PHYSICAL REVIEW A **90**, 042335 (2014)

Quantum communication with coherent states and linear optics

Juan Miguel Arrazola and Norbert Lütkenhaus
Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, 200 University Avenue West, Waterloo, Ontario, Canada N2L 3G1

(Received 23 July 2014; published 29 October 2014)

We introduce a general mapping for encoding quantum communication protocols involving pure states of multiple qubits, unitary transformations, and projective measurements into another set of protocols that employ a coherent state of light in a linear combination of optical modes, linear-optics transformations, and measurements with single-photon threshold detectors. This provides a general framework for transforming protocols in quantum communication into a form in which they can be implemented with current technology. We explore the similarity between properties of the original qubit protocols and the coherent-state protocols obtained from the mapping and make use of the mapping to construct additional protocols in the context of quantum communication complexity and quantum digital signatures. Our results have the potential of bringing a wide class of quantum communication protocols closer to their experimental demonstration.

DOI: 10.1103/PhysRevA.90.042335 PACS number(s): 03.67.Hk, 42.50.Ex, 89.70.Hj

I. INTRODUCTION

What information-processing tasks are unachievable in a classical world but become possible when exploiting the intrinsic quantum-mechanical properties of physical systems? This question has been a driving force of numerous research endeavors over the last few decades and remarkable progress has been made in our understanding of the advantages that quantum mechanics can provide, as well as in developing the experimental platforms that will allow them to be realized in practice [1–4]. An example is the field of quantum communication [5], where quantum systems can be used, for instance, to distribute secret keys [6,7] or reduce the amount of communication required for joint computations [8–11].

In terms of experimental implementations, only quantum key distribution (QKD) has been routinely demonstrated and deployed over increasingly complex networks and large distances [12,13]. This is possible largely due to the fact that, fundamentally, QKD can be carried out with sequences of independent signals and measurements [4]. Other tasks typically require sophisticated quantum states to be prepared and transmitted as well as having complex operations performed on them. Overall, there is a large set of quantum communication protocols whose potential advantages currently escape the grasp of available technology, with only a few proof-of-principle implementations having been reported [14–16].

Confronted with these challenges we face two alternatives: We can either strive to improve current technology or we can flip the issue around and ask: Can protocols in quantum communication be adapted to a form that makes them ready to be deployed with available techniques? To adopt the latter strategy is to push for a theoretical reformulation that converts previously intractable protocols into a form that, while conserving their relevant features, eliminates the obstacles affecting their implementation. This is precisely the road that has already been successfully followed for QKD.

In this work, we describe an abstract mapping that converts quantum communication protocols that use pure states of multiple qubits, unitary operations, and projective measurements into another class of protocols that use only a sequence of coherent states, linear-optics operations, and measurements with single-photon threshold detectors. This class of protocols requires a number of optical modes equal to the dimension of the original states, but the total number of photons can be chosen independently of the dimension and is typically very small. The protocols obtained from the mapping share important properties with the original ones, meaning that they can also fulfill the goal that the original protocols where intended to achieve. Overall, the mapping is suitable for its application to quantum communication protocols that originally require a moderate number of qubits, but are still hard to implement with the usual methods.

In the remainder of this paper, we describe the mapping in detail and discuss the various properties of the coherent-state protocols. We proceed by examining how the mapping can be applied to construct protocols in quantum communication complexity and describe protocols for the hidden matching problem and for quantum digital signatures, both of which can be realized with technology that is within current reach.

II. COHERENT-STATE MAPPING

We consider a wide class of quantum communication protocols that require only three basic operations: the preparation of pure states of a fixed dimension, unitary transformations on these states, and projective measurements on a canonical basis. The simplest form of a protocol in this class is one in which Alice prepares a state $|\psi\rangle$ and sends it to Bob, who then applies a unitary transformation U_B to that state, followed by a projective measurement on the canonical basis. More complex protocols can be constructed by increasing the number of these basic operations as well as the number of parties. Even though these protocols generally involve states of some arbitrary dimension d, it is common to think of them as corresponding to a system of $O(\log_2 d)$ qubits. Hence, we refer to them as *qubit protocols*.

An *exact* implementation of such protocols can be achieved without the use of actual physical qubits by instead considering a single photon in a linear combination of optical modes. Any pure state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$, with $\sum_{k=1}^{d} |\lambda_k|^2 = 1$, can be equally thought of as the state of a single photon in a linear

combination of d modes,

$$a_{\psi}^{\dagger}|0\rangle = \sum_{k=1}^{d} \lambda_k |1\rangle_k, \tag{1}$$

where $a_{\psi}^{\dagger} = \sum_{k=1}^{d} \lambda_k b_k^{\dagger}$ for a collection of creation operators $\{b_1, b_2, \ldots, b_d\}$ corresponding to d optical modes, and where $|1\rangle_k$ is the state of a single photon in the kth mode.

In this picture, unitary operations correspond exactly to linear-optics transformations [17], and measurements in the canonical basis are equivalent to a photon-counting measurement in each of the modes. Note that the quantum information is encoded by photons residing in linear combinations of modes.

From a practical perspective, the issue with implementing qubit protocols in terms of a single photon in a linear combination of modes is that the experimental preparation of these states presents daunting challenges. Instead, we are interested in an adaptation of this formulation of qubit protocols into another that is more readily implementable in practice. As discussed in Ref. [18], as an alternative to a single photon we can consider a single coherent state in a linear combination of modes. In that case, instead of the state of Eq. (1), we have

$$D_{a_{\psi}}(\alpha)|0\rangle = \bigotimes_{k=1}^{d} |\alpha\, \lambda_k\rangle_k, \tag{2}$$

where $D_{a_{\psi}}(\alpha) = \exp(\alpha a_{\psi}^{\dagger} - \alpha^* a_{\psi})$ is the displacement operator. Once again, the quantum information is encoded in the mode structure, but we have a coherent state instead of the single photon of Eq. (1) as the quantum state of light. Remarkably, this state is equivalent to a sequence of coherent states over d optical modes.

With this idea in mind, we now outline a method for converting qubit protocols into another class of protocols that, although seemingly disparate, actually retain the essential properties of the original ones. We call these *coherent-state protocols* since they can be implemented by using only coherent states of light and linear-optics operations. The recipe for constructing coherent-state protocols is specified by the following rules:

Coherent-state mapping

(1) The original Hilbert space $\mathcal{H}$ of dimension d with canonical basis $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ is mapped to a set of d orthogonal optical modes with corresponding annihilation operators $\{b_1, b_2, \ldots, b_d\}$:

$$|k\rangle \longrightarrow b_k. \tag{3}$$

(2) A state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$ is mapped to a coherent state with parameter α in the mode $a_{\psi} = \sum_{k=1}^{d} \lambda_k b_k$:

$$|\psi\rangle \longrightarrow |\alpha, \psi\rangle := \bigotimes_{k=1}^{d} |\alpha\, \lambda_k\rangle_k,$$

where $|\alpha\, \lambda_k\rangle_k$ is a coherent state with parameter $\alpha\, \lambda_k$ in the kth mode. The value of the amplitude α can be chosen freely as a parameter of the mapping, independently of the dimension d, but remains fixed.

(3) A unitary operation U acting on a state in $\mathcal{H}$ is mapped into a linear-optics transformation corresponding to the same unitary operator U acting on the modes $\{b_1, b_2, \ldots, b_d\}$. Thus, the transformation of a state is linked to a transformation of the modes as

$$|\psi'\rangle = U|\psi\rangle \longrightarrow b_k = \sum_{l} U_{kl} b'_l. \tag{4}$$

This linear-optics network has the effect of transforming the coherent state $|\alpha, \psi\rangle = \bigotimes_{k=1}^{d} |\alpha\, \lambda_k\rangle_k$ to the state

$$|\alpha, \psi'\rangle = \bigotimes_{k=1}^{d} |\alpha\, \lambda'_k\rangle_k, \tag{5}$$

where $\lambda'_k = \sum_l U_{kl} \lambda_l$. This is the same state obtained from applying the mapping directly to the output state $|\psi'\rangle$ of the original protocol.

(4) A projective measurement in the canonical basis $\{|1\rangle, |2\rangle, \ldots, |d\rangle\}$ is mapped into a two-outcome measurement in each of the modes with single-photon threshold detectors:

$$\{|1\rangle\langle 1|, |2\rangle\langle 2|, \ldots, |d\rangle\langle d|\} \longrightarrow \left\{ \bigotimes_{k=1}^{d} F_c^k \right\}, \tag{6}$$

where $c =$ "click," or "no click," $F^k_{\text{no click}} = |0\rangle\langle 0|$ is a projection onto the vacuum, $F^k_{\text{click}} = \sum_{n=1}^{\infty} |n\rangle_k \langle n|_k$, and $|n\rangle_k$ is a state with n photons in the kth mode. As such, an outcome in a coherent-state protocol corresponds to a pattern of clicks across the modes.

Since any qubit protocol can be constructed from the basic operations of state preparation, unitary transformations, and projective measurements, the above instructions are sufficient to construct the coherent-state version of any qubit protocol. However, as there are 2^d possible outcomes compared to the d possible outcomes of the qubit protocol, the interpretation of the outcomes in the coherent-state protocol is not immediately provided by the mapping. Nevertheless, as will be discussed later, the statistics closely resemble those of the original protocol and they can be thought of as arising from several independent runs of the original qubit protocol. As an illustration, a simple qubit protocol and its coherent-state counterpart are depicted in Fig. 1.

An immediate appealing property of coherent-state protocols is that their implementation faces much smaller obstacles than their qubit counterparts. Indeed, the fundamental challenge of a quantum-optical implementation of qubit protocols lies in the difficulty of generating entangled states of many qubits and performing global unitary transformations on them. On the other hand, coherent-state protocols face significantly less daunting obstacles. The experimental generation of coherent states is a commonplace task and the construction of linear-optical circuits can, in principle, be realized with simple devices such as beam splitters and phase shifters [17], although experimental challenges may remain depending on the required unitary operation. Moreover, the platforms for linear-optics experiments continue to improve at a fast rate, most notably with the development of integrated optics [19].

As we have mentioned already, an advantage of coherent-state protocols is that they employ a coherent state in a linear combination of modes, which is equivalent to a tensor

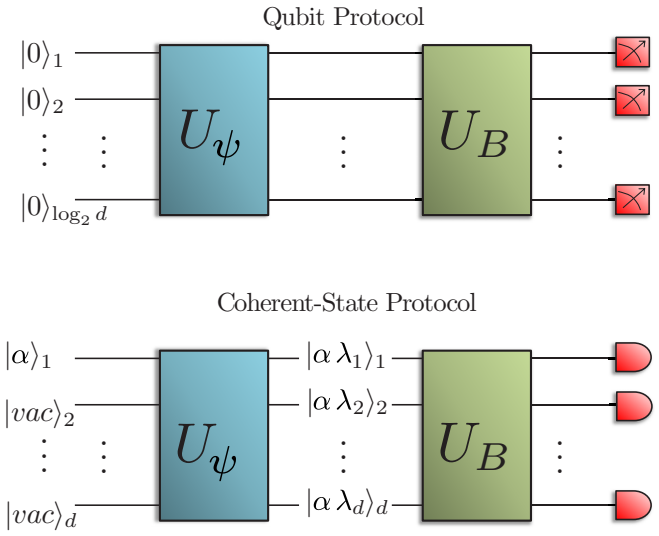

FIG. 1. (Color online) In a simple qubit protocol, Alice prepares a state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k |k\rangle$ of $\log_2 d$ qubits by applying a unitary transformation U_ψ on an inital state $|\bar{0}\rangle := |0\rangle^{\otimes \log_2 d}$. She sends the state to Bob, who applies a unitary transformation U_B and measures the resulting state in the computational basis. In the equivalent coherent-state protocol, the initial state corresponds to a coherent state in a single mode and the vacuum on the others. The state $|\alpha,\psi_x\rangle = \bigotimes_{k=1}^{d} |\alpha\,\lambda_k\rangle_k$ is prepared by applying the transformation U_ψ to the optical modes. This state is sent to Bob, who applies the transformation U_B and consequently measures each mode for the presence of photons with threshold single-photon detectors.

product of individual coherent states across the various modes. However, qubit protocols usually require high amounts of entanglement. This seems to indicate that the "quantumness" of the original qubit protocol has been lost through the mapping. Nevertheless, it is important to realize that this is not the case, as coherent-state protocols showcase a truly quantum property: nonorthogonality. Given two states $|\alpha,\psi\rangle = \bigotimes_{k=1}^{d} |\alpha\,\lambda_k\rangle_k$ and $|\alpha,\varphi\rangle = \bigotimes_{k=1}^{d} |\alpha\,\nu_k\rangle_k$, with $d \gg |\alpha|^2$, the amplitude of the individual coherent states will typically satisfy $|\alpha\,\lambda_k| \sim |\frac{\alpha}{\sqrt{d}}| \ll 1$. Therefore, the inner product of the individual states obeys

$$|\langle \alpha\,\nu_k|\alpha\,\lambda_k\rangle|^2 = e^{-|\alpha(\lambda_k-\nu_k)|^2} \approx 1, \tag{7}$$

and so the individual states are typically highly nonorthogonal. In fact, it can be useful to intuitively think of the coherent-state mapping as an exchange between entanglement and nonorthogonality, since an implementation of qubit protocols with actual physical qubits usually requires entanglement among the qubits.

In coherent-state protocols, the average photon number $|\alpha|^2$ is a parameter that can be chosen independently of the dimension of the states of the original qubit protocol. This is to be put in contrast with any quantum protocol that encodes a qubit in the degrees of freedom of a photon, which inevitably requires a number of photons that scales with the dimension of the states. Hence, coherent-state protocols offer an intrinsic saving in the number of photons required for their implementation. The drawback, of course, is that the required number of optical modes is equal to the dimension of the states in the original protocol. This implies that the mapping will lead to practical protocols only if the dimension of the original states is comparable to the number of modes that can be efficiently manipulated with existing technologies.

Fortunately, current laser sources can operate with clock rates of at least 1 GHz [20], permitting the generation of a very large number of modes per second. This makes it possible in practice to apply the mapping to quantum communication protocols involving states of a moderate number of qubits. As we discuss in Secs. III and IV, there are many qubit protocols to which we can apply the mapping that require only a modest number of qubits but still currently escape the grasp of direct implementations. From a theoretical perspective, the relationship between these two types of protocol may provide an insight into the trade-offs between different resources in quantum communication, as well as into the interplay between entanglement and nonorthogonality in quantum mechanics.

Now that we have specified how to construct coherent-state protocols, our goal is to understand their properties. We pay special attention to their resemblance to qubit protocols, but also concentrate on understanding the features that may provide an advantage over their qubit counterparts or find applications in quantum communication.

Transmitted information. We are often interested in quantifying the amount of transmitted information, i.e., the amount of communication, that takes place in a quantum protocol. Informally, this is done by counting the number of qubits that are employed. But what happens if a protocol uses physical systems that are manifestly *not* qubits? In that case, we quantify the transmitted information in terms of the smallest number of qubits that would be required, in principle, to replicate the performance of the protocol. More precisely, if a quantum protocol uses states in a Hilbert space of dimension d, this space can be associated with a system of $O(\log_2 d)$ qubits. Therefore, the amount of communication C in a quantum protocol is generally given by

$$C = \log_2[\dim(\mathcal{H})], \tag{8}$$

where $\mathcal{H}$ is the smallest Hilbert space containing all states of the protocol, which can be significantly smaller than the entire Hilbert space associated with the physical systems. Moreover, Holevo's theorem [21] guarantees that no more than $O(\log_2 d)$ classical bits of information could be transmitted, on average, by a quantum protocol that uses states in a Hilbert space of dimension d.

By quantifying the amount of communication carefully, we gain a better understanding of the different physical resources that are required to transmit a certain amount of information. For example, the fact that the same amount of information can be transmitted by a single photon in n optical modes, at most n photons in a single mode, or $\log_2 n$ qubits is understood because the smallest Hilbert space containing all possible states in each of the three cases has the same dimension.

Quantifying the amount of transmitted information in qubit protocols is straightforward. For coherent-state protocols obtained from the mapping, even though the *actual* Hilbert space associated with all possible signal states is large (distinct coherent states are linearly independent), they effectively occupy a small Hilbert space, as is expressed in the following theorem:

Theorem 1 [22]. For any state $|\psi\rangle$ in a Hilbert space of dimension d and for any $\epsilon > 0$, there exists a Hilbert space $\mathcal{H}_\alpha$ of dimension d_α such that

$$\langle\alpha,\psi|P_{\mathcal{H}_\alpha}|\alpha,\psi\rangle \geqslant 1-\epsilon,$$
$$\log_2 d_\alpha = O(\log_2 d),$$

and where $P_{\mathcal{H}_\alpha}$ is the projector onto $\mathcal{H}_\alpha$.

Proof. For a given $\Delta > 0$, we choose $\mathcal{H}_\alpha$ to be the subspace spanned by the set of Fock states $\{|n_1\rangle \otimes |n_2\rangle \otimes \cdots \otimes |n_d\rangle\}$ over d modes whose total photon number $n = \sum_{k=1}^{d} n_k$ satisfies $|n - |\alpha|^2| \leqslant \Delta$. In other words, this is the space of states whose total photon number is close to $|\alpha|^2$.

The dimension of the Hilbert space spanned by states of n photons is equal to the number of distinct ways in which n photons can be distributed into the d different modes. Since the photons are indistinguishable, this quantity is given by the binomial factor $\binom{n+d-1}{d-1}$ [23]. In the case of $\mathcal{H}_\alpha$, there are 2Δ different possible values of n, the largest being $n = |\alpha|^2 + \Delta$. Thus, the dimension d_α of this subspace satisfies

$$d_\alpha \leqslant 2\Delta\binom{|\alpha|^2+\Delta+d-1}{d-1}, \tag{9}$$

which gives

$$\begin{aligned}\log_2 d_\alpha &\leqslant \log_2\left[2\Delta\binom{|\alpha|^2+\Delta+d-1}{d-1}\right]\\ &\leqslant (|\alpha|^2+\Delta)\log_2[(|\alpha|^2+\Delta+d-1)] + \log_2(2\Delta),\end{aligned} \tag{10}$$

which is $O(\log_2 d)$ for any fixed α and Δ.

Now notice that the number $\langle\alpha,\psi|P_{\mathcal{H}_\alpha}|\alpha,\psi\rangle$ is equal to the probability of performing a photon-number measurement on $|\alpha,\psi\rangle$ and obtaining a value n satisfying $|n - |\alpha|^2| \leqslant \Delta$. Since any coherent state $|\alpha,\psi\rangle$ has a Poissonian photon-number distribution with mean $|\alpha|^2$, independently of $|\psi\rangle$, we can use the properties of this distribution to calculate the probability that the measured number of photons lies within the desired range. This probability satisfies [24]

$$P(|n-|\alpha|^2| \geqslant \Delta) \leqslant 2e^{-|\alpha|^2}\left(\frac{e|\alpha|^2}{|\alpha|^2+\Delta}\right)^{|\alpha|^2+\Delta}, \tag{11}$$

which can be made equal to any $\epsilon > 0$ by choosing Δ accordingly while keeping α fixed. ■

Therefore, the fact that the mean photon number $|\alpha|^2$ is fixed in coherent-state protocols leads to the states involved effectively occupying a Hilbert space of dimension that is comparable to that of the original one. This implies that the asymptotic behavior of the amount of transmitted information is the same for both classes of protocols. Moreover, the effectively unused sections of the entire Hilbert space can still be used, in principle, for other purposes such as the transmission of additional classical or quantum information through multiplexing schemes. A method for achieving this in practice is a line for future research.

It is important to note that this correspondence in the transmitted information is not exactly mirrored in terms of the expenditure of physical resources. A coherent-state protocol obtained from the mapping employs d modes but a number of photons that is tunable and independent of this dimension. This is to be put in contrast with any quantum protocol that encodes a qubit in the degrees of freedom of a photon, which employs $O(\log_2 d)$ optical modes and $O(\log_2 d)$ photons.

Outcome probabilities. In qubit protocols, the probability of obtaining an outcome k upon a measurement of a state $|\psi\rangle = \sum_{k=1}^{d} \lambda_k|k\rangle$ is given by

$$p_k = |\langle k|\psi\rangle|^2 = |\lambda_k|^2, \tag{12}$$

with $\sum_{k=1}^{d} p_k = 1$. For coherent-state protocols, the situation is different since we are performing independent measurements on each of the modes. In this case, the individual detector clicks are not mutually exclusive: We can have many clicks across the various modes, or even no clicks at all.

Nevertheless, for the state $|\alpha,\psi\rangle$, the probability distribution of the number of photons in each mode is equivalent to the one obtained from many repetitions of a measurement on the single-photon state $|\psi\rangle = \alpha_\psi^\dagger|0\rangle$ of Eq. (1), where the number of repetitions is drawn from a Poisson distribution with mean $\mu = |\alpha|^2$.

To see this, first note that the state $|\alpha,\psi\rangle$ can be written as

$$|\alpha,\psi\rangle = D_{a_\psi}(\alpha)|0\rangle = e^{-|\alpha|^2}\sum_{n=0}^{\infty}\frac{\alpha^n}{\sqrt{n!}}|n\rangle_{a_\psi}. \tag{13}$$

The state of n photons in mode α_ψ is itself given by

$$|n\rangle_{a_\psi} = \frac{1}{\sqrt{n!}}(\alpha_\psi^\dagger)^n|0\rangle = \frac{1}{\sqrt{n!}}\left(\sum_{k=1}^{d}\lambda_k b_k^\dagger\right)^n|0\rangle. \tag{14}$$

For this state, the probability of obtaining $n_1,n_2,\ldots,n_d$ photons in each of the modes $b_1,b_2,\ldots,b_d$, with $\sum_k n_k = n$, is given by

$$\Pr(n_1,\ldots,n_d) = \frac{n!}{n_1!\cdots n_d!}|\lambda_1|^{2n_1}\cdots|\lambda_d|^{2n_d}, \tag{15}$$

which, from the multinomial theorem, is exactly equal to that obtained from n measurements of the single-photon state $|\psi\rangle = \alpha_\psi^\dagger|0\rangle$. Since the number of photons n in the state $|\alpha,\psi\rangle$ is Poissonian distributed with mean $\mu = |\alpha|^2$, this proves the claim.

Whenever possible, we will not use photon-number-resolving detectors in protocols obtained from coherent-state mapping, but threshold detectors that give clicks or no clicks. Note that while the statistics of photon counts is directly derived from the Poissonian distribution of repetitions of the single-photon protocol, this does not hold for the statistics of clicks of the threshold detectors.

However, for most states, the coefficients λ_k will typically be very small, so that the mean number of photons $|\alpha\,\lambda_k|^2$ will also be small provided α is not too large. Then it is unlikely that more than one photon will be present in each mode, and the number-resolving properties of the detectors are not necessary.

For example, with threshold detectors, the probability of obtaining a click on the kth mode after a measurement of a state $|\alpha,\psi\rangle = \bigotimes_{k=1}^{d}|\alpha\,\lambda_k\rangle_k$ is given by

$$p_{\alpha,k} = 1 - \exp(-|\alpha\,\lambda_k|^2), \tag{16}$$

which for $|\alpha\,\lambda_k| \ll 1$ gives

$$p_{\alpha,k} \approx |\alpha\,\lambda_k|^2. \tag{17}$$

If we choose $|\alpha|^2 = 1$, we recover a behavior very similar to that of the qubit protocol: Only one click is expected to occur and it does so with a probability that is essentially identical to that of the original protocol.

In any case, the multiple-photon property of a coherent-state protocol constitutes a potential advantage over its qubit counterpart. The expected number of clicks can be controlled by modifying α appropriately, and a larger number of clicks will give rise to more information gained per measurement.

State overlap. All of the physically relevant information of a set of quantum states $\{|\psi_1\rangle,|\psi_2\rangle,\ldots,|\psi_N\rangle\}$ is contained in its Gram matrix, which is defined as

$$G_{i,j} = \langle\psi_i|\psi_j\rangle. \tag{18}$$

Thus, for quantum communication protocols defined over a set of possible signal states, it is natural to ask how the overlap between states behaves under a coherent-state mapping. The answer is provided by the following observation.

Observation 1. Let $|\psi\rangle = \sum_k \lambda_k|k\rangle$ and $|\varphi\rangle = \sum_k \nu_k|k\rangle$ be two arbitrary states with overlap $\langle\psi|\varphi\rangle = \delta$. Then the overlap of their coherent-state versions satisfies

$$\delta_\alpha := \langle\psi,\alpha|\varphi,\alpha\rangle = \exp[|\alpha|^2(\delta-1)]. \tag{19}$$

Proof. The overlap of the coherent-state versions is given by

$$\begin{aligned}\langle\psi,\alpha|\varphi,\alpha\rangle &= \prod_k \langle\alpha\,\lambda_k|\alpha\,\nu_k\rangle \\ &= \prod_k \exp\left[-\frac{|\alpha|^2}{2}(|\lambda_k|^2+|\nu_k|^2-2\lambda_k^*\nu_k)\right] \\ &= \exp\left[-\frac{|\alpha|^2}{2}\sum_k(|\lambda_k|^2+|\nu_k|^2-2\lambda_k^*\nu_k)\right] \\ &= \exp\left[|\alpha|^2(\langle\psi|\varphi\rangle-1)\right] \\ &= \exp[|\alpha|^2(\delta-1)],\end{aligned}$$

where we have used the relations $\sum_k |\lambda_k|^2 = \sum_k |\nu_k|^2 = 1$ and $\langle\psi|\varphi\rangle = \sum_k \lambda_k^*\nu_k$. ∎

Once again, there is an added richness in coherent-state protocols, since the overlaps may be adapted by varying the value of the parameter α. For example, in many quantum communication protocols, all overlaps between pairs of states are real numbers, and consequently so are those of their coherent-state versions. In that case, the parameter α can be chosen to increase or decrease the overlap, or to match the exact overlap for a given pair of states. This is illustrated in Fig. 2.

Now that we have outlined the properties of coherent-state protocols, we continue by describing how these techniques can be applied in the construction of protocols in quantum communication complexity and quantum digital signatures.

III. QUANTUM COMMUNICATION COMPLEXITY

Communication complexity is the study of the amount of communication that is required to perform distributed information-processing tasks. This corresponds to the scenario

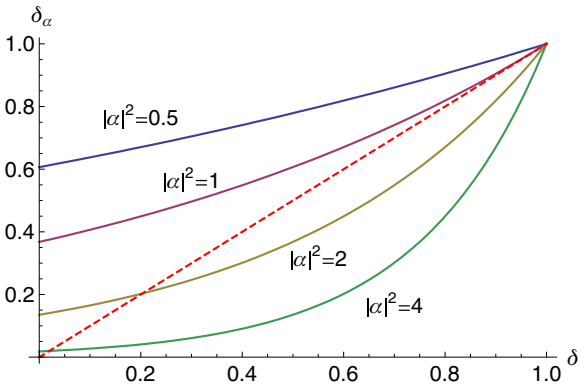

FIG. 2. (Color online) Overlaps of states in coherent-state protocols for different values of the mean photon number $|\alpha|^2$ and choice of real values of δ (implying real values of δ_α). For $|\alpha|^2 < 1$, the overlap δ_α is larger than the original overlap δ. For $|\alpha|^2 \approx 1$, both the original and coherent-state overlaps are close to each other when δ is close to 1 and when $|\alpha|^2$ is large, δ_α can be made smaller than almost any value of the original overlap. In fact, in the limit $\alpha \to \infty$, any two states become orthogonal, while in the limit $\alpha \to 0$ any two states are mapped to the vacuum and thus have unit overlap. Finally, for any $\delta \neq 0$ there exists a value of α such that $\delta = \delta_\alpha$.

in which two parties Alice and Bob respectively receive inputs $x \in \{0,1\}^n$ and $y \in \{0,1\}^n$ and their goal is to collaboratively compute the value of a Boolean function $f(x,y)$ with as little communication as possible [25]. Although they can always do this by communicating their entire input, the pertinent question in communication complexity concerns the minimum amount of communication that is really needed. Likewise, quantum communication complexity studies the case where the parties are allowed to employ quantum resources such as quantum channels and shared entanglement [2,26]. Remarkably, it has been proven that there exist various problems for which the use of quantum resources offers exponential savings in communication compared to their classical counterparts [8–11,27]. In this section, our goal is to employ the mapping to construct protocols that can be implemented using only coherent states and linear optics.

We focus on the bounded-error model in which Alice and Bob have randomness at their disposal and need to determine the value of the function $f(x,y)$ only with probability greater than or equal to $1-\epsilon$ (with $\epsilon < \frac{1}{2}$) even for the worst-case values of x and y. They can send quantum states to each other, apply unitary transformations on these states, and make measurements in the same way as in the quantum communication protocols discussed before. Since they are interested only in learning the value of the function, their final measurement can always be thought of as a projective measurement onto two orthogonal subspaces H_0 and H_1, corresponding to $f(x,y) = 0$ and $f(x,y) = 1$, respectively.

In a coherent-state version of this model, the crucial difference lies in the measurement stage, where the subspaces H_0 and H_1 are mapped onto sets of modes S_0 and S_1, where many clicks can occur. In this case, in order to decide between both values of $f(x,y)$, the strategy is to count the number of clicks that occur in each set of modes. If there are more clicks in the set S_0 than in the set S_1, the output of the protocol

is $f(x,y) = 0$, and vice versa. In this way we map the large number of possible click patterns in the coherent-state protocol to the two outcomes of interest.

We now provide conditions such that, if the original protocol had success probability larger than $1-\epsilon$, its coherent-state version will also have success probability larger than $1-\epsilon$. Let C_b be the random variable corresponding to the number of clicks observed in the set of modes S_b, with $b = 0,1$. The distribution of C_b is known as a Poisson-binomial distribution and its expectation value is given by

$$\mathbb{E}(C_b) = \sum_{k\in S_b} p_{\alpha,k} := \mu_b. \tag{20}$$

This distribution can be difficult to work with in its exact form, so it is usual to approximate it by a Poisson distribution with the same mean. This approximation can be made precise through the following result:

Theorem 2 [28]. Let C_b be a Poisson-binomial random variable with mean μ_b. Similarly, let L_b be a Poisson random variable with the same mean μ_b. Then, for any set A, it holds that

$$|\Pr(C_b \in A) - \Pr(L_b \in A)| \leqslant \min\left(1,\mu_b^{-1}\right)\tau_b, \tag{21}$$

where $\tau_b := \sum_{k\in S_b}(p_{\alpha,k})^2$ and $p_{\alpha,k}$ is the probability of obtaining a click on the kth mode.

We can use this fact to show that, under certain conditions, a coherent-state version of a bounded-error qubit protocol also gives the correct value of the function with bounded error.

Theorem 3. Let a qubit protocol for communication complexity have a probability of success $P_s \geqslant 1-\epsilon$. Then the corresponding coherent-state protocol has a probability of success $P_\alpha > 1-\epsilon$ if there exists a mean photon number $\mu = |\alpha|^2$ such that

$$2e^{-P_s\mu}(2eP_s\mu)^{\mu/2} + \max_{\mu_0,\mu_1}\left\{\min\left(1,\mu_b^{-1}\right)\right\}\tau \leqslant \epsilon, \tag{22}$$

where μ_b is the expected number of clicks in the set of modes S_b and $\tau = \sum_k (p_{\alpha,k})^2$.

Proof. Without loss of generality, we take $f(x,y) = 0$ to correspond to the correct value of the function. We can bound the success probability as

$$\begin{aligned} P_\alpha = \Pr(C_0 > C_1) &\geqslant \Pr\left(C_0 > \frac{\mu}{2}\right)\Pr\left(C_1 < \frac{\mu}{2}\right) \\ &= \left[1 - \Pr\left(C_0 < \frac{\mu}{2}\right)\right]\left[1 - \Pr\left(C_1 > \frac{\mu}{2}\right)\right]. \end{aligned}$$

From Theorem 2 we can also write

$$\begin{aligned} \Pr\left(C_0 < \frac{\mu}{2}\right) &\leqslant \Pr\left(L_0 < \frac{\mu}{2}\right) + \min\left(1,\mu_0^{-1}\right)\tau_0 \\ &\leqslant e^{-\mu_0}\left(\frac{2e\mu_0}{\mu}\right)^{\mu/2} + \min\left(1,\mu_0^{-1}\right)\tau_0, \end{aligned}$$

where we have bounded the Poisson distribution as in Eq. (11). Similarly we have

$$\Pr\left(C_1 > \frac{\mu}{2}\right) \leqslant e^{-\mu_1}\left(\frac{2e\mu_1}{\mu}\right)^{\mu/2} + \min\left(1,\mu_1^{-1}\right)\tau_1.$$

Putting these together we get

$$\begin{aligned} P_\alpha &\geqslant \left[1 - e^{-\mu_0}\left(\frac{2e\mu_0}{\mu}\right)^{\mu/2} - \min\left(1,\mu_0^{-1}\right)\tau_0\right] \\ &\quad\times\left[1 - e^{-\mu_1}\left(\frac{2e\mu_1}{\mu}\right)^{\mu/2} - \min\left(1,\mu_1^{-1}\right)\tau_1\right] \\ &> 1 - e^{-\mu_0}\left(\frac{2e\mu_0}{\mu}\right)^{\mu/2} - e^{-\mu_1}\left(\frac{2e\mu_1}{\mu}\right)^{\mu/2} \\ &\quad - \min\left(1,\mu_0^{-1}\right)\tau_0 - \min\left(1,\mu_1^{-1}\right)\tau_1 \\ &\geqslant 1 - e^{-P_s\mu}(2eP_s\mu)^{\mu/2} - e^{-(1-P_s)\mu}[2e(1-P_s)\mu]^{\mu/2} \\ &\quad - \max_{\mu_0,\mu_1}\left\{\min\left(1,\mu_b^{-1}\right)\right\}\tau, \end{aligned}$$

where $\tau = \tau_0 + \tau_1 = \sum_k (p_{\alpha,k})^2$ and we have used the fact that

$$P_s\mu = \sum_{k\in S_0}|\alpha|^2 p_k > \sum_{k\in S_0}\left(1 - e^{-|\alpha|^2 p_k}\right) = \mu_0 \tag{23}$$

and similarly $(1-P_s)\mu > \mu_1$. Whenever $P_s > 1/2$, it holds that $e^{-P_s\mu}P_s > e^{-(1-P_s)\mu}(1-P_s)$ so we can finally write

$$P_\alpha > 1 - 2e^{-P_s\mu}(2eP_s\mu)^{\mu/2} - \max_{\mu_0,\mu_1}\left\{\min\left(1,\mu_b^{-1}\right)\right\}\tau. \tag{24}$$

From this expression it is clear that whenever condition (22) holds, $P_\alpha > 1-\epsilon$ as desired. ■

Notice that the quantity $2e^{-P_s\mu}(2eP_s\mu)^{\mu/2}$ can be made arbitrarily small for any $P_s > 1-\epsilon$ by choosing a large enough value of $\mu = |\alpha|^2$. However, large values of μ result in higher values of the individual click probabilities $\{p_{\alpha,k}\}$, and consequently larger values of $\tau = \sum_k (p_{\alpha,k})^2$, making it harder for the quantity $\max_{\mu_0,\mu_1}\{\min(1,\mu_b^{-1})\}\tau$ to be small. Therefore, condition (22) will be satisfied only when the original probabilities $\{p_i\}$ are very small, as this results in a small τ even when μ is large. Of course, whenever the communicated states lie in a Hilbert space of large dimension, we expect the outcome probabilities to be small and the coherent-state protocol to function adequately.

We are interested in applying the coherent-state mapping to known protocols in quantum communication complexity. In fact, this has already been demonstrated in Ref. [22], where, essentially, a coherent-state mapping was used to construct a protocol for quantum fingerprinting. We now discuss how the mapping can be used to construct a protocol for the hidden matching problem.

The hidden matching problem. In this communication complexity problem, Alice receives an n-bit string $x \in \{0,1\}^n$ as input, with n an even number. Bob receives a matching $M = \{(i_1,j_1),(i_2,j_2),\ldots,(i_{n/2},j_{n/2})\}$ on the set of numbers $\{1,2,\ldots,n\}$, i.e., a partition into $n/2$ pairs. Only one-way communication from Alice to Bob is permitted and the goal is for Bob to output at least one element of the matching (i,j) and a corresponding bit value v such that $v = x_i \oplus x_j$, where x_i is the ith bit of the string x.

It has been shown that in the bounded-error model, any classical protocol requires $\Omega(\sqrt{n})$ bits of communication [11]. It was also shown in Ref. [11] that there exists an efficient quantum protocol that uses only $O\log_2 n$ qubits of communication and outputs a correct answer with certainty. In

this protocol, Alice prepares the state

$$|x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle \tag{25}$$

and sends it to Bob, who measures it in the basis

$$\left\{ \frac{1}{\sqrt{2}} (|i\rangle \pm |j\rangle) \right\}, \tag{26}$$

with $(i,j) \in M$. Since these states form a complete basis, one of these outcomes will always occur, and it will always correspond to the correct value since $\frac{1}{\sqrt{2}}(|i\rangle + |j\rangle)$ occurs only if $x_i \oplus x_j = 0$, and similarly $\frac{1}{\sqrt{2}}(|i\rangle - |j\rangle)$ occurs only if $x_i \oplus x_j = 1$. This allows Bob to give a correct output after performing his measurement. Note that Bob's measurement basis is constructed from the canonical basis by applying a Hadamard transformation to the subspaces $\{|i\rangle, |j\rangle\}$, with $(i,j) \in M$.

To construct a coherent-state protocol for the hidden matching problem, we just have to apply the rules of the mapping.

Hidden matching protocol

(1) Alice prepares the state

$$|\alpha, x\rangle = \bigotimes_{i=1}^{n} \left| (-1)^{x_i} \frac{\alpha}{\sqrt{n}} \right\rangle \tag{27}$$

according to her input x and sends it to Bob.

(2) Bob permutes the modes according to the matching M and interferes all pairs of modes $\{b_i, b_j\}$, with $(i,j) \in M$, in a balanced beam splitter. The detectors in the output ports of the beam splitters are labeled "0" and "1."

(3) If detector $v = 0,1$ clicks, corresponding to the modes (b_i, b_j), Bob outputs v and (i,j).

The protocol is illustrated in Fig. 3. Note that the linear-optical equivalent of a Hadamard gate is a balanced beam splitter, which explains the form of Bob's measurement in step 2. Additionally, if the incoming states to the input ports

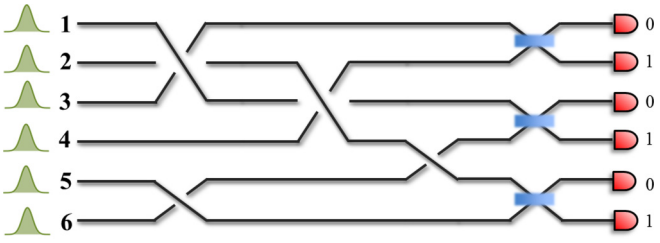

FIG. 3. (Color online) An example of an implementation of a coherent-state protocol for the hidden matching problem. Alice receives a string of six bits and Bob receives the matching (1,6),(2,5),(3,4). Alice encodes her input values in the phases of six coherent states in different modes and sends them to Bob. His measurement consists of a circuit in which the modes are permuted in accordance with the matching and then interefere pairwise in three balanced beam splitters. Bob can output a correct solution to the problem based on the detectors that click.

of the beam splitter are

$$\left| (-1)^{x_i} \frac{\alpha}{\sqrt{n}} \right\rangle \otimes \left| (-1)^{x_j} \frac{\alpha}{\sqrt{n}} \right\rangle, \tag{28}$$

the output states will be

$$\left| [1 + (-1)^{x_i \oplus x_j}] \frac{\alpha}{\sqrt{n}} \right\rangle \otimes \left| [1 - (-1)^{x_i \oplus x_j}] \frac{\alpha}{\sqrt{n}} \right\rangle. \tag{29}$$

For each possible value of $x_i \oplus x_j$, one of the output states will be a vacuum while the other is a coherent state with nonzero amplitude. Therefore, we can associate a value $v = 0,1$ with each of the output detectors so that whenever a click occurs, the correct value of $x_i \oplus x_j$ can be inferred with certainty. Even if there are many clicks, they will always correspond to a correct value.

The only issue that can arise is that no clicks occur and the probability that this happens is given by

$$P_{\text{no click}} = e^{-|\alpha|^2}, \tag{30}$$

which can be made arbitrarily small by choosing α appropriately. Moreover, Theorem 1 guarantees that the amount of information that is transmitted in the coherent-state protocol is $O \log_2 n$ and an exponential separation in communication complexity is maintained.

Having explored the application of the coherent-state mapping to the realm of quantum communication complexity, we now study how it can be useful in the context of quantum digital signatures.

IV. QUANTUM DIGITAL SIGNATURES

Quantum digital signatures (QDSs) were first proposed in Ref. [29] as a method of guaranteeing the authenticity and integrity of a classic message with unconditional security based only on fundamental principles of quantum mechanics. Recently, other protocols for QDSs have been proposed that, notably, use sequences of coherent states and linear-optics transformations [30–33]. In this section, we apply the mapping to construct an additional QDS protocol that can be realized using sequences of coherent states and simple linear-optics transformations. In addition to this, we use the mapping to establish a connection between the protocol of Ref. [29] and those of Refs. [30–32] and also to better understand the properties of these latter protocols.

We begin by briefly describing a simplified version of the QDS protocol of Ref. [29]. Alice holds a pair of classical bit strings $\{k_0, k_1\}$ known as private keys, which she will later use to sign a single bit b. The protocol makes use of an encoding of classical bit strings into quantum states $k \mapsto |f_k\rangle$ which is known to all recipients. For instance, the encoding could correspond to the states [8]

$$|f_k\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{k_{b,i}} |i\rangle, \tag{31}$$

where $k_{b,i}$ is the ith bit of the private key k_b.

In the distribution stage of the protocol, Alice sends each recipient Bob and Charlie two copies of the quantum states corresponding to her private keys and bit value, i.e., she sends $(0, |f_{k_0}\rangle, |f_{k_0}\rangle)$ and $(1, |f_{k_1}\rangle, |f_{k_1}\rangle)$ to each one. Upon receiving

the quantum states from Alice, and for each value of b, the recipients perform a swap test [8,29,34] on each pair of states to test whether they are different. The swap test is a comparison test of two states: If the states are the same, they always pass the test, and if they are different, they fail the test with probability $(1+|\delta|^2)/2$, where δ is the overlap of the states. Once this is done, one of the recipients, for example Bob, forwards one of the copies to Charlie, who also performs a swap test on his state and the forwarded state in order to check that they do not differ. If any of the swap tests fail, the protocol is aborted.

In the messaging stage, Alice signs a single bit by publicly announcing the message (b,k_b). Each recipient independently performs the map $k_b \mapsto |f_{k_b}\rangle$ and checks, using another swap test, that the resulting state coincides with the one sent by Alice during the distribution stage. Intuitively, security against forging arises from the fact that only an exponentially smaller number of bits can be learned from a measurement of the states $|f_{k_b}\rangle$ compared to the number of encoded bits, and security against repudiation is obtained from the swap tests which prevent Alice from sending differing states to each recipient.

This protocol is difficult to implement, since it requires the preparation and transmission of complex quantum states, performing challenging operations on the states, and storing them in a quantum memory until the messaging stage. Instead, we can apply the coherent-state mapping to build a protocol that is much simpler to implement.

First consider the states of Eq. (31) that are used as public keys. Applying the mapping we obtain the states

$$|\alpha, f_{k_b}\rangle = \bigotimes_{i=1}^{m} \left|(-1)^{k_{b,i}}\frac{\alpha}{\sqrt{n}}\right\rangle_i. \tag{32}$$

When the recipients receive the states, they need to ensure that both copies are equal. Originally, they achieved this by performing a swap test. However, using coherent states, there is a simpler alternative: They can pass a single state through a balanced beam splitter, creating copies of the original state, albeit with reduced amplitude. Similarly, even though we could apply the mapping to the operation corresponding to the swap tests between recipients, we can alternatively perform a simpler equality test as was outlined in Ref. [22] for the case of quantum fingerprinting. This test needs only the interference of the individual coherent states in a balanced beam splitter, and the measurement statistics are analogous to the outcome probabilities of a swap test. Furthermore, as is described in Ref. [30], in a coherent-state protocol it suffices to perform unambiguous state discrimination [35] of the individual coherent states and store the unambiguous outcomes in a classical memory. This classical data can then be used to verify the authenticity of the signed message. Overall, the QDS protocol is specified as follows:

QDS protocol

(1) Alice selects two n-bit strings k_0,k_1 uniformly at random and sends each of Bob and Charlie a copy of the states,

$$|\alpha, f_{k_b}\rangle = \bigotimes_{i=1}^{m} \left|(-1)^{k_{b,i}}\frac{\alpha}{\sqrt{n}}\right\rangle_i.$$

She sends a copy of each to both Bob and Charlie.

(2) Each recipient passes the states through a balanced beam splitter, obtaining two copies of the states $|\frac{\alpha}{\sqrt{2}}, f_{k_b}\rangle$.

(3) Using the first copy of their state, Bob and Charlie perform an unambiguous state discrimination of the individual coherent states $|+\frac{\alpha}{\sqrt{2n}}\rangle, |-\frac{\alpha}{\sqrt{2n}}\rangle$ and store the unambiguous outcomes in a classical memory.

(4) One of the recipients sends his second copy to the other and both of these second copies are interfered in a balanced beam splitter, whose output ports are labeled "equal" and "not Equal." If more than a certain fraction f of clicks are observed in the NEQ detector, the protocol is aborted.

(5) To sign a message, Alice publicly reveals (b,k_b) and sends it to one of the recipients, Bob for example. Bob accepts the message as valid if the number of mismatches between his unambiguous outcomes and Alice's revealed key is below a certain fraction $s_a > 0$.

(6) To forward the message to Charlie, Bob sends him Alice's message. Charlie verifies the validity of the message if the number of mismatches between his unambiguous outcomes and Alice's revealed key is below a certain fraction $s_v > s_a$.

Overall, the QDS protocol we have constructed through the coherent-state mapping can be implemented with the use of sequences of coherent states and beam splitters only, as illustrated in Fig. 4.

It is important to note that we are not providing a full security proof for this protocol, since this is usually a demanding and lengthy task, and the security statements can be complicated functions of the many protocol parameters. Our main goal in this section is to illustrate the usefulness of the mapping to construct and understand quantum communication protocols. Nevertheless, we expect that a full security proof can be constructed from the results of Refs. [29,30].

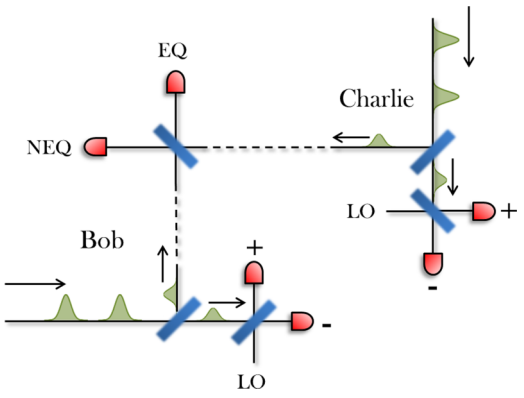

FIG. 4. (Color online) A protocol for QDSs. Bob and Charlie receive a train of pulses from Alice, which they split into two copies of smaller amplitude, keeping one copy for themselves and interfering the other in a balanced beam splitter in Bob's laboratory. They perform unambiguous state discrimination of the states $|+\alpha/\sqrt{2n}\rangle$ and $|-\alpha/\sqrt{2n}\rangle$ by interfering their kept signals with a local oscillator (LO). Whenever it is unambiguously revealed that the incoming state could not have been $|+\alpha/\sqrt{2n}\rangle$ or $|-\alpha/\sqrt{2n}\rangle$, the information is stored in a classical memory. Simultaneously, Bob and Charlie compare their received pulses by interfering their signals and they record the number of "not equal" (NEQ) outcomes. If they exceed a certain fraction of all clicks, the protocol is aborted.

The coherent-state mapping can also be used to understand existing QDS protocols. For example, in the protocol of Ref. [30], the public-key states are also of the form of Eq. (32). This implies that they can be equally thought of as arising from an application of the coherent-state mapping to the qubit states of Eq. (31). Furthermore, we note that the protocol of Ref. [30] has already been experimentally demonstrated [32], showing that these protocols can indeed be readily implemented.

The mapping also helps us to understand why these QDS protocols do not require a quantum memory. In a qubit protocol for QDS, only $\log_2 n$ bits of information of the private key can be obtained from a measurement on the states of Eq. (31). On the other hand, as discussed in Sec. II, by choosing the value of α appropriately, we can effectively choose the amount of information about the private keys that can be obtained. This permits the protocol to enter the statistical domain, in which enough classical information can be gathered in order to verify the authenticity of a message, but not enough information is available to successfully forge a message.

V. CONCLUSIONS

We have outlined a general framework for encoding quantum communication protocols involving pure states, unitary transformations, and projective measurements into another set of protocols that employs a coherent state of light in a linear combination of modes, linear-optics transformations, and measurements with single-photon threshold detectors. This provides a general method for mapping protocols in quantum communication into a form in which they can be implemented with current technology.

The advantages of the coherent-state protocols obtained from the mapping come at the price of a number of optical modes that is equal to the dimension of the original states in the qubit protocol. For practical purposes, this implies that they are suited for protocols that originally do not require a very large number of qubits. But as we have seen, there exists a regime in which the mapping leads to practical protocols whose implementation was previously inaccessible. As such, we expect that our results will pave the way for the experimental demonstration of a wide range of protocols in quantum communication.

From a theoretical perspective, the coherent-state mapping can be thought of as a tool for understanding fundamental aspects about quantum communication and information. For example, the mapping provides us with a connection between two intrinsically quantum properties: entanglement and nonorthogonality. Additionally, the mapping can also be applied in reverse: to obtain qubit protocols from coherent-state protocols. This provides a connection between the interferometry of coherent states with single-photon detectors, and abstract quantum communication protocols using qubits. Besides being of fundamental interest, this may serve as a theoretical test bed for proving results regarding qubit protocols, in the same way that many other dualities have been useful in both physics and mathematics.

ACKNOWLEDGMENTS

J.M.A. is grateful for the support of the Mike and Ophelia Lazaridis Fellowship. We acknowledge support from Industry Canada, the NSERC Strategic Project Grant (SPG) FREQUENCY, and the NSERC Discovery Program. J.M.A. would like to thank A. Ignjatovic for valuable discussions.

[1] T. D. Ladd, F. Jelezko, R. Laflamme, Y. Nakamura, C. Monroe, and J. L. OBrien, Nature (London) **464**, 45 (2010).
[2] H. Buhrman, R. Cleve, S. Massar, and R. de Wolf, Rev. Mod. Phys. **82**, 665 (2010).
[3] V. Giovannetti, S. Lloyd, and L. Maccone, Phys. Rev. Lett. **96**, 010401 (2006).
[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[5] N. Gisin and R. Thew, Nat. Photon. **1**, 165 (2007).
[6] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[7] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[8] H. Buhrman, R. Cleve, J. Watrous, and R. de Wolf, Phys. Rev. Lett. **87**, 167902 (2001).
[9] H. Buhrman, R. Cleve, and A. Wigderson, in *Proceedings of the 30th Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 1998), pp. 63–68.
[10] R. Raz, in *Proceedings of the 31st Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 1999), pp. 358–367.
[11] Z. Bar-Yossef, T. S. Jayram, and I. Kerenidis, in *Proceedings of the 36th Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2004), pp. 128–137.
[12] D. Stucki, N. Walenta, F. Vannel, R. T. Thew, N. Gisin, H. Zbinden, S. Gray, C. Towery, and S. Ten, New J. Phys. **11**, 075003 (2009).
[13] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka *et al.*, Opt. Express **19**, 10387 (2011).
[14] J. Zhang, X.-H. Bao, T.-Y. Chen, T. Yang, A. Cabello, and J.-W. Pan, Phys. Rev. A **75**, 022302 (2007).
[15] P. Trojek, C. Schmid, M. Bourennane, C. Brukner, M. Zukowski, and H. Weinfurter, Phys. Rev. A **72**, 050305 (2005).
[16] R. T. Horn, S. A. Babichev, K.-P. Marzlin, A. I. Lvovsky, and B. C. Sanders, Phys. Rev. Lett. **95**, 150502 (2005).
[17] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, Phys. Rev. Lett. **73**, 58 (1994).
[18] S. Massar, Phys. Rev. A **71**, 012310 (2005).
[19] S. Tanzilli, A. Martin, F. Kaiser, M. P. De Micheli, O. Alibart, and D. B. Ostrowsky, Laser Photon. Rev. **6**, 115 (2012).
[20] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, Opt. Express **16**, 18790 (2008).
[21] A. S. Holevo, Probl. Peredachi Inf. **9**, 3 (1973).
[22] J. M. Arrazola and N. Lütkenhaus, Phys. Rev. A **89**, 062305 (2014).
[23] R. Sheldon, *A First Course In Probability, 6/E* (Pearson Education, London, 2002).

[24] M. Franceschetti, O. Dousse, D. Tse, and P. Thiran, IEEE Trans. Inf. Theory **53**, 1009 (2007).
[25] A. C.-C. Yao, in *Proceedings of the 11th Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 1979), pp. 209–213.
[26] G. Brassard, Found. Phys. **33**, 1593 (2003).
[27] D. Gavinsky, in *Proceedings of the 40th Annual ACM Symposium on Theory of Computing* (ACM Press, New York, 2008), pp. 95–102.
[28] A. D. Barbour, L. Holst, and S. Janson, *Poisson Approximation* (Clarendon Press, Oxford, 1992).
[29] D. Gottesman and I. Chuang, arXiv:quant-ph/0105032.
[30] V. Dunjko, P. Wallden, and E. Andersson, Phys Rev. Lett. **112**, 040502 (2014).
[31] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, Nat. Commun. **3**, 1174 (2012).
[32] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, Phys. Rev. Lett. **113**, 040502 (2014).
[33] V. Dunjko, P. Wallden, and E. Andersson, arXiv:1403.5551.
[34] J. C. Garcia-Escartin and P. Chamorro-Posada, Phys. Rev. A **87**, 052330 (2013).
[35] E. Andersson, M. Curty, and I. Jex, Phys. Rev. A **74**, 022304 (2006).