SCIENTIFIC REPORTS

OPEN

Received: 15 March 2016
Accepted: 23 August 2016
Published: 23 September 2016

# A quantum approach to homomorphic encryption

Si-Hui Tan[1], Joshua A. Kettlewell[1], Yingkai Ouyang[1], Lin Chen[2,3] & Joseph F. Fitzsimons[1,4]

**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 a subgroup of operations to present a private-key quantum homomorphic encryption scheme that enables a broad class of quantum computation on encrypted data. The quantum data is encoded on bosons of distinct species in distinct spatial modes, and the quantum computations are manipulations of these bosons in a manner independent of their species. A particular instance of our encoding hides up to a constant fraction of the information encrypted. This fraction can be made arbitrarily close to unity with overhead scaling only polynomially in the message length. 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 homomorphic encryption schemes. Indeed, a number of attempts have been made to find a quantum analogue of homomorphic encryption[19–24], 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[25]. As a result, some schemes[19–22] 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. Another scheme by Broadbent and Jeffery[23] allow the evaluation of circuits of low $T$-gate complexity by building on a classical fully homomorphic encryption scheme. Incorporating ideas from the garden-hose model of computation, Dulek, Schaffner, and

[1]Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372. [2]School of Mathematics and Systems Science, Beihang University, Beijing 100191, China. [3]International Research Institute for Multidisciplinary Science, Beihang University, Beijing 100191, China. [4]Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117543. Correspondence and requests for materials should be addressed to S.-H.T. (email: sihui_tan@sutd.edu.sg)

Speelman[24] expanded this scheme to allow the evaluation of polynomial-depth circuits. However, these schemes are dependent on computational assumptions, necessary for the underlying classical homomorphic encryption schemes, for their security. The question then remains as to whether information theoretically secure homomorphic encryption is possible without expanding the definition to include interactive protocols. One might consider implementing a quantum one-time pad on the data, which takes the data to the maximally mixed state. One could perform arbitrary quantum computations on the encrypted data, and then construct a decryption algorithm that depends on the computation performed[19]. However homomorphic encryption schemes need to satisfy compactness: the decryption operation must be less computationally expensive than the evaluation on the encrypted data. The Achilles heel of such a scheme is that it fails to satisfy compactness. A first step in the direction of non-interactive quantum protocols with compactness was presented by Rohde *et al.*[26] for a restricted model of quantum computation known as the BosonSampling model[27] 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 processing of encrypted data beyond BosonSampling is not known to date.

In this paper, we present a private-key homomorphic encryption protocol that supports a broad class of computations, including and extending beyond BosonSampling, while providing certain information theoretic security guarantees by bounding the information accessible to an adversary. While this is not a standard cryptographic measure of security, it provides a reasonable measure of privacy in a standalone setting which is free of computational assumptions. However, stronger security definition based on trace distance exists[28]. The protocol we present ensures a gap between the information accessible to an adversary and actual information encoded that grows as $m\log_2(d/m) + m(\log 2)^{-1}$ bits when $m \log_2 d$ bits are encrypted using $m$ $d$-level systems. This is a significantly stronger security guarantee than that offered by the scheme presented by Rohde *et al.*[26]. 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 for a broad class of computations to be performed on encrypted data for a range of encryption schemes satisfying certain symmetry constraints. This class of quantum computations can be thought of as manipulations of bosons in a manner independent of their internal state. The computation begins with a set of bosons, each in a unique spatial mode with all modes occupied, with the internal state of each boson specifying the input to the computation. The computation consists of manipulating the spatial degree of freedom of the bosons, in such a way that operations depend only on the number of bosons in a mode and not their internal state. At the end of the computation, both the spatial and internal degree of freedom of the bosons are measured. This model includes BosonSampling, using the encoding due to Rohde *et al.*[26], but extends far beyond it due to a much richer group structure of the set of allowed operations. We conclude with a concrete encoding which supports such computations while satisfying the necessary symmetry constraints and show that it limits the accessible information as described above.

## Results

**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. The set of operations used to perform the encryption must be chosen as a subset of this centralizer. While it is not immediately obvious that encryption operations chosen this way should actually be able to hide information, the BosonSampling scheme presented in Rohde *et al.*[26] provides an example of such an encoding where a non-trivial amount of information is hidden.

**Representation of computation.** Our protocol uses $m$ identical bosonic particles; each particle has a spatial degree of freedom limited to a finite number of modes $x = 1, \ldots, m$ and an internal state $\alpha = 0, \ldots, d-1$ (see Fig. 1). We design our scheme such that the encryption operations affect only the internal states of the particles, and the computation operations affect only the spatial modes of the particles. Since the input to the computation is supplied using the internal states of the particles, but the computation is performed using manipulation of only spatial modes, it may appear that the input does not affect the computation. This is not the case, however, since the internal states of the particles affect the computation by altering interference between particles.

Each particle can be represented as a state $|\alpha\rangle_x$ created out from a vacuum state $|\mathrm{vac}\rangle$ via a creation operator $\hat{a}^\dagger_{x,\alpha}$, with $|\alpha\rangle_x = \hat{a}^\dagger_{x,\alpha}|\mathrm{vac}\rangle$. The bosonic creation operators $\hat{a}^\dagger_{x,\alpha}$ and $\hat{a}^\dagger_{y,\beta}$ commute, and satisfy the orthogonality condition $[a_{x,\alpha}, a^\dagger_{y,\beta}] = \delta_{\alpha,\beta}\,\delta_{x,y}$. Note that we make no assumption on the internal states of the $m$ particles, any two particles can have the same or different internal states. Explicitly, the initial state of our scheme is

$$\hat{a}^\dagger_{1,\alpha_1} \ldots \hat{a}^\dagger_{m,\alpha_m}|\mathrm{vac}\rangle = |\alpha_1\rangle_1 \otimes \ldots \otimes |\alpha_m\rangle_m, \tag{1}$$

which we denote as $|\overrightarrow{\alpha}\rangle$ for short, where $\overrightarrow{\alpha} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}_d^m$ is our plaintext. Since the values of $\alpha_1, \ldots, \alpha_m$ are selected from the integers from 0 to $d-1$, there are $d^m$ possible orthogonal input states, spanning a complex Euclidean space $(\mathbb{C}^d)^{\otimes m}$.

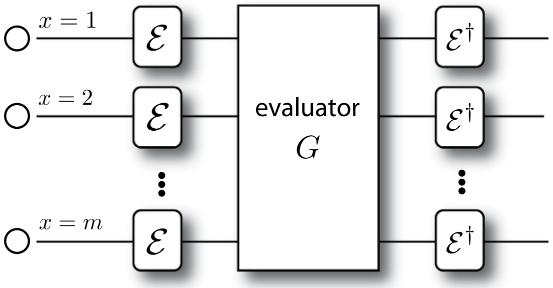

**Figure 1. This figure shows Alice's encoding scheme for *m* bosonic particles each in one of *d* internal states.** Each particle has a spatial degree of freedom labeled by $x$. The encoding operation $\mathcal{E}$ is effected across the particles in a tensor product way. The evaluation operation is taken from the group $G$, which acts non-trivially only on the spatial modes of the $m$ bosons, and can put multiple bosons in a single spatial mode. Post-evaluation, the encryption is removed via the inverse encoding operation to reveal the evaluated plaintext.

The set of computation operations that we are allowed to perform contains a group of unitary operations, generated by a set of infinitesimal generators with a large cardinality. The state space of $m$ identical bosons can be expressed as a symmetric subspace of a Hilbert space $\mathcal{H}_m = \mathcal{H}_{\text{internal}} \otimes H_{\text{spatial}}$, where $\mathcal{H}_{\text{internal}}$ and $\mathcal{H}_{\text{spatial}}$ denote the space for the internal degrees of freedom and the spatial modes of the $m$ identical bosons respectively. Due to the indistinguishability of the bosons, the state of the system is invariant under permutation of particles, and hence the system can only occupy states within the subspace of $\mathcal{H}_m$ which respect this permutational symmetry. The computational operations, which act only on $\mathcal{H}_{\text{spatial}}$, must respect this symmetry, and hence the infinitesimal generators of the group of such operations are permutation-invariant. We proceed to elucidate the structure of these infinitesimal generators. Each boson can be in one of $m$ possible spatial modes, and hence there are $m^2$ generalized Pauli operators each of dimension $m$ that act non-trivially on the spatial degree of freedom of each boson. Let the corresponding Hermitian and non-Hermitian generalized Pauli operators constitute the sets $\mathcal{B}_i$ and $\mathcal{B}_i'$ respectively. We construct a set $\mathcal{C}_i'$ that contains a maximal number of linearly independent operators from $\left\{\frac{1}{2}(P + P^\dagger)\colon P \in \mathcal{B}_i'\right\} \cup \left\{\frac{i}{2}(P - P^\dagger)\colon P \in \mathcal{B}_i'\right\}$. The Hermitian set $\overline{\mathcal{B}}_i = \mathcal{B}_i \cup \mathcal{C}_i'$ then comprises of $m^2$ infinitesimal generators of the unitary group operating non-trivially only on the spatial modes on the $i$-th boson. The infinitesimal generators of group of computation operations are then symmetric sums of the $m$-fold tensor product of elements from $\overline{\mathcal{B}}_i$, with each such element corresponding to one boson. The number of such symmetric sums is exactly the number of ways to distribute $m$ indistinguishable spatial labels (because of the requirement of permutation-invariance) among $m^2$ distinct elements of $\overline{\mathcal{B}}_i$, which is $\binom{m^2 + m - 1}{m}$. Hence the set of computation operations $G$ that we can perform contains a group of unitary operators, $G_C$, generated by a set of infinitesimal generators with a cardinality of at least $\binom{m^2 + m - 1}{m} \geq \frac{(m^2)^m}{m!} \geq m^m e^{m-1}/\sqrt{m}$. If we denote the set of all infinitesimal generators of the spatial part of $G_C$ by $C$, then $G_C = \{\mathbb{I}_{\text{int}} \otimes \exp(i\sum_{c\in C}\theta_c c)\colon \theta_c \in \mathbb{R}\}$, where $\mathbb{I}_{\text{int}}$ is the identity operator on the internal states of the $m$ bosons. The computation subgroup $G_C$ intuitively corresponds to a model of computation with interacting bosons of $d$ species in which the computation only depends on the spatial labels of the bosons.

Contained within $G_C$ are unitaries generated by the following infinitesimal generators:

$$\widehat{C}_{x,y}\colon = \sum_{\alpha=0}^{d-1} \hat{a}_{x,\alpha}^\dagger \hat{a}_{y,\alpha}, \tag{2}$$

for $1 \leq x, y \leq m$. These operators $\widehat{C}_{x,y}$ are infinitesimal generators for operations that are equivalent to beam-splitters for $x \neq y$, and phase-shifters for $x = y$ in the quantum optics setting. Since we can generate the phase-shifters and the beam-splitters as in Reck *et al.*[29], these infinitesimal generators generate a dimension $m$ unitary group isomorphic to $\mathrm{U}(m)$[30–32] from which the evaluator's computation operations can be chosen. These are the same elements used to construct those of the BosonSampling model. All particles in the BosonSampling model are indistinguishable (have the same internal states); the particles in our model however need not be indistinguishable, because each particle can be chosen as a $d$-level system independently. If we were to filter out particles with one of the $d$ internal states, we are left with a system that is equivalent to $d - 1$ BosonSampling models by linearity of passive linear optics. This is a generalization of the insight used to encrypt BosonSampling instances in Rohde *et al.*[26].

Hence our computation space includes a hard sampling problem as a special case. However, it is currently unknown whether our model allows for encoded universal computation on a space of size exponential in $m$.

*Encoding scheme* — For the encryption operation, a unitary operator $\mathcal{E}$, is applied to the internal state of the $m$ particles as is depicted in Fig. 1. Since $\mathcal{E}$ only acts on the internal states of the particles, provided that it operates identically on all particles, it commutes with our computation operations that act trivially on the internal states of the particles. In this section, we give a specific choice $\mathcal{E}$ which enables non-trivial hiding of information.

In what follows, we drop the spatial labels of the particles and make them implicit. We define the computational basis states of each particle to be $|\alpha\rangle$ for $\alpha = 0, \ldots, d-1$, and define the discrete Fourier transform on $\mathbb{C}^d$ as

$$F = \sum_{\alpha,\beta=0}^{d-1} \frac{1}{\sqrt{d}} \exp\left(\frac{2\pi i\alpha\beta}{d}\right) |\beta\rangle\langle\alpha|. \tag{3}$$

Denote the basis states of $\mathbb{C}^d$ in the Fourier transform basis as $|\alpha_F\rangle = F|\alpha\rangle$, and define the trigonometric terms $c_\alpha(k) = \cos(2\pi\alpha k/d)$ and $s_\alpha(k) = \sin(2\pi\alpha k/d)$ for arbitrary integers $\alpha$ and $k$. The generators of the encoding are, for $k = 1, \ldots, \left\lfloor \frac{d}{2} \right\rfloor$,

$$\begin{aligned} \widehat{\Delta}_k &= \frac{\widehat{L}^k + \widehat{L}^{-k}}{2} = \sum_{\alpha=0}^{d-1} c_\alpha(k)\,|\alpha_F\rangle\langle\alpha_F|, \\ \widehat{\Delta}_{k+\left\lfloor \frac{d}{2} \right\rfloor} &= -\frac{\widehat{L}^k - \widehat{L}^{-k}}{2i} = \sum_{\alpha=0}^{d-1} s_\alpha(k)\,|\alpha_F\rangle\langle\alpha_F|, \end{aligned} \tag{4}$$

where $\widehat{L}$ is the cyclic shift operation on the internal state of each particle such that $\widehat{L}|\alpha\rangle = |\alpha + 1(\mathrm{mod}\, d)\rangle$. To simplify our calculations, we choose to express our generators in the following basis instead:

$$\widehat{H}_\ell = \frac{1}{d}\left(\mathbb{I} - \eta_\ell \widehat{\Delta}_{\left\lfloor \frac{d}{2} \right\rfloor} + \sum_{k=1}^{\left\lfloor \frac{d}{2} \right\rfloor}\left(2c_\ell(k)\widehat{\Delta}_k + 2s_\ell(k)\widehat{\Delta}_{k+\left\lfloor \frac{d}{2} \right\rfloor}\right)\right), \tag{5}$$

where $\eta_\ell = \frac{1+(-1)^d}{2}\cos(\ell\pi)$. It is easy to verify that in the Fourier transform basis, $\widehat{H}_\ell = |\ell_F\rangle\langle\ell_F|$.

Data represented using the logical basis can be encrypted by choosing a key, $\vec{\kappa} = (\kappa_1, \ldots, \kappa_{d-1})$, where each $\kappa_\ell$ is an integer chosen uniformly at random from the non-negative integers $\{0, \ldots, m\}$, and applying the random unitary operation $\mathcal{E}$ on each particle, where

$$\mathcal{E} = \exp\left(\sum_{\ell=1}^{d-1} i\phi_\ell \widehat{H}_\ell\right), \tag{6}$$

and $\phi_\ell = \frac{2\pi}{m+1}\kappa_\ell$ are the secret random angles. It is convenient to think of $\mathcal{E}$ as a product of integer powers of $\mathcal{E}_\ell = \exp\left(i\widehat{H}_\ell \frac{2\pi}{m+1}\right)$, so that $\mathcal{E} = \mathcal{E}_1^{\kappa_1} \ldots \mathcal{E}_{d-1}^{\kappa_{d-1}}$.

After the encoding, computation can still be performed on the encrypted data using the operations described in the previous section. However, for an adversary that does not have access to $\vec{\kappa}$, the information encoded is obscured. Once the evaluation is completed, the output can be decrypted by applying $\mathcal{E}^\dagger$ on every particle to yield the processed plaintext. Surprisingly, with this simple encryption-decryption process, *any* quantum computation chosen from $G$ which is performed on the encrypted state yields the same result when decrypted, as if it were performed on the unencrypted state. The result is an encryption scheme that admits privacy homomorphisms for operations chosen from $G$.

Our scheme works because the encryption operators affect only the internal states of the particles at each site, while the computation leaves the internal states of every particle invariant. In the particular encryption scheme we have chosen, the encryption operators generate an abelian group $A$ that acts trivially on the spatial modes. Hence the evaluator can perform operations in the tensor product of the group $G$ and the abelian group $A$.

**Hidden information.** Here we show that our quantum homomorphic scheme can hide a number of bits proportional to $m$. Without knowing the key, the ensemble is $\{\hat{\rho}_{\vec{\alpha}}, p_{\vec{\alpha}}\}$ where $\vec{\alpha} = (\alpha_1, \alpha_2, \ldots, \alpha_m)$ denotes the plaintext, and the corresponding encrypted state is

$$\hat{\rho}_{\vec{\alpha}} = \frac{1}{(m+1)^{d-1}} \sum_{\kappa_1,\ldots,\kappa_{d-1}=0}^{m} \mathcal{E}^{\otimes m}|\vec{\alpha}\rangle\langle\vec{\alpha}|(\mathcal{E}^\dagger)^{\otimes m}. \tag{7}$$

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

$$\mathcal{F}(\hat{\rho}_{\vec{\alpha}}) = \frac{1}{d^m} \sum_{\vec{\beta},\vec{\beta}'\in\mathbb{Z}_d^m} e^{-\frac{2\pi i\vec{\alpha}\cdot(\vec{\beta}-\vec{\beta}')}{d}} |\vec{\beta}\rangle\langle\vec{\beta}'| \times \prod_{\ell=0}^{d-1} \delta(\mathrm{wt}_\ell(\vec{\beta}) - \mathrm{wt}_\ell(\vec{\beta}')), \tag{8}$$

where $\mathrm{wt}_\ell(\vec{\beta})$ is the Lee weight which counts the number of times $\ell$ appears in the vector $\vec{\beta}$. The non-zero terms in Eq. (8) 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. (8), 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 $\vec{\beta}$. With this notation, we get

$$\mathcal{F}(\hat{\rho}_{\vec{\alpha}}) = \frac{1}{d^m}\sum_{\lambda\in P_{m,d}} R_\lambda |\Psi_\lambda^{\vec{\alpha}}\rangle\langle\Psi_\lambda^{\vec{\alpha}}|, \tag{9}$$

where $R_\lambda = \binom{m}{\lambda_0,\, \lambda_1,\, \ldots,\, \lambda_{d-1}}$ is the multinomial coefficient, and

$$|\Psi_\lambda^{\vec{\alpha}}\rangle = \frac{1}{\sqrt{R_\lambda}} \sum_{\substack{\vec{\beta}:\mathrm{wt}_j(\vec{\beta})=\lambda_j\\ j=0,\ldots,d-1}} e^{-\frac{2\pi i}{d}\vec{\alpha}\cdot\vec{\beta}}|\vec{\beta}\rangle, \tag{10}$$

which is invariant under permutation of the particles.

**Theorem 1** For all probability distributions $p_{\vec{\alpha}}$ over plaintexts $\vec{\alpha}$, the accessible information of the encoding, without knowing the key, is upper bounded by $\log_2 m!$ bits when Alice sends $m$ $d$-level particles.
Proof: First, we observe that the elements of $\{|\alpha\rangle,\ \alpha = 0, \ldots,\ d - 1\}$ are related by powers of $\hat{L}$. Since $\hat{L}$ is unitary and commutes with the encoding $\mathcal{E}$, it must be that $S(\hat{\rho}_{\vec{\alpha}})$ is the same for all $\vec{\alpha}$. For simplicity, we analyze $S(\hat{\rho}_{\vec{0}})$:

$$\begin{aligned} S(\hat{\rho}_{\vec{0}}) &= S(\mathcal{F}(\hat{\rho}_{\vec{0}}))\\ &= S\left(\sum_{\lambda\in P_{m,d}} \frac{R_\lambda}{d^m}|\Psi_\lambda^{\vec{0}}\rangle\langle\Psi_\lambda^{\vec{0}}|\right)\\ &= H\left(\left\{\frac{R_\lambda}{d^m}\right\}\right) + \sum_{\lambda\in P_{m,d}}\frac{R_\lambda}{d^m}S\ \left(|\Psi_\lambda^{\vec{0}}\rangle\langle\Psi_\lambda^{\vec{0}}|\right)\\ &= H\left(\left\{\frac{R_\lambda}{d^m}\right\}\right), \end{aligned} \tag{11}$$

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

$$\begin{aligned} S(\hat{\rho}) &= S\left(\sum_{\vec{\alpha}\in\mathbb{Z}_d^m} p_{\vec{\alpha}}\sum_{\lambda\in P_{m,d}}\frac{R_\lambda}{d^m}|\Psi_\lambda^{\vec{\alpha}}\rangle\langle\Psi_\lambda^{\vec{\alpha}}|\right)\\ &\leq S\left(\sum_{\vec{\alpha}\in\mathbb{Z}_d^m}\frac{1}{d^m}\sum_{\lambda\in P_{m,d}}\frac{R_\lambda}{d^m}|\Psi_\lambda^{\vec{\alpha}}\rangle\langle\Psi_\lambda^{\vec{\alpha}}|\right)\\ &= H\left(\left\{\frac{R_\lambda}{d^m}\right\}\right) + \sum_\lambda\frac{R_\lambda}{d^m}S\left(\sum_{\vec{\alpha}}\frac{1}{d^m}|\Psi_\lambda^{\vec{\alpha}}\rangle\langle\Psi_\lambda^{\vec{\alpha}}|\right). \end{aligned} \tag{12}$$

The inequality above occurs because applying a channel that randomizes over $\vec{\alpha}$, by applying a random power of $\hat{L}$ to each particle, symmetrizes the probability distribution $p_{\vec{\alpha}}$ to the uniform distribution, but cannot decrease entropy. The second term of Eq. (12) obeys the identity

$$\frac{1}{d^m}\sum_{\vec{\alpha}\in\mathbb{Z}_d^m}|\Psi_\lambda^{\vec{\alpha}}\rangle\langle\Psi_\lambda^{\vec{\alpha}}| = \frac{1}{R_\lambda}\sum_{\substack{\vec{\beta}:\mathrm{wt}_j(\vec{\beta})=\lambda_j\\ j=0,\ldots,d-1}}|\vec{\beta}\rangle\langle\vec{\beta}|, \tag{13}$$

and is hence a maximally mixed state in the partition labeled by $\lambda$ with a rank of $R_\lambda$, with entropy at most $\max_\lambda \log_2 R_\lambda \leq \log_2 m!$. Using these facts and putting Eqs (11–13) together, we obtain a bound on the Holevo quantity of

$$\chi(\{\hat{\rho}_{\vec{\alpha}}, p_{\vec{\alpha}}\}) \leq \log_2 m! \tag{14}$$

which in turn bounds the accessible information.

## Discussion

When $m$ is large,

$$\chi(\{\hat{\rho}_{\vec{\alpha}}, p_{\vec{\alpha}}\}) \leq m\log_2 m - \frac{1}{\log 2}m + \mathcal{O}(\log(m)). \tag{15}$$

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

$$\begin{aligned} \Gamma &= m\log_2 d - \chi(\{\hat{\rho}_{\vec{\alpha}}, p_{\vec{\alpha}}\})\\ &\approx m\log_2(d/m) + m(\log 2)^{-1}. \end{aligned} \tag{16}$$

Thus if $d = m$ and $m\ \log_2 m$ bits are encoded, this gap scales at least proportional to $m$. Moreover if $d = m^{\frac{1}{r}}$ for $r$ in the open unit interval, the gap asymptotically approaches $(1 - r)$ as a fraction of bits encoded. This is a significantly stronger security than that offered by Rohde *et al.*[26], while at the same time significantly extending the functionality by allowing computations beyond BosonSampling to be performed on the encrypted data, thus bringing us closer to the goal of achieving a quantum fully homomorphic encryption scheme. As our bound in Eq. (14) 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.

## Methods

The aim of this section is two-fold. First, to give the explicit form of the computation operators contained in $G_C$ which is strictly a subgroup of $G$. Second, to show that the encryption and computation operators of our QHE scheme commute.

Let $\mathcal{H}_{\text{internal}} \otimes \mathcal{H}_{\text{spatial}} = \text{span}(\mathcal{K})$, where $\mathcal{K}$ is the set of all states of the form $|\alpha_1, x_1\rangle \otimes |\alpha_2, x_2\rangle \otimes \ldots \otimes |\alpha_m, x_m\rangle$ where $\alpha_j \in \{0, 1, \ldots, d-1\}$ and $x_j \in \{1, 2, \ldots, m\}$ are the internal and spatial labels respectively. Hence the Hilbert space of $m$ bosons lies within the tensor product space $\mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_m$, where each $\mathcal{H}_j = \mathcal{H}_{\text{internal},j} \otimes \mathcal{H}_{\text{spatial},j}$ denotes the Hilbert space of each boson with the subscript $j$ as a label on the $j$-th boson, and is equal to $\mathcal{H}_{\text{internal}} \otimes \mathcal{H}_{\text{spatial}}$. As our particles are identical bosons, the state of the $m$ particles must be invariant under permutation of the labels of the particles. Thus, the set of all possible states for our $m$-bosons is the symmetric subspace of $\mathcal{H}_1 \otimes \ldots \otimes \mathcal{H}_m$.

For our scheme, the computation operators act only on the spatial mode of the particles. Each bosonic particle can be in one of $m$ possible spatial modes, and hence there are $m^2$ generalized Pauli operators each of dimension $m$ that act non-trivially on the spatial degree of freedom of each boson. In order to define the infinitesimal generators of the computation, let us first define the multi-qudit generalized Pauli operator given a tensor product of generalized Pauli operators[34]. The set of generalized Pauli operators of size $m$ can be defined as

$$\mathcal{P} = \{X^a Z^b\colon a,\ b \in \{0, \ldots,\ m - 1\}\}, \tag{17}$$

where $X\colon = \sum_{k=0}^{m-1} |k + 1 \mod m\rangle\langle k|$, and $Z\colon = \sum_{k=0}^{m-1} e^{2\pi ik/m}\ |k\rangle\langle k|$. Define $\mathcal{B}$ and $\mathcal{B}'$ as the Hermitian and non-Hermitian operators in $\mathcal{P}$ respectively. Now let $\mathbb{I}_{\text{spatial},j}$ denote the identity operator on the Hilbert space $\mathcal{H}_{\text{spatial},j}$ and define $\check{\mathbb{I}}_{\text{spatial},j}$ to be the identity operator on the internal subsystem of all the bosons except for the $j$-th boson, given explicitly by

$$\check{\mathbb{I}}_{spatial,j} = \begin{cases} \mathbb{I}_{spatial,2} \otimes \ldots \otimes \mathbb{I}_{spatial,m}, & j = 1 \\ \mathbb{I}_{spatial,1} \otimes \ldots \otimes \mathbb{I}_{spatial,j-1} \otimes \mathbb{I}_{spatial,j+1} \otimes \ldots \otimes \mathbb{I}_{spatial,m}, & 2 \leq j < m. \\ \mathbb{I}_{spatial,1} \otimes \ldots \otimes \mathbb{I}_{spatial,m-1}, & j = m \end{cases} \tag{18}$$

For every generalized Pauli operator $P \in \mathcal{P}$, we define $\omega_j(P) = \check{\mathbb{I}}_{\text{spatial},j} \otimes P$ to be the multi-particle operator that only acts non-trivially on the spatial degree of freedom of the $j$-th particle where it applies the operator $P$. Correspondingly define the Hermitian and non-Hermitian operators on particle $j$ as $\mathcal{B}_j$ and $\mathcal{B}'_j$ respectively. Then our multi-particle generalized Pauli has the form

$$\sigma = \omega_1(P_1) \ldots \omega_m(P_m), \tag{19}$$

where $P_1, \ldots, P_m \in \mathcal{P}$.

The generalized Pauli operators $\mathcal{P}$ are not always Hermitian, but the infinitesimal generators of unitary operations must be Hermitian. To generate unitary elements, we would have to make the non-Hermitian operators of $\mathcal{B}'_j$ Hermitian. Let $\mathcal{C}'_j$ denote a subset of $\left\{\frac{1}{2}(P + P^\dagger)\colon P \in \mathcal{B}'_j\right\} \cup \left\{\frac{i}{2}(P - P^\dagger)\colon P \in \mathcal{B}'_j\right\}$ comprising of a maximal number of linearly independent elements. Then an orthogonal set of Hermitian operators in the Hilbert-Schmidt inner product that acts on the $j$-th particle is $\overline{\mathcal{B}}_j = \mathcal{B}_j \cup \mathcal{C}'_j$.

For a given $m$-tuple of operators, $\vec{b} = (b_1, \ldots, b_m)$, $b_j \in \overline{\mathcal{B}}_j$, we define the corresponding symmetric sum,

$$c_{\vec{b}} = \sum_{\pi \in S_m} \prod_{j=1}^{m} \omega_{\pi(j)}(b_j), \tag{20}$$

where $S_m$ denotes the symmetric group of order $m$. The set of $C = \left\{c_{\vec{b}}\colon \vec{b} = (b_1, \ldots, b_m),\ b_j \in \overline{\mathcal{B}}_j\right\}$ denotes the set of all infinitesimal generators for the spatial part of $G_C$. The group $G_C$ of unitary operators generated from $C$ that is contained within $G$ is

$$G_C = \left\{g = \mathbb{I}_{\text{int}} \otimes \exp\left(i \sum_{c \in C} \theta_c c\right)\colon \theta_c \in \mathbb{R}\right\}, \tag{21}$$

where $\mathbb{I}_{\text{int}} = \otimes_{j=1}^{m} \mathbb{I}_{\text{int },j}$ is the identity operator on the internal state of the $m$ bosons. It is in this sense that the infinitesimal generators in $C$ generate the group $G_C$. The cardinality of $C$ is precisely the number of ways to distribute $m$ indistinguishable spatial labels among $m^2$ distinct elements of $\overline{\mathcal{B}}_j$ which is $\binom{m^2 + m - 1}{m}$. Any encryption operator $\widetilde{\mathcal{E}}$ that we consider can be written as a linear operator on the tensor product space $\mathcal{H}_{\text{int}} \otimes \mathcal{H}_{\text{spatial}}$ where

$$\widetilde{\mathcal{E}} = \mathcal{E} \otimes \mathbb{I}_{\text{spatial}}, \tag{22}$$

where $\mathbb{I}_{\text{spatial}}$ is the identity operator on the spatial subsystem of the $m$ bosons. This trivially commutes with all computation operators from $G_C$, as can be seen from Eq. (21).

The no-go theorem of Yu *et al.*[25] implies that for perfect information theoretic security, the size of the encoding must scale with the number of bits required to the computation to be performed on the encrypted data. For extremely limited classes of computation, such as only applying Pauli operators, this is trivially satisfiable with an encoding that scales linearly with the input size. However, when the set of possible computation has super-exponential cardinality, as is the case for universal classical or quantum computation, perfect security cannot be achieved. Our results, then, can be seen as evidence that an equivalent no-go theorem does not hold when the security demand is relaxed.

## References

1. Shor, P. W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM journal on computing* **26,** 1484–1509 (1997).
2. Grover, L. K. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-eighth Annual ACM Symposium on Theory of Computing,* STOC '96, 212–219 (1996).
3. Lloyd, S. *et al.* Universal quantum simulators. *Science* **273,** 5278, 1073–1077 (1996).
4. Bennett, C. H. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and signal processing* vol. 175, 8 (1984).
5. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67,** 661–663 (1991).
6. Rivest, R. L., Adleman, L. & Dertouzos, M. L. On data banks and privacy homomorphisms. *Foundations of Secure Computation, Academic Press* 169–179 (1978).
7. Gentry, C. Fully homomorphic encryption using ideal lattices. In *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing,* STOC '09, 169–178 (ACM, New York, NY, USA, 2009).
8. van Dijk, M., Gentry, C., Halevi, S. & Vaikuntanathan, V. Fully homomorphic encryption over the integers. In Gilbert, H. (ed.) *Advances in Cryptology EUROCRYPT 2010,* vol. 6110 of *Lecture Notes in Computer Science,* 24–43 (Springer Berlin Heidelberg, 2010).
9. Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. In *Proceedings of the 50th Annual IEEE Symposium on Foundations of Computer Science, FOCS '09,* 517–526 (2009).
10. Aharonov, D., Ben-or, M. & Eban, E. Interactive proofs for quantum computations. *arXiv:0810.5375* (2008).
11. Barz, S. *et al.* Demonstration of blind quantum computing. *Science* **335,** 6066, 303–308 (2012).
12. Morimae, T. & Fujii, K. Blind quantum computation protocol in which Alice only makes measurements. *Phys. Rev. A* **87,** 050301 (2013).
13. Giovannetti, V., Maccone, L., Morimae, T. & Rudolph, T. G. Efficient universal blind quantum computation. *Phys. Rev. Lett.* **111,** 230501 (2013).
14. Mantri, A., Pérez-Delgado, C. A. & Fitzsimons, J. F. Optimal blind quantum computation. *Phys. Rev. Lett.* **111,** 230502 (2013).
15. Fitzsimons, J. F. & Kashefi, E. Unconditionally verifiable blind computation. *arXiv:1203.5217* (2013).
16. Reichardt, B. W., Unger, F. & Vazirani, U. Classical command of quantum systems. *Nature* **496,** 456–460 (2013).
17. Barz, S., Fitzsimons, J. F., Kashefi, E. & Walther, P. Experimental verification of quantum computation. *Nat Phys* **9,** 727-731 (2013).
18. McKague, M. Self-testing graph states. *arXiv:1010.1989* (2010).
19. Liang, M. Symmetric quantum fully homomorphic encryption with perfect security. *Quantum Information Processing* **12,** 3675–3687 (2013).
20. Liang, M. Quantum fully homomorphic encryption scheme based on universal quantum circuit. *Quantum Information Processing* **14,** 2749–2759 (2015).
21. Fisher, K. A. G. *et al.* Quantum computing on encrypted data. *Nat. Commun.* **5** (2014).
22. Childs, A. M. Secure assisted quantum computation. *Quantum Info. Comput.* **5,** 456–466 (2005).
23. Broadbent, A. & Jeffery, S. Quantum homomorphic encryption for circuits of low *T*-gate complexity. In *Advances in Cryptology*, CRYPTO '15 (2015).
24. Dulek, Y., Schaffner, C. & Speelman, F. Quantum homomorphic encryption for polynomial-sized circuits. *arXiv:1603.09717v1* (2016).
25. Yu, L., Perez-Delgaodo, C. A. & Fitzsimons, J. F. Limitations on information-theoretically-secure quantum homomorphic encryption. *Phys. Rev. A* **90,** 050303(R) (2014).
26. Rohde, P. P., Fitzsimons, J. F. & Gilchrist, A. Quantum walks with encrypted data. *Phys. Rev. Lett.* **109,** 150501 (2012).
27. Aaronson, S. & Arkhipov, A. The computational complexity of linear optics. In *Proceedings of the 43rd Annual ACM Symposium on Theory of Computing,* STOC '11 (2011).
28. Ouyang, Y., Tan, S.-H. & Fitzsimons, J. F. Quantum homomorphic encryption from quantum codes. *arXiv:1508.00938* (2015).
29. Reck, M., Zeilinger, A., Bernstein, H. J. & Bertani, P. Experimental realization of any discrete unitary operator. *Phys. Rev. Lett.* **73,** 58 (1994).
30. Klein, A. & Marshalek, E. R. Boson realizations of lie algebras with applications to nuclear physics. *Rev. Mod. Phys.* **63,** 375–558 (1991).
31. Rowe, D. J., Sanders, B. C. & de Guise, H. Representations of the Weyl group and Wigner functions for su(3). *Journal of Mathematical Physics* **40,** 3604–3615 (1999).
32. Iachello, F. *Lie Algebras and Applications* (Springer, Berlin Heidelberg, 2006), first edn.
33. Nielsen, M. & Chuang, I. L. *Quantum Computation and Quantum Information* (Cambridge University Press, New York, 2011), 10 anniv. edn.
34. Ouyang, Y. Concatenated quantum codes can attain the quantum Gilbert-Varshamov bound. *IEEE trans. Inf. Theory* **60,** 3117–3122 (2014).

## Acknowledgements

We thank H. de Guise for helpful discussions, and L. Yu 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. LC was supported by the NSF of China (Grant No. 11501024), and the Fundamental Research Funds for the Central

Universities (Grant Nos. 30426401 and 30458601). JFF and ST acknowldeges support from the Air Force Office of Scientific Research under grant FA2386-15-1-4082.

## Author Contributions

J.F.F., J.A.K. and S.T. formulated the protocol; L.C., J.F.F., S.-H.T. and Y.O. proved the theorems; J.F.F., S.-H.T. and Y.O. wrote the manuscript, all authors contributed to discussions about the results and the manuscript; and J.F.F. supervised the project.

## Additional Information

**Competing financial interests:** The authors declare no competing financial interests.

**How to cite this article**: Tan, S.-H. *et al.* A quantum approach to homomorphic encryption. *Sci. Rep.* **6**, 33467; doi: 10.1038/srep33467 (2016).

This work is licensed under a Creative Commons Attribution 4.0 International License. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in the credit line; if the material is not included under the Creative Commons license, users will need to obtain permission from the license holder to reproduce the material. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/

© The Author(s) 2016