Practical somewhat-secure quantum somewhat-homomorphic encryption with coherent states

Si-Hui Tan,[1,2,*] Yingkai Ouyang,[1,2,†] and Peter P. Rohde[3]

[1] *Singapore University of Technology and Design, 8 Somapah Road, Singapore 487372, Singapore*
[2] *Centre for Quantum Technologies, National University of Singapore, Block S15, 3 Science Drive 2, Singapore 117543, Singapore*
[3] *Centre for Quantum Software and Information, Faculty of Engineering and Information Technology, University of Technology Sydney, Sydney, NSW 2007, Australia*

(Received 16 October 2017; published 5 April 2018)

We present a scheme for implementing homomorphic encryption on coherent states encoded using phase-shift keys. The encryption operations require only rotations in phase space, which commute with computations in the code space performed via passive linear optics, and with generalized nonlinear phase operations that are polynomials of the photon-number operator in the code space. This encoding scheme can thus be applied to any computation with coherent-state inputs, and the computation proceeds via a combination of passive linear optics and generalized nonlinear phase operations. An example of such a computation is matrix multiplication, whereby a vector representing coherent-state amplitudes is multiplied by a matrix representing a linear optics network, yielding a new vector of coherent-state amplitudes. By finding an orthogonal partitioning of the support of our encoded states, we quantify the security of our scheme via the indistinguishability of the encrypted code words. While we focus on coherent-state encodings, we expect that this phase-key encoding technique could apply to any continuous-variable computation scheme where the phase-shift operator commutes with the computation.

DOI: 10.1103/PhysRevA.97.042308

I. INTRODUCTION

In classical cryptography, homomorphic encryption has been a topic of intense interest in recent years [1–3]. It is a form of encryption that allows a computation to be performed on the encrypted text without having to first decrypt the text. If an arbitrary computation is allowed, then the encryption is said to be *fully homomorphic*. The first fully homomorphic encryption scheme was only discovered recently by Gentry in 2009 [2]. However, like many other classical cryptographic primitives, these homomorphic schemes only offer computational security, which means that they are secure as long as certain problems are computationally intractable. The search for information-theoretically secure encryption problems has led to quantum analogs of homomorphic encryption [4–6]. These schemes only have to hide the quantum input to the computation, unlike a related quantum cryptographic protocol known as blind quantum computation (BQC) [7] which also hides the desired computation. However, unlike BQC, no interactive protocols are allowed in quantum homomorphic encryption. Other schemes that perform quantum computing on encrypted data that require interactions are known [8–11], though confusingly some of them have been labeled as “quantum homomorphic encryption” [8,9]. Others have focused on hybrid schemes [12–14] that bootstrap on a classical fully homomorphic encryption scheme to achieve computational security while allowing certain classes of quantum computations to be performed on encrypted data. However, some restrictions have arisen. It has been shown that efficient quantum fully homomorphic encryption is impossible [15,16], even when relaxing from perfect to imperfect security. Nonetheless, the key insights contributed by the advent of these quantum schemes still expand the possibilities for implementations of homomorphic encryption in various forms and for different uses, especially since partial information security is still possible for sets of computations of large cardinality [4,5].

It was shown in [4] that homomorphic encryption may be implemented for a restricted class of quantum computation known as the boson-sampling model [17–21]. In the boson-sampling model, computation is performed via a passive linear optical network with a subset of the input modes of this network initialized with a single photon, and the remainder initialized in the vacuum state. To implement the homomorphic encryption described in [4], the client begins by inputting a single photon into *every* mode, as opposed to just a subset of the modes. Modes where a single photon should have been present are vertically polarized, whereas modes where no photon should have been present are horizontally polarized. Because horizontally and vertically polarized photons do not interfere, they effectively evolve independently through the linear optics network, and by discarding all horizontally polarized photons at the output the desired computation is recovered. Security is achieved by applying the same random polarization rotation to every photon before entry to the network. The angle of rotation acts as the client’s private key, which is not disclosed to the party performing the evaluation. After the evaluation, the photons are returned to the user, who subsequently applies the inverse rotation and discards all horizontally polarized photons, thereby recovering the computation. However, in the absence of knowledge of the key, it is difficult to differentiate between photons that belong to the computation and those which should be discarded. With this scheme, $O(\log_2(m))$ bits

[*] sihui_tan@sutd.edu.sg
[†] yingkai_ouyang@sutd.edu.sg

can be hidden when m bits are encrypted. Using group theoretical insights, this homomorphic scheme has been expanded upon to enable quantum computation beyond boson sampling while improving the security [5] to hide a constant fraction of the number of bits sent. This fraction can be made arbitrarily close to unity by increasing the number of internal states of the bosons used to encode information.

Quantum information theory relies on representing information using quantum states. The underlying algebra of the states, and hence of the operations forming the encoding, affect the performance of the encryption scheme. In this paper, we explore the use of a phase rotation encoding for coherent-state qubits. The advantages of using coherent states are plentiful. Coherent states are produced relatively easily; a laser source closely approximates a coherent state. In phase space a coherent state is a "blob," where the distance from the origin is the amplitude of the coherent state and the angle is its phase. Schemes exist to encode classical bits onto coherent states [22], to create a collection of universal gate sets for computations with these encodings [23,24], and to map general quantum communication protocols involving pure states of multiple qubits into one that employs coherent states [25]. The ease of producing, manipulating, and distributing coherent states has seeded continuous-variable (CV) analogs [26], primarily featuring coherent states, of quantum cryptography schemes such as quantum key distribution [27–29] and random ciphers for quantum encryption [30,31].

In this paper, we present a somewhat-homomorphic encryption scheme that utilizes a logical encoding onto coherent states and encrypts with random rotations in phase space. The scheme works as follows: each classical bit is represented on a single coherent state. A random private key is generated, and the same corresponding random phase shift is applied to every coherent state. An evaluation that is made up of elements from an allowed set of operations, G, is then performed on the encrypted data. The set G contains beamsplitters, linear and nonlinear phase shifts, and unitaries that commute with encryption operators. Both the Kerr and cross-Kerr interactions are also included in G. In fact, any operator that preserves photon number will work. Although this scheme follows a similar principle to those of [4,5], it is a different primitive. The main differences are that it is a continuous-variable protocol, and the encryption and computation operators act on the same Hilbert space nontrivially. The other two schemes are discrete-variable protocols, and have encryption and computation operators that act nontrivially only on distinct subspaces.

We quantify the security of our protocol with the trace distance between any two encrypted inputs. In this notion of security, an adversary without knowledge of the secret key attempts to distinguish the encryptions of any two messages. The smaller the trace distance, the more indistinguishable the encrypted messages are to the adversary. We find this trace distance by showing that the encoding operation induces a partition structure in the states of the microcanonical ensemble where most of the off-diagonal terms are zeroed out. The partition structure gives a closed-form equation for the trace distance between two encrypted inputs. By comparing this trace distance to that for the corresponding unencrypted state, we show that our encryption scheme suppresses the distinguishability of the encoded states and thus provides some security against an adversary attempting to identify the encoded message. Our scheme demonstrates that quantum somewhat-homomorphic encryption is possible for qubit encodings using continuous-variable states. While we focus on a coherent-state encoding, a similar phase-key encoding scheme might be applicable to other CV computation schemes. In principle, this encoding could be applied to any CV scheme where the phase-shift operator commutes with the computation, for any choice of basis states that are not rotation symmetric in phase space, such as photon-number states.

II. LOGICAL ENCODING USING COHERENT STATES

Consider an encoding of logical qubits using coherent states with $|0_L\rangle = |\alpha\rangle$ and $|1_L\rangle = |-\alpha\rangle$, where $|\alpha\rangle = \sum_{n=0}^{\infty} e^{-\frac{|\alpha|^2}{2}} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$ with $\alpha \in \mathbb{C}$. An m-bit binary string $\mathbf{x} := (x_1, x_2, \ldots, x_m)$ is represented by the tensor product state $|\psi_{\mathbf{x}}\rangle = |(-1)^{x_1}\alpha\rangle\, |(-1)^{x_2}\alpha\rangle \ldots |(-1)^{x_m}\alpha\rangle$. These logical qubits are not orthogonal as $|\langle\alpha| - \alpha\rangle|^2 = e^{-4|\alpha|^2} > 0$. Consequently, when m bits are encoded using the ensemble $\{p_{\mathbf{x}}, \hat{\rho}_{\mathbf{x}}\}$, where $p_{\mathbf{x}}$ is the prior probability for the string $\mathbf{x}$ and $\hat{\rho}_{\mathbf{x}} = |\psi_{\mathbf{x}}\rangle\langle\psi_{\mathbf{x}}|$, the accessible information of the ensemble, $I_{\text{acc}}(\{p_{\mathbf{x}}, \hat{\rho}_{\mathbf{x}}\})$, is less than m bits.

A lower bound on the accessible information of the encoding ensemble can be obtained for a uniform prior by the mutual information between $\mathbf{x}$ and the outcomes given by a pretty-good measurement (PGM) [32], $\mathbf{y}_{\text{PGM}}$. The assumption that the prior distribution of the code words is uniform corresponds to the case where the evaluator has no prior information about the source. The PGM is described by the positive-operator valued measure (POVM) $\{\hat{\rho}^{-\frac{1}{2}}\hat{\rho}_{\mathbf{x}}\hat{\rho}^{-\frac{1}{2}}, \mathbf{x} \in \mathbb{Z}_2^m\}$, where $\hat{\rho} = \frac{1}{2^m}\sum_{\mathbf{x}\in\mathbb{Z}_2^m} \hat{\rho}_{\mathbf{x}} = \frac{1}{2^m}(\hat{\rho}_0 + \hat{\rho}_1)^{\otimes m}$, $\hat{\rho}_0 := |\alpha\rangle\langle\alpha|$, and $\hat{\rho}_1 := |-\alpha\rangle\langle-\alpha|$. Here $\hat{\rho}^{-\frac{1}{2}}$ denotes the pseudoinverse of the matrix square root of the density matrix $\hat{\rho}$.

Every element of the POVM is a tensor product over the m modes, thus the mutual information for the m-mode inputs $\mathbf{x}$ to outputs $\mathbf{y}_{\text{PGM}}$ is

$$I(\mathbf{x}; \mathbf{y}_{\text{PGM}}) = m I(x; y_{\text{PGM}}), \tag{1}$$

where the $I(x; y_{\text{PGM}})$ is the mutual information for a single-mode discrimination by the PGM. Let $p_x(\ell) := \frac{1}{2}$ and $p_y(j)$ be the prior and posterior probabilities for obtaining $x = \ell$ and $y = j$, respectively. Then, we have

$$I(x; y_{\text{PGM}}) = \sum_{j,\ell=0}^{1} p_x(\ell) p(j|\ell) \log_2\left(\frac{p(j|\ell)}{p_y(j)}\right), \tag{2}$$

where $p(j|\ell) := \text{tr}(\Pi_j\, |\ell_L\rangle\langle\ell_L|)$, and $\Pi_j = 2(\hat{\rho}_0 + \hat{\rho}_1)^{-\frac{1}{2}}\hat{\rho}_{x_j}(\hat{\rho}_0 + \hat{\rho}_1)^{-\frac{1}{2}}$ is the conditional probability that the jth outcome was measured given that $|\ell_L\rangle$ was sent, and

$$\Pi_j := \left(\frac{\hat{\rho}_0 + \hat{\rho}_1}{2}\right)^{-\frac{1}{2}} |(-1)^j\alpha\rangle\langle(-1)^j\alpha| \left(\frac{\hat{\rho}_0 + \hat{\rho}_1}{2}\right)^{-\frac{1}{2}}. \tag{3}$$

The mixed state $\frac{1}{2}(\hat{\rho}_0 + \hat{\rho}_1)$ has the spectral decomposition $a_+ |\psi_+\rangle \langle\psi_+| + a_- |\psi_-\rangle \langle\psi_-|$ [33] where the eigenvectors are

$$|\psi_\pm\rangle := \frac{|\alpha\rangle \pm |-\alpha\rangle}{\sqrt{2}\sqrt{1 \pm \exp(-2|\alpha|^2)}}, \tag{4}$$

with eigenvalues $a_\pm := \frac{1}{2}[1 \pm \exp(-2|\alpha|^2)]$, respectively. The conditional probabilities are explicitly

$$p(j|\ell) = \begin{cases} \frac{1}{2}\left(\sqrt{a_+} + \sqrt{a_-}\right)^2, & j = \ell \\ \frac{1}{2}\left(\sqrt{a_+} - \sqrt{a_-}\right)^2, & j \neq \ell \end{cases}, \tag{5}$$

and thus

$$\begin{aligned} I(x; y_{\text{PGM}}) = {} & (\sqrt{a_+} + \sqrt{a_-})^2 \log_2(\sqrt{a_+} + \sqrt{a_-}) \\ & + (\sqrt{a_+} - \sqrt{a_-})^2 \log_2(\sqrt{a_+} - \sqrt{a_-}). \end{aligned} \tag{6}$$

When $|\alpha| \to 0$, we have $I(x; y_{\text{PGM}}) = 2|\alpha|^2/\ln(2) + O(|\alpha|^4)$, while, if $|\alpha| \to \infty$, $I(x; y_{\text{PGM}}) \to 1$. This is expected because $|\alpha\rangle$ and $|-\alpha\rangle$ are barely distinguishable for small $|\alpha|$, but become nearly orthogonal as $|\alpha|$ becomes large.

III. HOMOMORPHIC ENCRYPTION

Here, we define encoding and decoding operations that encrypt and decrypt the data. We follow the approach of [5], wherein the encoding operators are chosen to commute with those of the computation in the code space.

After the classical string is encoded onto coherent-state qubits, the user chooses a key k uniformly at random from the set $\{0,1,\ldots,d-1\}$, where d is a positive integer. A phase-space rotation is then implemented on every mode, each with the same angle. The phase-space rotation operator on the jth mode is

$$\widehat{\Phi}_j(\theta_k) = \exp(-i\theta_k \hat{a}_j^\dagger \hat{a}_j), \tag{7}$$

where $\theta_k := 2\pi k/d$. Such an operation on a coherent state yields also a coherent state with the same amplitude, but rotated in phase space by θ_k around the origin. The application of the above operator on every mode gives a net operator that is generated by the total photon-number operator, $\hat{N} := \sum_{j=1}^m \hat{a}_j^\dagger \hat{a}_j$. The encrypted state is then processed before decryption. The processing is performed by an evaluator, who is able to process the encrypted state without knowing the secret key. Finally, the output bit string $\mathbf{y} := (y_1, y_2, \ldots, y_m)$ can be determined by a measurement on the modes after an inverse rotation $\widehat{\Phi}_j(-\theta_k)$. Since the computation operators are conditioned to commute with the encryption (and decryption) operators and the decryption algorithm is constant in the length of the input, our scheme satisfies Broadbent and Jeffery's condition of *correctness* and *compactness* [12]. In the next section, we will show that nontrivial computation operators which commute with $\bigotimes_{j=1}^m \widehat{\Phi}(\theta_k)$ exist. Then, we discuss the complexity of these allowed computations in our scheme. They are closely linked to boson sampling [17] and quantum walks [34,35]—equivalent nonuniversal models of quantum computation.

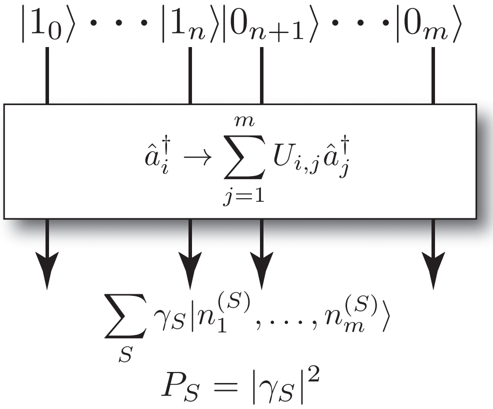
$|1_0\rangle \cdots |1_n\rangle |0_{n+1}\rangle \cdots |0_m\rangle$
$\hat{a}_i^\dagger \to \sum_{j=1}^{m} U_{i,j} \hat{a}_j^\dagger$
$\sum_S \gamma_S |n_1^{(S)}, \ldots, n_m^{(S)}\rangle$
$P_S = |\gamma_S|^2$

FIG. 1. The boson-sampling model. A string of n single photons is prepared in m optical modes. They are evolved via a passive interferometer U. Finally the photon statistics are sampled from the distribution $P(S)$.

IV. ALLOWED COMPUTATIONAL OPERATIONS

The evaluation of quantum operations on the ciphertext is implemented via a unitary operator $U = e^{-iHt/\hbar}$ with its evaluation Hamiltonian H implemented by quantum optical components that are necessarily (Hermitian) photon-number-preserving operators. Using Ehrenfest's theorem, we have the following evolution of the total photon-number operator $\widehat{N}$ under a given Hamiltonian H: $d\langle\widehat{N}\rangle/dt = \frac{1}{i\hbar}\langle[\widehat{N}, H]\rangle$. Since the evaluation operators do not change the photon number of the input, then $d\langle\widehat{N}\rangle/dt = 0$. This implies that $\langle[\widehat{N}, H]\rangle = 0$. A set of photon-number-preserving computations that also commutes with $\hat{N}$ includes operations in passive linear optics (phase shifts and beamsplitters) and operations that are polynomials of the number operators. We call the latter set the generalized nonlinear phase operations and their Hamiltonians are of the form

$$H_{\text{NL}} := \sum_{\mathbf{n} \in \mathbb{N}^m} g_{n_1,\ldots,n_m} \prod_{k=1}^m (a_k^\dagger a_k)^{n_k}, \tag{8}$$

where $g_{n_1,\ldots,n_m}$ is a coupling constant. The single-mode Kerr and cross-Kerr interactions are special cases of H_{NL} [36]. Let K be a constant that is proportional to a third-order nonlinear susceptibility. The single-mode Kerr interaction is given by $m = 1$, $g_1 = -\hbar K$, $g_2 = \hbar K$, and $g_{n_1} = 0$ otherwise, while the cross-Kerr interaction is given by $m = 2$, $g_{1,1} = \hbar K$, and $g_{n_1,n_2} = 0$ otherwise.

Passive linear optics is featured heavily in the boson-sampling model, where we begin by preparing n single photons in m optical modes (see Fig. 1). This input state evolves via nonadaptive, passive linear optics, which implements a unitary map on the photon creation operators, $\hat{a}_i^\dagger \to \sum_{j=1}^m U_{i,j} \hat{a}_j^\dagger$. The output state to the interferometer has the form $|\psi_{\text{out}}\rangle = \sum_S \gamma_S |n_1^{(S)}, \ldots, n_m^{(S)}\rangle$, where S represents a photon-number configuration with $n_i^{(S)}$ photons in the ith mode, and γ_S are the associated amplitudes. Finally, coincidence photodetection is performed, which samples from the probability distribution $P(S) = |\gamma_S|^2$. Aaronson and Arkhipov showed that sampling from $P(S)$ is likely to be a hard problem for classical computers for some scaling of m with n [17].

Nonetheless, when the inputs to the circuit are switched from single photons to coherent states, the quantum computation performed can be efficiently simulated classically [37], using simple $m \times m$ matrix multiplication. This changes, however, when we also allow Kerr interactions in the circuit, because this interaction allows the production of cat states from coherent states [38]. For instance, in the interaction picture where $K(\hat{a}^\dagger \hat{a})^2$ is regarded as the interaction part of the evaluation Hamiltonian, an initial coherent state will evolve to $e^{-i\hbar K t(\hat{a}^\dagger \hat{a})^2} |\alpha\rangle = \frac{1}{\sqrt{2}}(e^{-i\pi/4}|\alpha\rangle + e^{i\pi/4}|-\alpha\rangle)$ at time $t = \frac{\pi}{2\hbar K}$. Cat states when evolved via passive linear optics and sampled with number-resolved photodetection implement a classically hard sampling problem under plausible complexity theoretic assumptions [39], although it is not believed to be universal for quantum computation.

V. SECURITY ANALYSIS

Without knowledge of the key, the encrypted input state is

$$\mathcal{E}(\hat{\rho}_{\mathbf{x}}) := \frac{1}{d}\sum_{k=0}^{d-1}\bigotimes_{j=1}^{m}\widehat{\Phi}_j\left(\frac{2\pi k}{d}\right)|\psi_{x_j}\rangle\langle\psi_{x_j}|\widehat{\Phi}_j\left(-\frac{2\pi k}{d}\right)$$
$$= \left(\bigotimes_{j=1}^{m} V_j^{x_j}\right)\mathcal{E}(\hat{\rho}_{\mathbf{0}})\left(\bigotimes_{j=1}^{m} V_j^{\dagger x_j}\right), \tag{9}$$

where x_j is the jth element of the string $\mathbf{x}$, $|\psi_{x_j}\rangle := |(-1)^{x_j}\alpha\rangle$ is the state of the jth mode of $|\psi_{\mathbf{x}}\rangle$, and $V_j = \widehat{\Phi}_j(\pi)$. If someone without knowledge of the key were to attempt to measure the encrypted input state, $\hat{\rho}_{\mathbf{x}}$, they would perceive a state highly mixed in the phase degree of freedom, and have difficulty in differentiating between states that belong to the computation. This indistinguishability gives a security for our scheme which we now make precise.

To quantify the security of our encryption scheme, we obtain an upper bound on the trace distance between the encrypted states given by $D(\mathcal{E}(\hat{\rho}_{\mathbf{u}}),\mathcal{E}(\hat{\rho}_{\mathbf{v}}))$ for arbitrary pairs of m-bit strings $\mathbf{u}$ and $\mathbf{v}$, where $D(\sigma,\tau) = \frac{1}{2}\|\sigma - \tau\|_{\text{tr}}$ denotes the trace distance between the density matrices σ and τ. It suffices to obtain an upper bound on $D(\mathcal{E}(\hat{\rho}_{\mathbf{x}}),\mathcal{E}(\hat{\rho}_{\mathbf{0}}))$ where $\mathbf{x} = \mathbf{u} \oplus \mathbf{v}$, because using the invariance of the trace distance under unitary transformation we can get to the trace distance between any pairs of encrypted states.

We first write the phase-shift operator on the Fock space $\widehat{\Phi}(\frac{2\pi}{d}) := \sum_{y\in\mathbb{N}} \omega^y |y\rangle\langle y|$ where $\omega = e^{-2\pi i/d}$ and $\mathbb{N}$ is the set of non-negative integers. Let $\phi(\mathbf{z}) = \sum_i z_i \mod d$. Now for every integer ℓ, the matrix $[\widehat{\Phi}(\frac{2\pi}{d})^{\otimes m}]^\ell$ is equivalent to $\sum_{\mathbf{y}\in\mathbb{N}^m} \omega^{\ell\phi(\mathbf{y})}|\mathbf{y}\rangle\langle\mathbf{y}|$. Hence, using the Fourier identity $\frac{1}{d}\sum_{\ell=0}^{d-1}\omega^{\ell\phi(\mathbf{y}-\mathbf{z})} = \delta_{\phi(\mathbf{y}-\mathbf{z}),0}$,

$$\mathcal{E}(\hat{\rho}_{\mathbf{0}}) = \sum_{\mathbf{z},\mathbf{y}\in\mathbb{N}^m}\delta_{\phi(\mathbf{y}-\mathbf{z}),0}\, b_{\mathbf{z}} b_{\mathbf{y}}^* |\mathbf{z}\rangle\langle\mathbf{y}|, \tag{10}$$

where $b_{\mathbf{z}} = b_{z_1}b_{z_2}\dots b_{z_m}$ is a product of complex coefficients, each given by $b_n := e^{-|\alpha|^2/2}\frac{\alpha^n}{\sqrt{n!}}$. The state $\mathcal{E}(\hat{\rho}_{\mathbf{0}})$ admits a block-diagonal decomposition, with each block labeled by $\phi(\mathbf{y}-\mathbf{z}) = j$. The support of the jth block is $\{|\mathbf{z}\rangle \in G_j : z \in \mathbb{N}^m\}$, where $G_j := \{\mathbf{z}\in\mathbb{N}^m : \phi(\mathbf{z}) = j\}$ is a partition of $\mathbb{N}^m$. Defining $|g_j\rangle := \sum_{\mathbf{z}\in G_j} b_{\mathbf{z}}|\mathbf{z}\rangle$, then

$$\mathcal{E}(\hat{\rho}_{\mathbf{0}}) = \sum_{j=0}^{d-1} q_j |\tilde{g}_j\rangle\langle\tilde{g}_j|, \tag{11}$$

where $|\tilde{g}_j\rangle = |g_j\rangle/\sqrt{q_j}$ is a normalized state and

$$q_j = \langle g_j|g_j\rangle = \sum_{\mathbf{z}\in G_j}|b_{\mathbf{z}}|^2.$$

This partition structure makes it straightforward to compute the trace distance between $\mathcal{E}(\hat{\rho}_{\mathbf{x}})$ and $\mathcal{E}(\hat{\rho}_{\mathbf{0}})$. Using Eq. (10) in the expression in Eq. (9), we have

$$\mathcal{E}(\hat{\rho}_{\mathbf{x}}) = \sum_{\ell=0}^{d-1} q_\ell |\tilde{h}_\ell\rangle\langle\tilde{h}_\ell|, \tag{12}$$

where $|\tilde{h}_\ell\rangle$ is the normalized state

$$|\tilde{h}_\ell\rangle = \bigotimes_{k=1}^{m} V_k^{x_k}|\tilde{g}_\ell\rangle = \frac{1}{\sqrt{q_\ell}}\sum_{\mathbf{z}\in G_\ell} b_{\mathbf{z}}(-1)^{\mathbf{x}\cdot\mathbf{z}}|\mathbf{z}\rangle. \tag{13}$$

The states $|\tilde{g}_k\rangle$ and $|\tilde{h}_\ell\rangle$ satisfy the relationship

$$\langle\tilde{h}_\ell|\tilde{g}_k\rangle = \begin{cases} A_k & \text{if } k = \ell \\ 0 & \text{otherwise} \end{cases}, \tag{14}$$

where $A_k = \frac{1}{q_k}\sum_{\mathbf{z}\in G_k}|b_{\mathbf{z}}|^2(-1)^{\mathbf{x}\cdot\mathbf{z}}$ and is a real constant. Owing to the orthogonality of the blocks in the block decomposition of $\mathcal{E}(\hat{\rho}_{\mathbf{0}})$ and $\mathcal{E}(\hat{\rho}_{\mathbf{x}})$, we can express the trace distance between them as a sum across blocks. Let $\widehat{O}_k := |\tilde{h}_k\rangle\langle\tilde{h}_k| + |\tilde{g}_k\rangle\langle\tilde{g}_k| - A_k|\tilde{h}_k\rangle\langle\tilde{g}_k| - A_k|\tilde{g}_k\rangle\langle\tilde{h}_k|$. Then

$$D(\mathcal{E}(\hat{\rho}_{\mathbf{u}}),\mathcal{E}(\hat{\rho}_{\mathbf{v}})) = \frac{1}{2}\sum_{k=0}^{d-1} q_k \text{tr}\left(\sqrt{\widehat{O}_k}\right) = \sum_{k=0}^{d-1} q_k\sqrt{1 - A_k^2}, \tag{15}$$

where $1 - A_k^2$ is the eigenvalue of $\hat{O}_k$ of multiplicity 2 (please see Appendix A for derivation).

In the limit $d \to \infty$, we can drop the modulus in $\phi(\mathbf{z})$ and use the multinomial theorem to simplify q_k and A_k. We have

$$q_k \overset{d\to\infty}{=} e^{-m|\alpha|^2}\frac{(m|\alpha|^2)^k}{k!} \tag{16}$$

and

$$A_k \overset{d\to\infty}{=} \frac{1}{q_k}[m - 2\text{wt}(\mathbf{x})]^k e^{-m|\alpha|^2}\frac{|\alpha|^{2k}}{k!}, \tag{17}$$

respectively, where wt($\mathbf{x}$) is the Hamming weight of $\mathbf{x} = \mathbf{u} \oplus \mathbf{v}$. Details of the derivation of q_k and A_k are given in Appendix B. If d is finite, the modulus in the definition of the function $\phi(\mathbf{x})$ prevents us from using the multinomial theorem, and these results would not apply. Explicitly, we have

$$D(\mathcal{E}(\hat{\rho}_{\mathbf{v}}),\mathcal{E}(\hat{\rho}_{\mathbf{u}})) \overset{d\to\infty}{=} \sum_{k=1}^{\infty}\frac{e^{-E}E^k\sqrt{1 - \left(\frac{m-2\text{wt}(\mathbf{x})}{m}\right)^{2k}}}{k!}, \tag{18}$$

where $E = m|\alpha|^2$, and once again $\mathbf{x} = \mathbf{u} \oplus \mathbf{v}$.

For comparison, we compute the trace distance between the unencrypted states $\hat{\rho}_{\mathbf{u}}$ and $\hat{\rho}_{\mathbf{v}}$ which is equal to that between the unencrypted states $\hat{\rho}_{\mathbf{x}}$ and $\hat{\rho}_{\mathbf{0}}$ for $\mathbf{x} = \mathbf{u} \oplus \mathbf{v}$, because of the

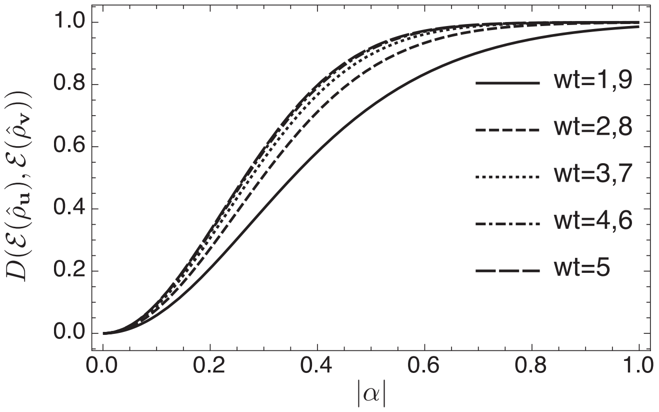

FIG. 2. A plot of $D(\mathcal{E}(\hat{\rho}_{\mathbf{u}}),\mathcal{E}(\hat{\rho}_{\mathbf{v}}))$ vs $|\alpha|$ for $m = 10$ and $d = 100$, and for various values of $w = \mathrm{wt}(\mathbf{u} \oplus \mathbf{v})$.

invariance of the trace distance under a unitary transformation. This trace distance can be expressed in terms of a rank matrix $\hat{Q} := |\psi_{\mathbf{x}}\rangle\langle\psi_{\mathbf{x}}| + |\psi_{\mathbf{0}}\rangle\langle\psi_{\mathbf{0}}| - B\,|\psi_{\mathbf{x}}\rangle\langle\psi_{\mathbf{0}}| - B\,|\psi_{\mathbf{0}}\rangle\langle\psi_{\mathbf{x}}|$, where $B := e^{-2\mathrm{wt}(\mathbf{x})|\alpha|^2}$. Specifically

$$D(\hat{\rho}_{\mathbf{u}},\hat{\rho}_{\mathbf{v}}) = \tfrac{1}{2}\mathrm{tr}\left(\sqrt{\hat{Q}}\right) = \sqrt{1-B^2}$$
$$= \sqrt{1-e^{-4\mathrm{wt}(\mathbf{x})|\alpha|^2}}, \qquad (19)$$

where $1 - B^2$ is the eigenvalue of $\hat{Q}$ (see Appendix A for derivation). The trace distances in Eqs. (18) and (19) are plotted for strings of length $m = 10$ in Figs. 2 and 3, respectively. Figure 2 was calculated using an encryption key with $d = 100$.

The qualitative behaviors of the trace distances with and without encryption are quite similar, with the trace distance vanishing as $|\alpha| \to 0$, while approaching its maximum value of unity as $|\alpha|$ grows. However, quantitatively, the trace distances are suppressed for the encrypted states (see Fig. 4) and have a lower spread over the different $\mathrm{wt}(\mathbf{x})$ values. The encryption would make it harder for an adversary to distinguish between the different encoded states, thus providing some modest security. There is a tradeoff between security and the amount of transmitted accessible information, and we recommend a transmission that has a small but nonzero amplitude. In this regime, the operations allowed for our scheme are believed to be still of hard sampling complexity [39].

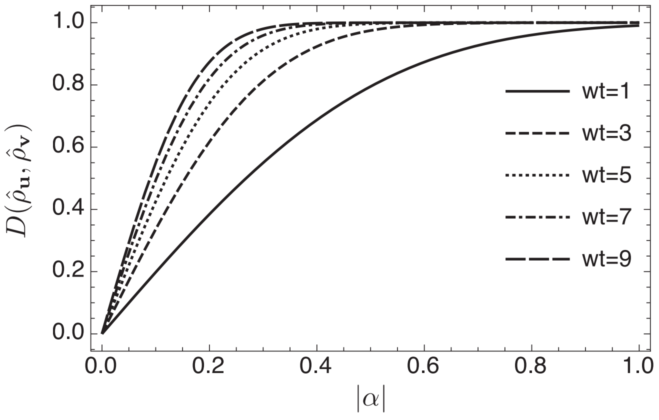

FIG. 3. A plot of $D(\hat{\rho}_{\mathbf{u}},\hat{\rho}_{\mathbf{v}})$ vs $|\alpha|$ for $m = 10$ and $d = 100$, and for various values of $w = \mathrm{wt}(\mathbf{u} \oplus \mathbf{v})$.

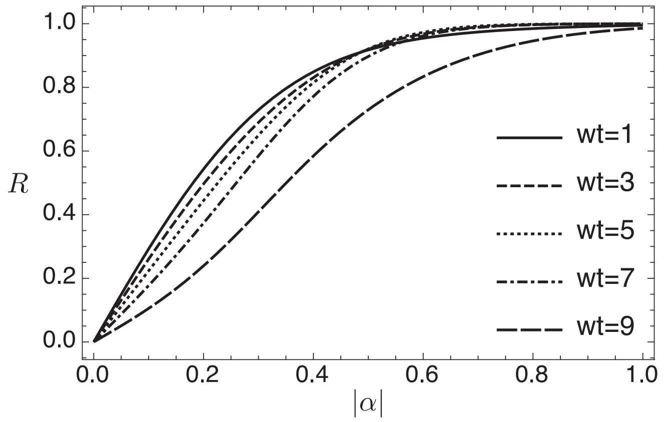

FIG. 4. A plot of $R = D(\mathcal{E}(\hat{\rho}_{\mathbf{u}}),\mathcal{E}(\hat{\rho}_{\mathbf{v}}))/D(\hat{\rho}_{\mathbf{u}},\hat{\rho}_{\mathbf{v}})$ vs $|\alpha|$ for $m = 10$ and $d = 100$ for various weights $w = \mathrm{wt}(\mathbf{u} \oplus \mathbf{v})$ values. The values of R are less than unity indicating a suppression of distinguishability by the encryption operation.

Let $R := D(\mathcal{E}(\hat{\rho}_{\mathbf{u}}),\mathcal{E}(\hat{\rho}_{\mathbf{v}}))/D(\hat{\rho}_{\mathbf{u}},\hat{\rho}_{\mathbf{v}})$, and $E := m|\alpha|^2$. We plot R versus m for (i) $E = 1.0$ and (ii) $E = m^r$, where $r = 0.3$ in Fig. 5. The ratios are less than unity, indicating that the trace distances are suppressed for the encrypted states. However, as the ratios increase with m, this suppression diminishes with an increasing length of the encoded string in both energy regimes.

The corresponding lower bounds on $I(\mathbf{x};\mathbf{y}_{\mathrm{PGM}})$ are plotted in Fig. 6, which shows $I(\mathbf{x};\mathbf{y}_{\mathrm{PGM}})$ increasing with m for both (i) $E = 1.0$ and $E = m^r$ where $r = 0.3$. This means that in these regimes of E someone with the secret key can send more information with increasing code length.

One might hope for an energy regime in which $I(\mathbf{x};\mathbf{y}_{\mathrm{PGM}})$ increases, while the ratio R vanishes with increasing m. However, this does not seem to be possible. Our scheme is still useful in situations where secure delegated quantum processing is desired when constrained to preparing simple resources like coherent states, and to short code words.

VI. CONCLUSION

In this paper, we present a homomorphic encryption scheme that allows processing on logical qubits encoded onto coherent

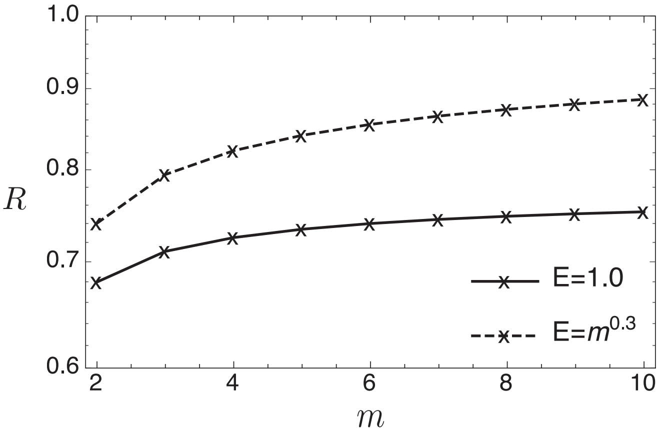

FIG. 5. A plot of R vs m with fixed $\mathrm{wt}(\mathbf{x}) = 1$ strings, where $\mathbf{x} = \mathbf{u} \oplus \mathbf{v}$, and $d = 100$ for (i) $E = 1.0$ and (ii) $E = m^r$, where $r = 0.3$.

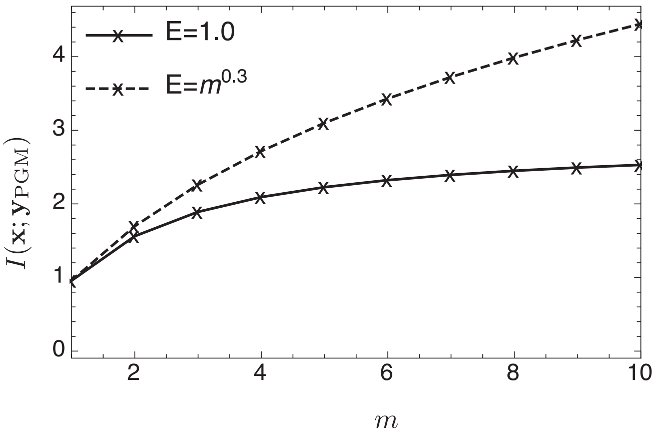

FIG. 6. A plot of $I(\mathbf{x};\mathbf{y}_{\mathrm{PGM}})$ vs m with $d = 100$, and fixed wt($\mathbf{x}$) = 1 strings for (i) $E = 1.0$ and (ii) $E = m^r$, where $r = 0.3$.

states while encrypted by a random rotation in phase space. Although the input states are classical, the set of allowed quantum operations is hard to simulate classically. We analyzed the security of our scheme through the trace distance of any two encrypted code words and showed that there exist regimes of coherent-state amplitudes and bit-string length in which the trace distance can be suppressed, indicating increased security afforded by the encryption. Our scheme is readily implementable with existing optical network technology, and is useful as a primitive for secure delegated quantum computing using continuous-variable resources.

ACKNOWLEDGMENTS

The authors would like to thank J. F. Fitzsimons for useful discussions. This research was supported in part by Singapore National Research Foundation Award No. NRF-NRFF2013-01. This research was conducted by the Australian Research Council Centre of Excellence for Engineered Quantum Systems (Project No. CE110001013). P.P.R. acknowledges financial support from Lockheed Martin, and is funded by an Australian Research Council (ARC) Future Fellowship (Project No. FT160100397). S.T. acknowledges support from the US Air Force Office of Scientific Research under Asian Office of Aerospace Research and Development (AOARD) Grant No. FA2386-15-1-4082.

APPENDIX A: CALCULATION OF EIGENVALUES

Let $|x\rangle$ and $|y\rangle$ be normalized states that are not orthogonal to one another. Let $|z\rangle$ be a normalized state that is orthogonal to $|x\rangle$ and in the plane spanned by $|x\rangle$ and $|y\rangle$. One can write $|y\rangle$ in terms of $|x\rangle$ and $|z\rangle$ as

$$\begin{aligned} |y\rangle &= (|x\rangle\langle x| + |z\rangle\langle z|)|y\rangle \\ &= |x\rangle\cos\theta + |z\rangle\sin\theta, \end{aligned} \tag{A1}$$

where $\cos\theta = \langle x|y\rangle$ and $\sin\theta = \langle z|y\rangle$. Then a given matrix

$$M = |x\rangle\langle x| - C|x\rangle\langle y| - C|y\rangle\langle x| + |y\rangle\langle y| \tag{A2}$$

can be rewritten in terms of $|x\rangle$ and $|z\rangle$ as

$$\begin{aligned} M &= |x\rangle\langle x|(1 - 2C\cos\theta + \cos^2\theta) \\ &\quad + |x\rangle\langle z|(-C\sin\theta + \sin\theta\cos\theta) \\ &\quad + |z\rangle\langle x|(-C\sin\theta + \sin\theta\cos\theta) \\ &\quad + |z\rangle\langle z|\sin^2\theta, \end{aligned} \tag{A3}$$

for which its eigenvalues are $\lambda_\pm = (1 \pm C)(1 \mp \cos\theta)$.

When $M = \hat{O}_k$, $C = A_k$, and $\cos\theta = \langle\tilde{g}_k|\tilde{h}_k\rangle = A_k$, we have $\lambda_+ = \lambda_- = 1 - A_k^2$. When $M = \hat{Q}$, $C = B$, and $\cos\theta = \langle\psi_{\mathbf{x}}|\psi_{\mathbf{0}}\rangle = B$, we have $\lambda_+ = \lambda_- = 1 - B^2$.

APPENDIX B: CALCULATION OF q_k AND A_k IN THE LIMIT $d \to \infty$

In the limit $d \to \infty$, we can drop the modulus in $\phi(\mathbf{z})$ and use the multinomial theorem to simplify q_k and A_k. We have

$$\begin{aligned} q_k &\overset{d\to\infty}{=} \sum_{\substack{\mathbf{z}\in\mathbb{N}^m \\ z_1+\ldots+z_m=k}} e^{-m|\alpha|^2}\frac{|\alpha|^{2(z_1+\ldots+z_m)}}{z_1!z_2!\ldots z_m!} \\ &= \sum_{\substack{\mathbf{z}\in\mathbb{N}^m \\ z_1+\ldots+z_m=k}} e^{-m|\alpha|^2}\frac{|\alpha|^{2k}}{k!}\binom{k}{z_1!z_2!\ldots z_m!} \\ &= e^{-m|\alpha|^2}\frac{(m|\alpha|^2)^k}{k!}, \end{aligned} \tag{B1}$$

where $\binom{k}{z_1,z_2,\ldots,z_m} := \frac{k!}{z_1!z_2!\ldots z_m!}$ is the multinomial coefficient and

$$\begin{aligned} A_k &\overset{d\to\infty}{=} \frac{1}{q_k}\sum_{\substack{\mathbf{z}\in\mathbb{N}^m \\ z_1+\ldots+z_m=k}} e^{-m|\alpha|^2}\frac{|\alpha|^{2(z_1+\ldots+z_m)}}{z_1!\ldots z_m!}(-1)^{\mathbf{x}\cdot\mathbf{z}} \\ &= \frac{1}{q_k}\sum_{\substack{\mathbf{z}\in\mathbb{N}^m \\ z_1+\ldots+z_m=k}} e^{-m|\alpha|^2}\frac{|\alpha|^{2k}}{k!}\binom{k}{z_1,z_2,\ldots,z_m}(-1)^{\mathbf{x}\cdot\mathbf{z}} \\ &= \frac{1}{q_k}e^{-m|\alpha|^2}\frac{|\alpha|^{2k}}{k!}\left[(-1)^{x_1} + \ldots + (-1)^{x_m}\right]^k \\ &= \frac{1}{q_k}[m - 2\mathrm{wt}(\mathbf{x})]^k e^{-m|\alpha|^2}\frac{|\alpha|^{2k}}{k!}, \end{aligned} \tag{B2}$$

respectively, where wt($\mathbf{x}$) is the Hamming weight of $\mathbf{x}$.

[1] R. L. Rivest, L. Adleman, and M. L. Dertouzos, *Foundations of Secure Computation* (Academic, New York, 1978), pp. 169–179.

[2] C. Gentry, in *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*, STOC '09 (ACM, New York, 2009), pp. 169–178.

[3] M. van Dijk, C. Gentry, S. Halevi, and V. Vaikuntanathan, in *Advances in Cryptology EUROCRYPT 2010*, edited by H. Gilbert, Lecture Notes in Computer Science Vol. 6110 (Springer, Berlin, 2010), pp. 24–43.

[4] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist, Phys. Rev. Lett. **109**, 150501 (2012).

[5] S.-H. Tan, J. A. Kettlewell, Y. Ouyang, L. Chen, and J. F. Fitzsimons, Sci. Rep. **6**, 33467 (2016).

[6] Y. Ouyang, S.-H. Tan, and J. Fitzsimons, arXiv:1508.00938 (2015).

[7] A. Broadbent, J. Fitzsimons, and E. Kashefi, in 50th Annual IEEE Symposium on Foundations of Computer Science (2009), pp. 517–526.

[8] M. Liang, Quant. Info. Proc. **12**, 3675 (2013).

[9] M. Liang, Quant. Info. Proc. **14**, 2749 (2015).

[10] K. A. G. Fisher, A. Broadbent, L. K. Shalm, Z. Yan, J. Lavoie, R. Prevedel, T. Jennewein, and K. J. Resch, Nat. Commun. **5**, 3074 (2014).

[11] A. M. Childs, Quantum Info. Comput. **5**, 456 (2005).

[12] A. Broadbent and S. Jeffery, Advances in Cryptology **9216**, 609 (2015).

[13] Y. Dulek, C. Schaffner, and F. Speelman, in *Advances in Cryptology—CRYPTO 2016*, edited by M. Robshaw and J. Katz (Springer, Berlin, 2016), pp. 3–32.

[14] G. Alagic, Y. Dulek, C. Schaffner, and F. Speelman, in *Advances in Cryptology—ASIACRYPT 2017*, edited by T. Takagi and T. Peyrin (Springer, New York, 2017), pp. 438–467.

[15] L. Yu, C. A. Pérez-Delgado, and J. F. Fitzsimons, Phys. Rev. A **90**, 050303 (2014).

[16] M. Newman and Y. Shi, arXiv:1704.07798v1 (2017).

[17] S. Aaronson and A. Arkhipov, The computational complexity of linear optics, in *Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing, San Jose, California*, STOC'11 (ACM, New York, 2011), pp. 333–342.

[18] M. A. Broome, A. Fedrizzi, S. Rahimi-Keshari, J. Dove, S. Aaronson, T. C. Ralph, and A. G. White, Science **339**, 794 (2013).

[19] J. B. Spring, B. J. Metcalf, P. C. Humphreys, W. S. Kolthammer, X.-M. Jin, M. Barbieri, A. Datta, N. Thomas-Peter, N. K. Langford, D. Kundys *et al.*, Science **339**, 798 (2013).

[20] M. Tillmann, B. Dakic, R. Heilmann, S. Nolte, A. Szameit, and P. Walther, Nat. Photonics **7**, 540 (2013).

[21] A. Crespi, R. Osellame, R. Ramponi, D. J. Brod, E. F. Galvao, N. Spagnolo, C. Vitelli, E. Maiorino, P. Mataloni, and F. Sciarrino, Nat. Photonics **7**, 545 (2013).

[22] T. C. Ralph, A. Gilchrist, G. J. Milburn, W. J. Munro, and S. Glancy, Phys. Rev. A **68**, 042319 (2003).

[23] H. Jeong and M. S. Kim, Phys. Rev. A **65**, 042305 (2002).

[24] A. Tipsmark, R. Dong, A. Laghaout, P. Marek, M. Ježek, and U. L. Andersen, Phys. Rev. A **84**, 050301(R) (2011).

[25] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **90**, 042335 (2014).

[26] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[27] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[28] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[29] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, New J. Phys. **17**, 053014 (2015).

[30] G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen, Phys. Rev. Lett. **90**, 227901 (2003).

[31] R. Nair, H. P. Yuen, E. Corndorf, T. Eguchi, and P. Kumar, Phys. Rev. A **74**, 052309 (2006).

[32] M. M. Wilde, *Quantum Information Theory*, 1st ed. (Cambridge University, Cambridge, England, 2013).

[33] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).

[34] Y. Aharonov, L. Davidovich, and N. Zagury, Phys. Rev. A **48**, 1687 (1993).

[35] P. P. Rohde, A. Schreiber, M. Štefaňák, I. Jex, and C. Silberhorn, New J. Phys. **13**, 013001 (2011).

[36] C. Gerry and P. Knight, *Introductory Quantum Optics*, 1st ed. (Cambridge University, Cambridge, England, 2004).

[37] S. D. Bartlett, B. C. Sanders, S. L. Braunstein, and K. Nemoto, Phys. Rev. Lett. **88**, 097904 (2002).

[38] B. Yurke and D. Stoler, Phys. Rev. Lett. **57**, 13 (1986).

[39] P. P. Rohde, K. R. Motes, P. A. Knott, J. Fitzsimons, W. J. Munro, and J. P. Dowling, Phys. Rev. A **91**, 012342 (2015).