_{x,y}$ commutes with $\hat{s} \otimes \hat{s}$, then it must also commute with $\hat{L}$, and hence with any power of $\hat{L}$. As the generators of the encoding, depend only on powers of $\hat{L}$, they must then commute with $\hat{C}_{x,y}$. Consequently, the groups generated by $\hat{H}$ and $\hat{C}_{x,y}$ also commute.

**Lemma 3:** $N(\alpha, \beta)_{xy}^{(n)}$ commutes with $E \otimes E$.

Proof: First, we note that $\hat{S} = \bigotimes_{k=1}^{m} S(\alpha_k, \beta_k)_{xy_m}$ swaps the qudit states at $x$ and $y$, while the first and second terms in the tensor product $E \otimes E$ act on the qudit states at $x$ and $y$ respectively. Then $\hat{S}$ must commute with $E \otimes E$ because $S(E \otimes E) = S(E \otimes I)(I \otimes E) = (I \otimes E)(E \otimes I)S = (E \otimes E)\hat{S}$. Since $N(\alpha, \beta)_{xy}^{(n)} = \frac{1}{\sqrt{2}}(I + i \hat{S})$ and both $\hat{I}$ and $\hat{S}$ commute with $E \otimes E$, then $N(\alpha, \beta)_{xy}^{(n)}$ must commute with $E \otimes E$.

Hidden information — Here we show that our quantum homomorphic scheme can hide a number of bits proportional to $d$.

Without knowing the key, the ensemble $\{\hat{p}_\alpha, p_\alpha\}$ for an input of $|\alpha\rangle = |\alpha_1, \alpha_2, \ldots, \alpha_m\rangle$, where

\[
\hat{p}_\alpha = \frac{1}{(d+1)^{d-1}} \sum_{\kappa_1, \ldots, \kappa_{d-1}=0}^{d-1} E^{\otimes m} |\alpha\rangle_L^E |\alpha\rangle^E \langle \alpha|^E \langle \alpha|^E .
\]

It is illuminating to look at the ensemble in the Fourier transform basis as here the encoding is diagonal. We can write $\hat{p}_\alpha$ in the form $\sum_{\beta, \beta' \in \mathbb{Z}_d^2} |\beta\rangle_L^E \langle \beta'| c_{\beta, \beta'}$ and the non-zero coefficients are those for which the number of $\ell$’s in $\beta$ is equal to the number of $\ell$’s in $\beta'$ for all $\ell = 1, \ldots, d - 1$. Let $F(\hat{O})$ denote $(E^\dagger)^{\otimes m} \hat{O} F^{\otimes m}$. Then

\[
F(\hat{p}_\alpha) = \frac{1}{d^m} \sum_{\beta, \beta' \in \mathbb{Z}_d^2} e^{-2\pi i \alpha \beta} |\beta\rangle_L^E \langle \beta'| c_{\beta, \beta'} \times \prod_{\ell=0}^{d-1} \delta(\text{wt}_\ell(\beta) - \text{wt}_\ell(\beta')) ,
\]

where $\text{wt}_\ell(\beta)$ is the Lee weight which counts the number of times $\ell$ appears in the vector $\beta$. The non-zero terms in eq. (1) can be partitioned into sets labeled by integer partitions of $m$. Let $P_{m,d}$ be the set of integer partitions of $m$ into $d$ (possibly empty) parts and let $\lambda$ be a partition in $P_{m,d}$. In eq. (1), strings for which all Lee weights are equal belong to the same partition $\lambda$. The entries in $\lambda = (\lambda_0, \lambda_1, \ldots, \lambda_{d-1})$ give the number of times a particular element appears in $\beta$. With this notation, we get

\[
F(\hat{p}_\alpha) = \frac{1}{d^m} \sum_{\lambda \in P_{m,d}} R_{\lambda} \langle \Psi_\lambda^0 | \Psi_\lambda^0 \rangle ,
\]

where $R_{\lambda} = \left( \begin{array}{c} m \\ \lambda_0, \lambda_1, \ldots, \lambda_{d-1} \end{array} \right)$ is the multinomial coefficient, and

\[
|\Psi_\lambda^0 \rangle = \frac{1}{\sqrt{R_{\lambda}}} \sum_{\beta: \text{wt}_\lambda(\beta) = \lambda_j} e^{-2\pi i \alpha \beta} |\beta\rangle_L^E ,
\]

which is invariant under permutation of the qudits.

**Theorem 2:** For all probability distributions $p_\alpha$, the accessible information of the encoding $E$, without knowing the key, is upper bounded by $\log_2 m$ bits when Alice sends $m$ qudits.

Proof: First, we observe that the elements of $\{|\alpha\rangle_L, \alpha = 0, \ldots, d-1\}$ are related by powers of $\hat{L}$. Since $\hat{L}$ is unitary and commutes with the encoding $E$, it must be that $S(\hat{p}_\alpha)$ is the same for all $\alpha$. For simplicity, we analyze $S(\hat{p}_0)$:

\[
S(\hat{p}_0) = S(F(\hat{p}_0))
\]

\[
= S \left( \sum_{\lambda \in P_{m,d}} R_{\lambda} \langle \Psi_\lambda^0 | \Psi_\lambda^0 \rangle \right)
\]

\[
= H \left( \left\{ \frac{R_{\lambda}}{d^m} \right\} \right) + \sum_{\lambda \in P_{m,d}} \frac{R_{\lambda}}{d^m} S( \langle \Psi_\lambda^0 | \Psi_\lambda^0 \rangle )
\]

\[
= H \left( \left\{ \frac{R_{\lambda}}{d^m} \right\} \right) ,
\]

where we have used the orthogonality of the different partitions labelled by $\lambda$ in third equality [33], and that $\langle \Psi_\lambda^0 | \Psi_\lambda^0 \rangle$ has rank one in the final equality. Similar ar-
guments can be made for \( \hat{\rho} = \sum_{\alpha} p_{\alpha} \rho_{\alpha} \).

\[
S(\hat{\rho}) = S \left( \sum_{\alpha \in \mathbb{Z}_d^n} p_{\alpha} \sum_{\lambda \in \mathbb{C}_{m,d}} \frac{R_{\lambda}}{d^m} |\Psi_{\alpha}^{\lambda}\rangle \langle \Psi_{\alpha}^{\lambda}| \right) \\
\leq S \left( \sum_{\alpha \in \mathbb{Z}_d^n} \frac{1}{d^m} \sum_{\lambda \in \mathbb{C}_{m,d}} \frac{R_{\lambda}}{d^m} |\Psi_{\alpha}^{\lambda}\rangle \langle \Psi_{\alpha}^{\lambda}| \right) \\
= H \left( \left\{ \frac{R_{\lambda}}{d^m} \right\} \right) + \sum_{\lambda} \frac{R_{\lambda}}{d^m} S \left( \sum_{\alpha} \frac{1}{d^m} |\Psi_{\alpha}^{\lambda}\rangle \langle \Psi_{\alpha}^{\lambda}| \right). \tag{3}
\]

The inequality above occurs because applying a channel that randomizes over \( \alpha \), by applying a random power of \( \hat{L} \) to each qudit, symmetrizes the probability distribution \( p_{\alpha} \) to the uniform distribution, but cannot decrease entropy. The second term of eq. (3) obeys the identity

\[
\frac{1}{d^m} \sum_{\alpha \in \mathbb{Z}_d^n} |\Psi_{\alpha}^{\lambda}\rangle \langle \Psi_{\alpha}^{\lambda}| = \frac{1}{R_{\lambda}} \sum_{\beta \in \mathcal{W}(L)=\lambda} |\beta\rangle \langle \beta|, \tag{4}
\]

and is hence a maximally mixed state in the partition labeled by \( \lambda \) with a rank of \( R_{\lambda} \), with entropy at most \( \log_2 R_{\lambda} \leq \log_2 m \). Using these facts and putting eqs. (2)-(4) together, we obtain a bound on the Holevo quantity of

\[
\chi(\{\hat{\rho}_{\alpha}, p_{\alpha}\}) \leq \log_2 m! \tag{5}
\]

which in turn bounds the accessible information.

When \( m \) is large,

\[
\chi(\{\hat{\rho}_{\alpha}, p_{\alpha}\}) \leq m \log_2 m - \frac{1}{\log 2} m + O(\log(m))
\]

and the gap, between the encoded information and the information accessible to an adversary, is at least

\[
\Gamma = m \log_2 d - \chi(\{\hat{\rho}_{\alpha}, p_{\alpha}\}) \\
\approx m \log_2 (d/m) + m(\log 2)^{-1}.
\]

Thus if \( d = m \) and \( m \log_2 m \) bits are encoded, this gap scales at least proportional to \( m \). This is a significantly stronger security than that offered by [24], while at the same time dramatically extending the functionality by allowing universal computation to be performed on the encrypted data. As our bound in eq. (5) is independent of the probability distribution used for the encoding, the bound on the accessible information holds even if the a priori distribution on the plaintext is not uniform.

In conclusion, we have constructed a quantum fully-homomorphic encryption scheme, with information-theoretic security guarantees on the amount of information leaked. Our scheme serves as a proof-of-principle that such fully-homomorphic encryption schemes can exist. While our scheme does not offer perfect security, we believe that the approach to homomorphic encryption based on centralizers of reducible representations we describe offers a new approach which may lead to further improvements in security in the future.

**Acknowledgements** — We thank H. de Guise for helpful discussions, and Y. Li for useful comments. This material is based on research supported in part by the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01.

---

* Electronic address: joseph_fitzsimons@sutd.edu.sg

[1] P. W. Shor, SIAM journal on computing 26, 1484 (1997).
[2] L. K. Grover, in Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing, STOC ‘96 (ACM, New York, NY, USA, 1996) pp. 212–219.
[3] S. Lloyd et al., SCIENCE-NEW YORK THEN WASHINGTON- , 1073 (1996).
[4] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems and signal processing, Vol. 175 (1984) p. 8.
[5] A. K. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[6] R. L. Rivest, L. Adleman, and M. L. Dertouzos, Foundations of Secure Computation, Academia Press , 169 (1978).
[7] C. Gentry, in Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing, STOC ‘09 (ACM, New York, NY, USA, 2009) pp. 169–178.
[8] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, in Advances in Cryptology EUROCRYPT 2010, Lecture Notes in Computer Science, Vol. 6110, edited by H. Gilbert (Springer Berlin Heidelberg, 2010) pp. 24–43.
[9] A. Broadbent, J. Fitzsimons, and E. Kashefi, in Foundations of Computer Science, 2009. FOCS ’09. 50th Annual IEEE Symposium on (2009) pp. 517–526.
[10] D. Aharonov, M. Ben-or, and E. Eban, arXiv:0810.5375 (2008).
[11] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science 335, 303 (2012).
[12] T. Morimae and K. Fujii, Phys. Rev. A 87, 050301 (2013).
[13] V. Giovannetti, L. Maccone, T. Morimae, and T. G. Rudolph, Phys. Rev. Lett. 111, 230501 (2013).
[14] A. Mantri, C. A. Pérez-Delgado, and J. F. Fitzsimons, Physical review letters 111, 230502 (2013).
[15] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217 (2013).
[16] B. W. Reichardt, F. Unger, and U. Vazirani, Nature 496, 456 (2013).
[17] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, Nat Phys 9, 727 (2013).
[18] M. McGague, arXiv:1010.1989 (2010).
[19] M. Liang, Quantum Information Processing 12, 3675 (2013).
[20] M. Liang, arXiv:1410.2435v1 (2014).
[21] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, Nat Commun 5 (2014).
[22] A. M. Childs, Quantum Info. Comput. 5, 456 (2005).
[23] L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, Phys. Rev. A 90, 050303 (2014).
[24] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, Phys. Rev. Lett. 109, 150501 (2012).
[25] S. Aaronson and A. Arkhipov, in Proc. 43rd Ann. ACM Symp. Theory Comp., STOC ’11 (2011).
[26] P. Kok, W. J. Munro, K. Nemoto, T. C. Ralph, J. P. Dowling, and G. Milburn, Reviews of Modern Physics 79, 135 (2007).
[27] M. C. Tichy, M. Tiersch, F. Mintert, and A. Buchleitner, New Journal of Physics 14, 093015 (2012).
[28] A. Klein and E. R. Marshalek, Rev. Mod. Phys. 63, 375 (1991).
[29] D. J. Rowe, B. C. Sanders, and H. de Guise, Journal of Mathematical Physics 40, 3604 (1999).
[30] F. Iachello, “Lie algebras and applications,” (Springer, Berlin Heidelberg, 2006) 1st ed.
[31] J. L. Brylinski and R. Brylinski, in Mathematics of Quantum Computation, edited by R. Brylinski and G. Chen (Computational Mathematics (Chapman & Hall/CRC Press), Boca Raton, 2004).
[32] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Physical Review Letters 73, 58 (1994).
[33] M. Nielsen and I. L. Chuang, “Quantum computation and quantum information,” (Cambridge University Press, New York, 2011) 10th ed.