Information communicated by entangled photon pairs

Thomas Brougham and Stephen M. Barnett
Department of Physics, University of Strathclyde, Glasgow, G4 0NG, United Kingdom
(Received 21 December 2011; published 19 March 2012)

A key goal of quantum communication is to determine the maximum number of bits shared between two quantum systems. An important example of this is in entanglement-based quantum key distribution (QKD) schemes. A realistic treatment of this general communication problem must take account of the nonideal nature of the entanglement source and the detectors. The aim of this paper is to give such a treatment. We obtain analytic expression for the mutual information in terms of experimental parameters. The results are applied to communication schemes that rely on spontaneous parametric down conversion to generate entangled photons. We show that our results can be applied to tasks such as calculating the optimal rate of bits per photon in high-dimensional time-bin-encoded QKD protocols (prior to privacy amplification). A key finding for such protocols is that, by using realistic experimental parameters, one can obtain over 10 bits per photon. We also show how our results can be applied to characterize the capacity of a fiber array and to quantify entanglement using mutual information.

DOI: 10.1103/PhysRevA.85.032322 PACS number(s): 03.67.Hk

I. INTRODUCTION

A central concern of quantum information theory is to determine the maximum amount of information that can be shared between two quantum systems. The shared information gives an indication of the quantum correlations and is thus of fundamental interest [1–4]. In addition to this, knowledge of the shared information determines the performance of quantum communications [5] and is vital for many proposed applications of quantum information [6,7]. One important example of this is in quantum key distribution which, in one of the seminal insights within the field of quantum information, was the realization that quantum mechanics allows for the secure distribution of cryptographic keys [8–12]. An important class of quantum key distribution (QKD) schemes uses entanglement [13–16]. The security of entanglement-based QKD is based on the nonlocality of quantum mechanics.

An important issue to address for QKD is determining how many bits of the secret key are distributed. A prerequisite for this calculation is determining the maximum number of unsecured bits that the two parties can share. This is the information contained in the raw keys. To fully extract this information, error correction is necessary, followed by privacy amplification to minimize the information an eavesdropper might have access to [17]. If one is looking to optimize both the error correction and privacy amplification protocols, then it is essential to know the mutual information shared between the raw keys. This quantity will depend on both the detectors and the details of the source of the entangled states. Realistic physical models of each of these components is thus vital.

The effects of losses, inefficiencies, and imperfect sources have been studied previously [18]. In particular, spontaneous parametric down conversion sources with losses have been studied with regards to QKD [19,20]. The existing work, however, has concentrated on the case where the information is encoded in the polarization degree of freedom. As a result, this work cannot be applied to communications protocols that use high-dimensional entangled states with the aim of encoding multiple bits on each photon.

In this paper we determine the maximum shared information for realistic quantum sources and detectors. As most experimental implementations of quantum communication protocols are optically based, the examples we study will be limited to optical systems. The natural question to ask is what is the maximum shared information per photon? The main result of our paper will be to determine this for general but experimentally relevant conditions. This result is broader in its scope than earlier findings, such as [19,20]. In particular, our results apply not only to information encoded in polarization, but also to information encoded in high-dimensional entangled degrees of freedom. This fact is illustrated by applying our findings to different experimental setups, which include, but are not limited to, QKD experiments. Our results can thus be used to optimize a given experimental procedure. In particular, one can determine the power at which to operate a pump laser driving a spontaneous parametric down conversion source so as to maximize the mutual information.

The paper is organized in the following way: In Sec. II we discuss the general communication system that we consider. Special attention is paid to time-bin-encoded communication protocols [21–24]. In Secs. III and IV we construct simple mathematical models of the source, channels, and imperfect photon detectors. The mutual information is calculated in Secs. V and VI for sources that produce entangled pairs with a Poissonian distribution. In Sec. VII we discuss the relevance of our results to other tasks such as characterizing the capacity of a fiber array and information theoretic approaches to quantifying entanglement. Finally, our results are discussed in Sec. VIII.

II. COMMUNICATING SHARED BITS USING ENTANGLEMENT

The fundamental communications problem is distributing a shared string of bits between two parties, called Alice and Bob. One way of using quantum mechanics to achieve this is to use an entangled state; that is, one of the form

$$|\Psi\rangle_{AB} = \sum_k c_k |\varphi_k\rangle_A |\varphi'_k\rangle_B, \tag{1}$$

where $\langle\varphi_i|\varphi_j\rangle = \langle\varphi_i'|\varphi_j'\rangle = \delta_{ij}$. It can also be useful to consider hyperentangled states that have entanglement between multiple degrees of freedom [25,26]. A string of bits can then be generated from the correlation between one of the entangled degrees of freedom. If one is looking to communicate multiple bits per entangled state, then this requires high-dimensional entanglement. The idea is best illustrated by some simple examples.

Using spontaneous parametric down conversion (SPDC) one can produce pairs of photons that are entangled both in their polarization and in time and frequency [15,27]. It is convenient to express such states using continuous time creation and annihilation operators, which satisfy the commutator relation $[\hat{a}(t),\hat{a}^\dagger(t')] = \delta(t-t')$ [28]. The down-converted state thus has the form

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|HH\rangle_{AB} + |VV\rangle_{AB}) \otimes \int dt_1 dt_2 g(t_1,t_2)\hat{a}_A^\dagger(t_1)\hat{a}_B^\dagger(t_2)|0\rangle, \qquad (2)$$

where H and V respectively denote horizontal and vertical polarization, $\hat{a}_A^\dagger(t)$ $[\hat{a}_B^\dagger(t)]$ is the creation operator for Alice's (Bob's) photons and $g(t_1,t_2)$ is a normalized function that is zero when $|t_1 - t_2|$ become sufficiently large. This means that, if Alice detects a photon at time T, then Bob should also detect his photon at a time close to T. This correlation can be used to form a random bit string shared between Alice and Bob. One way of doing this is to divide the photon's possible arrival times into discrete time bins and record whether photons are found in each time bin. The measurement record of M time bins can then be used, at least in principle, to construct a string of M bits. The zeros and ones of the bit string would respectively correspond to the absence or detection of photons within a time bin.

A second example is to use the spatial modes of entangled photons generated by SPDC. It has been shown, for example, that the down converted photons are entangled in their orbital angular momentum and angular position [29–31]. The fact that angular momentum requires an unbounded Hilbert space means that measuring the angular momentum of the photons enables multiple bits to be extracted per photon pair. For example, if an experiment can distinguish between M different angular momentum eigenstates, then one can extract up to $\log_2(M)$ bits per photon pair.

It is worthwhile noting the connection between this communication problem and QKD. For a given quantum key distribution protocol, one wishes to distribute a *secret* shared string of bits. This requires us to outline a mechanism for checking the security of the bits. A common approach is to measure in two mutually unbiased bases and then publish a random sample of Alice and Bob's measurement results. The presence of an eavesdropper can then be established by looking at the cases where Alice and Bob measured in the same basis. In the absence of an eavesdropper, these measurement results should be correlated. The use of incompatible bases and implementing security checks necessarily reduces the communication rate.

The communication problem we are studying corresponds to determining the shared information when Alice and Bob both measure in the same basis. It is important to note that this is not the number of shared secret bits. To determine this one would need to find out the number of bits lost due to the additional constraints of security. For details on how the security of QKD decreases the shared information, see Refs. [7,17].

III. MODELLING PHOTON SOURCE, DETECTORS, AND LOSSES

The first part of the system that we will look at is the source of the entangled photons. We first assume that the source generates entangled pairs of photons. If four photons are generated, then this will correspond to two pairs of entangled photons.[1] The next assumption is that we have a probability $P(m)$ of producing m photon pairs at a time and that this is independent of the number of photon pairs produced earlier. For the example of time-bin-encoded photons, $P(m)$ corresponds to the probability of producing m photon pairs within a given time window. When the photons are generated by SPDC, $P(m)$ can be approximated by a Poissonian distribution [32].

The next aspect that we consider is the measurement process. We consider only measurements that are realized either by the detection of photons within time bins or within discrete spatial locations or modes. This does not limit us, however, to considering only temporal or spatial encoded information. The reason for this is that measurements of other degrees of freedom can be converted into measurements of either temporal or spatial degrees of freedom. A common example of this is measuring polarization by using a polarizing beam splitter. This converts information about the polarization into information about the spatial location of a photon. Similarly, one can convert measurements of different quantities into measurements of the time of arrival of a photon. For example, the spatial position of photons in an optical field have been measured using a time multiplexing fiber array. Different position at which the photon could be found were converted into different time windows in which the photon could be detected [33]. The advantage of this sort of experimental procedure is that only one photon detector is required to detect many different spatial modes.

Another assumption of our analysis is that one is equally likely to obtain any of the measurement outcomes. For example, in a time-binned system this would correspond to it being equally likely that photons are sent in each time bin. While the assumption is reasonable in the context of time-binned communication systems, it can appear prohibitive in other situations. The reason for making this assumption is that the aim of our analysis is to determine the effect of inefficiencies in the source, channel, and detectors. For this reason we consider only the simplest possible form for the entangled photonic states. More complex systems can, however, still be approximated by our analysis. For example, the effective Schmidt modes of a SPDC state with large

[1] In practice this condition may have to be relaxed slightly. Alternatively, one might filter the output of the source so as to postselect only those situations when pairs were emitted.

Schmidt number can, to a good approximation, be taken to be equiprobable [34].

Because our aim is to encode information on each photon pair and not in the number of photons, we shall consider only threshold detectors that do not resolve photon number. Consider first the situation where we have no losses. This would correspond to no transmission losses and ideal detectors that detect all photons incident on them. The probability for Alice or Bob's detector to fire is

$$\pi(c) = \sum_{m=1}^{\infty} P(m), \tag{3}$$

where $\pi(c)$ is the probability for the ideal detector to click and $P(m)$ is again the probability to find m photons within each time bin or spatial mode. In a real experiment, however, detectors do have losses. One can model an inefficient detector as an ideal detector with a lossy medium in front of it [35,36]. For our purposes, the lossy medium can be viewed as a beam splitter with transmission coefficient $\sqrt{\eta_d}$. The losses will thus correspond to photons being reflected at the beam splitter. The square of the transmission coefficient η_d corresponds to the efficiency of the detector. It is clear that a single photon incident on the nonideal detector will be detected with probability η_d.

In addition to the photons lost by the detectors there will be losses during transmission. This can again be modelled by a beam splitter, where the transmission coefficient is $\sqrt{\eta_l}$. It is convenient to incorporate both of these sources of loss into a single efficiency for the system. This would correspond to a beam splitter with transmission coefficient $\sqrt{\eta}$, where $\eta = \eta_d \eta_l$. The total efficiency η again gives the probability for any given emitted photon to be detected.

One further source of loss is in cross talk between multiple modes. This would be an issue if one is transmitting the information in spatial modes. The effect of cross talk is to cause photons to be lost from one mode and appear in a different one. A simple way to account for this in our current model is to adjust the efficiency η to include loss from cross talk. The effect of the photons appearing in a different mode can then be dealt with by increasing the effective dark count rate.

IV. JOINT DETECTION PROBABILITY

To calculate the mutual information we need to determine the joint probability for Alice and Bob to obtain the same measurement outcome. The key mathematical tool in our analysis is the moment generating function [37]. If $P(n)$ is the probability that a pulse contains n photons, then we define the moment generating function to be

$$M(\mu) = \sum_{n=0}^{\infty} P(n)(1-\mu)^n. \tag{4}$$

Moment generating functions have many useful properties, the simplest of which is

$$P(n) = \frac{1}{n!}\left(-\frac{d}{d\mu}\right)^n M(\mu)\bigg|_{\mu=1}. \tag{5}$$

It is straightforward to generalize the definition of $M(\mu)$ to a pair of pulses:

$$M(\mu,\xi) = \sum_{m,n=0}^{\infty} P(m,n)(1-\mu)^m(1-\xi)^n. \tag{6}$$

In our case the pair of pulses correspond to the entangled signal and idler beams for a single time bin or spatial mode. The number of photons in each pulse is the same, hence

$$P(m,n) = P(n)\delta_{m,n}. \tag{7}$$

The merit of using the moment generating functions is that it is easy to account for losses [37].

If we suppose that Alice and Bob both have identical detectors and that both their channels have the same losses, then we can assign to both parties the same total efficiency η. The generating function is

$$M_{\text{loss}}(\mu,\xi) = \sum_{m=0}^{\infty} P(m)(1-\eta\mu)^m(1-\eta\xi)^m. \tag{8}$$

Consider a particular measurement outcome. This will either correspond to a spatial location at which photons can be detected or a particular time bin in which the photons can be found. Let c and 0 denote the detectors registering a click and not registering a click, respectively. The joint probability for Alice and Bob to both get the same measurement outcome is $\pi^{AB}(i,j)$, where $i,j \in \{0,c\}$. In the ideal case $\pi(0,c) = \pi(c,0) = 0$; that is, Alice and Bob would either both detect photons or neither would detect any. This is not the case, however, when losses are present. In the absence of dark counts the probabilities are

$$\begin{aligned}
\pi^{AB}(0,0) &= M_{\text{loss}}(1,1),\\
\pi^{AB}(c,0) &= \sum_{l=1}^{\infty}\frac{1}{l!}\left(-\frac{d}{d\xi}\right)^l M_{\text{loss}}(1,\xi)\bigg|_{\xi=1},\\
\pi^{AB}(0,c) &= \pi^{AB}(c,0),\\
\pi^{AB}(c,c) &= \sum_{n=1}^{\infty} P(n)[1-(1-\eta)^n]^2.
\end{aligned} \tag{9}$$

The effect of the detectors registering dark counts can easily be modelled. Let q be the probability that, within a given period of time, Alice or Bob's detector fires when no photons are incident on it. The joint probability, $\mathcal{P}^{AB}(i,j)$, will thus be

$$\begin{aligned}
\mathcal{P}^{AB}(0,0) &= (1-q)^2\pi^{AB}(0,0),\\
\mathcal{P}^{AB}(0,c) &= (1-q)\pi^{AB}(0,c) + (1-q)q\pi^{AB}(0,0)\\
&= \mathcal{P}^{AB}(c,0),\\
\mathcal{P}^{AB}(c,c) &= \pi^{AB}(c,c) + 2q\pi^{AB}(0,c) + q^2\pi^{AB}(0,0).
\end{aligned} \tag{10}$$

It is straightforward to verify that these probabilities sum to one. The marginal probabilities for Alice or Bob's detector to fire are $\mathcal{P}(0) = (1-q)[\pi(0,0) + \pi(0,c)]$ and $\mathcal{P}(c) = 1 - \mathcal{P}(0)$. We have thus obtained a general expression for the joint and marginal probability distributions. These expressions are valid for any choice for the source probability $P(m)$ and consequently are not tied to one physical implementation.

V. MUTUAL INFORMATION

In the classic paper of Shannon it was shown that the maximum amount of information that two parties can share is given by the mutual information [38,39]. For a joint probability distribution $\mathcal{P}^{AB}(i,j)$ with marginal probabilities $\mathcal{P}^{A}(i)$ and $\mathcal{P}^{B}(j)$, the mutual information is defined as

$$H(A:B) = \sum_{i,j=0,c} \mathcal{P}^{AB}(i,j) \log_2 \left(\frac{\mathcal{P}^{AB}(i,j)}{\mathcal{P}^{A}(i)\mathcal{P}^{B}(j)} \right). \tag{11}$$

The quantity given in Eq. (11) is the mutual information that Alice and Bob share when they obtain the same measurement outcome. Consider a time-bin-encoded QKD protocol. If M time bins are used to create a key, then Alice and Bob will share a bit string of length $MH(A:B)$. When one is interested in QKD, then number of shared bits will, of course, be reduced by the need to perform privacy amplification.

For communication in the quantum regime, it often important to know the number of shared bits per photon. We must, however, be careful in how this quantity is defined. One approach would be to divide the mutual information by the mean number of photon pairs produced. If we denote the mean number of photon pairs by λ, then the information per photon is simply

$$I_g(A:B) = \frac{H(A:B)}{\lambda}. \tag{12}$$

The quantity $I_g(A:B)$ is the information per generated photon pair; however, not all generated photons are detected. This fact suggests an alternative way to define the information per photon. Instead of considering the information per generated photon pair, we can use the information per detected photon pair. This is defined as

$$I_d(A:B) = \frac{H(A:B)}{\eta^2\lambda + q^2}. \tag{13}$$

The formalism developed so far applies to any choice for $P(m)$. We shall examine a concrete example, where $P(m)$ is a Poissonian distribution.

VI. MUTUAL INFORMATION FOR SPDC SOURCES

An important way of generating entangled photons is via the process of spontaneous parametric down conversion (SPDC). In this approach a pump beam illuminates a nonlinear crystal. Within the crystal, each pump photon can be converted into two lower-frequency photons, referred to as signal and idler photons. By careful choice of the system parameters, one can arrange for the emitted photon pairs to be entangled. This entanglement can be both in the polarization and in the transverse spatial modes [40–42]. This method of generating entangled photons has been used in many experimental realizations of QKD [25,43].

To illustrate how SPDC can be used to distribute a string of random bits, consider the following two examples: A time-binned protocol can be implemented using a pulsed laser that is shone at a nonlinear crystal. The resulting down-converted photon pairs are entangled in time. Distributing these photons to Alice and Bob allows them to construct a shared random string of bits. The entangled time-bin states needed for this protocol have already been experimentally generated [21–23]. The second example is to use the spatial modes of photons generated by SPDC. By using a pump beam with an appropriate profile [44], one can generate photon pairs that carry angular momentum in their transverse modes [41,42,45]. The down converted photons will be entangled in the angular momentum degree of freedom. A mode sorter can be used to separate some of the different angular momentum states into different spatial locations, where photon detectors are located. In the limit of large Schmidt number, the effective modes of the photon pairs will be approximately equiprobable [34]. The analysis we present will apply to both of these examples as well as many other situations where photons are generated by SPDC.

The probability distribution for m pairs of photons to be generated by SPDC can be approximated by a Poissonian distribution

$$P(m) = e^{-\lambda}\frac{\lambda^m}{m!}. \tag{14}$$

It can easily be verified that λ is the mean number of photon pairs. Using this distribution we can derive the mutual information for QKD schemes that use SPDC to generate pairs of entangled photons. The use of a Poissonian for the probability distribution is only valid when the initial laser pulses are not too short. If we instead have short pulses, then it becomes necessary to use a thermal distribution [i.e., $P(m) = \lambda^m/(\lambda+1)^{m+1}$]. The moment generating function can again be calculated and the results of Sec. IV can be used to calculated the new value for the mutual information.[2]

The distribution (14) in Eq. (8) yields the following expression for the moment generating function:

$$M_{\text{loss}}(\mu,\xi) = \exp\left[-\eta\lambda(\mu + \xi - \eta\mu\xi)\right]. \tag{15}$$

From Eqs. (9) and (10) we find that the joint probability distribution for the detectors is

$$\begin{aligned}
&\mathcal{P}^{AB}(0,0) = (1-q)^2 e^{-\lambda\eta(2-\eta)},\\
&\mathcal{P}^{AB}(c,0) = (1-q)e^{-\lambda\eta} - (1-q)^2 e^{-\lambda\eta(2-\eta)},\\
&\mathcal{P}^{AB}(0,c) = \mathcal{P}^{AB}(c,0),\\
&\mathcal{P}^{AB}(c,c) = 1 - 2(1-q)e^{-\lambda\eta} + (1-q)^2 e^{-\lambda\eta(2-\eta)}.
\end{aligned} \tag{16}$$

The marginal probabilities for Alice's (or Bob's) detector to click is thus $\mathcal{P}(0) = (1-q)e^{-\lambda\eta}$ and $\mathcal{P}(c) = 1-(1-q)e^{-\lambda\eta}$. The mutual information can easily be calculated and is found to be

$$\begin{aligned}
H(A:B) = {} & 2H_2(A) + B\log_2 B \\
& + 2(A-B)\log_2(A-B) \\
& + [1-2A+B]\log_2[1-2A+B],
\end{aligned} \tag{17}$$

where $H_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$, $A = (1-q)e^{-\lambda\eta}$, and $B = A^2 e^{\lambda\eta^2}$. The above expression gives the mutual information between Alice and Bob as a function of the mean number of photons λ, the efficiency η and the probability of getting a dark count q. In Fig. 1 the mutual information is

[2] A quick calculation shows that, for a thermal distribution, the moment generating function is $M_{\text{loss}}(\mu,\xi) = (1+\eta\lambda[\mu+\xi-\eta\mu\xi])^{-1}$.

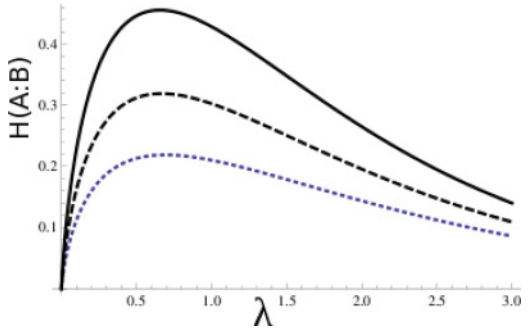

FIG. 1. (Color online) Plot of $H(A:B)$ as a function of λ, for different values of efficiency. In all of the plots $q = 3.9 \times 10^{-8}$, which corresponds to a dark count rate of 300/s and a time-bin width of 130 ps. The solid black line is for $\eta = 0.8$, the dashed line corresponds to $\eta = 0.7$, while the dotted line corresponds to $\eta = 0.6$. The mutual information $H(A:B)$ is measured units of bits.

plotted as a function of λ for different values of η, with $q = 3.9 \times 10^{-8}$, which corresponds to time bins of width 130 ps and the detectors having on average 300 dark counts per second. In the ideal case, $H(A:B)$ would be one bit. From Fig. 1 we see that inefficiencies can significantly decrease the mutual information. It is thus important to maximize the possible mutual information by controlling the value of λ. The optimal value for λ can be found using Eq. (17).

In order to compare different experimental QKD schemes it is often useful to determine the number of bits per photon. Equation (12) gives the number of bits per generated photon, while Eq. (13) gives the number of bits per detected photon. The mutual information per generated photon, $I_g(A;B)$, is plotted in Fig. 2 as a function of λ. Figure 2(a) shows that, for an efficiency of 0.85, we can have greater than 10 bits per generated photon. Figure 2(b) shows that, with a lower dark count and efficiency of 0.8, one can achieve more than 13 bits per generated photon. The information per detected photon, $I_d(A;B)$, is plotted in Fig. 3 as a function of λ. One can see that, in Fig. 3(a), we have more than 14 bits per detected photon, for $\eta = 0.8$. In Fig. 4(b) we find that, for $\eta = 0.8$ and a dark count that is about 10% of λ, we obtain about 20 bits per detected photon.

The result (17) can be used with Eqs. (12) and (13) to find the value of λ that maximizes the information per photon. From the perspective of experimentally implementing high-bit-rate QKD, one might wish to determine the laser intensity that optimizes the number of bits per photon. This task can be achieved using our results together with the fact that the value of λ will depend on the laser intensity [46]. This is one of the key findings of this paper.

The dependence of $I_g(A:B)$ and $I_d(A:B)$ on the efficiency can be of practical significance for implementing QKD. For example, in an experiment one might what to know how big an improvement there would be if better detectors are used. This problem can again be solved using Eq. (17). Mathematically the problem is to find the maximum of $I_g(A:B)$ or $I_d(A:B)$ for fixed values of η and q. This quantity is plotted in Fig. 4. The plot is for a fixed value of q; however, decreasing q does not significantly increase the information. Similarly, the information is not decreased by too

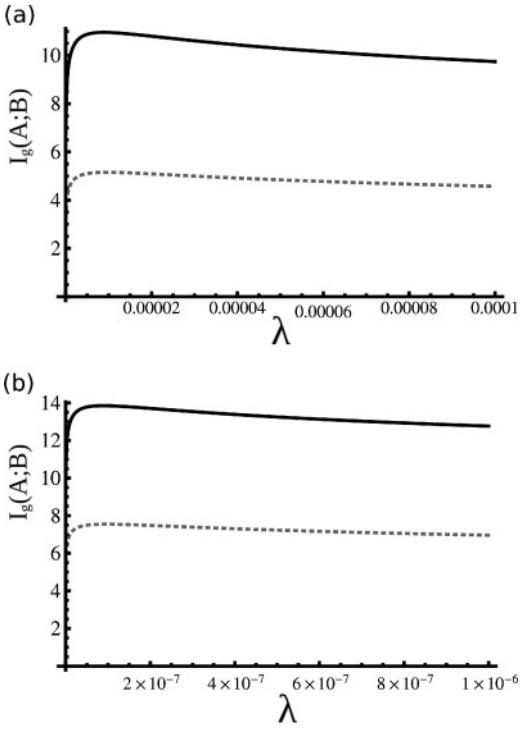

FIG. 2. Plot of $I_g(A;B)$ as a function of λ. Plots (a) have $q = 3.9 \times 10^{-6}$ and the dotted line is for $\eta = 0.6$, while the solid line is for $\eta = 0.85$. Plots (b) have $q = 3.9 \times 10^{-8}$ and the dotted line is for $\eta = 0.6$, while the solid line is for $\eta = 0.8$. In all plots the mutual information per generated photon is measured units of bits.

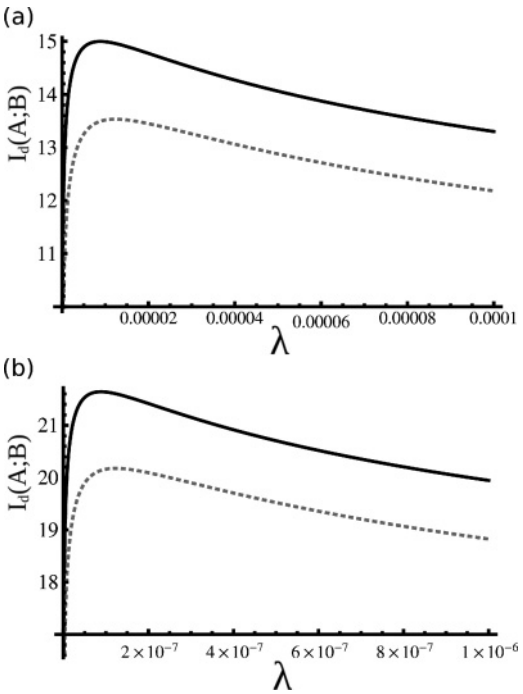

FIG. 3. Plot of $I_d(A;B)$ as a function of λ. Plots (a) are for $q = 3.9 \times 10^{-6}$, while in plots (b) are for $q = 3.9 \times 10^{-8}$. In both plots the dotted line is for $\eta = 0.4$ and the solid line corresponds to $\eta = 0.8$. The mutual information per detected photon is measured units of bits.

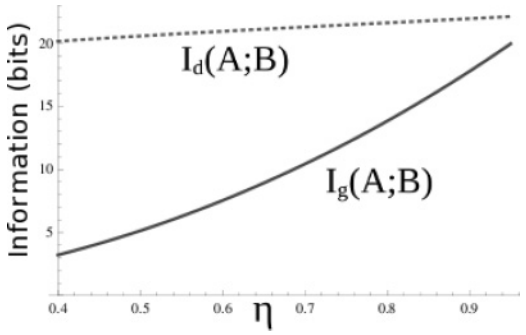

FIG. 4. Plot of $I(A;B)$ as a function of η. The probability of dark counts, q, is 3.9×10^{-8}. The mutual information per photon is measured units of bits.

much if q is increased by an order of magnitude. If q is increased by several orders of magnitude, then $I_{g,d}(A:B)$ will be decreased by an noticeable amount. One thus sees that for reasonable small dark counts, the efficiency is the main factor limiting the information per photon.

VII. FURTHER APPLICATIONS

A. Information-based classification of high-dimensional entangled states

The theory we have outlined has, thus far, been applied to quantum communication. There are, however, other situations where these results can be applied. An example of this is in developing experimentally useful classifications of entangled states. One approach is to use the information that two parties can extract from an entangled state as a figure of how entangled the state is [3,4,47]. Recently, this approach has been used as the basis for an experimental procedure for quantifying the entanglement in photons generated by SPDC [48]. The idea was to use the fact that a pair of photons generated by SPDC are entangled both in position and momentum. The results of measurements on each photon's position or momentum would thus be correlated.[3] The mutual information gained by measuring these quantities will thus give us an indication of the strength of the entanglement.

If one is to make accurate comparisons between experimental results and theory, it is important to factor in effects such as detector inefficiencies, dark counts, and imperfections in the source. This can be achieved using the formalism that we have developed. In particular, one can see how the experimental imperfections should affect the measured entanglement of the state.

In the experiments discussed in [48] the measurements of position and momentum were made using spatial-resolving photon detectors. These consisted of a detector with discrete pixels. Detection of photons by one of the pixels would thus allow for a measurement of the spatial location of the photons. Each pixel has a finite width. The measurement thus has a discrete set of outcomes. One subtle point is that if the region of space is chosen sufficiently large, then the probability for detecting photons at various locations can vary. In our analysis we implicitly assume that each outcome is equiprobable. This assumption means that applying our theory to this experiment will lead to a slight overestimate of the mutual information. This suggests that the proper way of viewing our results, when applied to this setup, is as providing an upper bound on the possible mutual information.

B. Capacity of fiber arrays

Another interesting application of our theory is in characterizing the information capacity of a fiber array. This would entail treating the array as a information channel and calculating the maximum mutual information between the outputs and input with a fixed probe beam. The capacity gives an information theoretic measure of the ability of a given array to transmit and sort optical pulses. An example of the sort of system where this could be important is in time multiplexing of detectors [33,49].

The two situations we consider are M input fibers coupled to a single detector and a single input fiber coupled to M fibers. In the former situation we have M inputs and one detector, while in the later we have one input and M detectors. One crucial difference between both of these cases and all our previous examples is that we are not considering pairs of entangled photons. Instead, our inputs will be pulses that contain n photons with probability $P(n)$. In many instances the statistics of the input pulses can be approximated by a Poissonian distribution; for example, if one takes each pulse to be in a coherent state [28]. When this is the case, the capacity can be calculated using Eq. (17).

The approach is best illustrated by a simple example. Suppose we have a fiber array composed of 8 output fibers coupled to a single detector. This situation has been experimentally realized in [33]. The array is designed so that each fiber has a different length so that the different inputs reach the detector at different well-defined times. Let us assume that the separation between these time bins is 1 ns, which is larger than the jitter of our detector. The efficiency of the detector and array is taken to be 40%, while the dark count rate is 300/s. The probability of obtaining a dark count in a given time window is thus $q = 3 \times 10^{-7}$. Finally, we assume that the input pulses have a Poissonian photon distribution with mean λ and that the pulses are equally likely to enter each input. Under these conditions

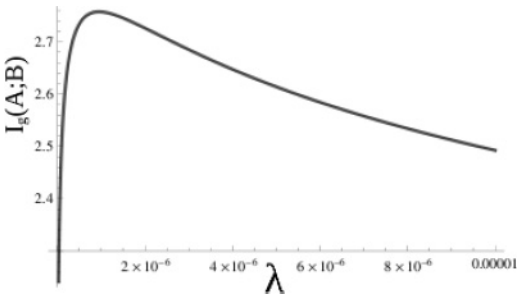

FIG. 5. Plot of $I_g(A;B)$ as a function of λ. The probability of dark counts, q, is 3×10^{-7} and the efficiency is $\eta = 0.4$. The quantity $I_g(A;b)$ is measured in units of bits.

[3]To simplify the discussion we do not differentiate between correlations and anticorrelations. The term correlated will thus encompass both situations.

Eq. (17) can be used to calculate the total information as a function of λ. In Fig. 5 we plot the average information per generated photon.

The previous calculations were for a beam that has a Poissonian photon distribution. If the beam is not Poissonian or cannot be approximated by a Poissonian, then Eq. (17) cannot be used. Instead, one can use the general formalism outlined in Sec. III. The procedure would thus be to calculate the generating function for the given choice of $P(n)$. Equations (9) and (10) can then be used to calculate the Alice and Bob's joint probability distribution.

VIII. CONCLUSIONS

We have investigated how realistic experimental conditions affect the amount of shared information that two parties can extract from entangled photons. A key goal of our work is to investigate systems where multiple bits can be encoded on each photon. This means that our analysis goes beyond previous work, which has focused on encoding information in polarization. Our approach was to construct simple but realistic models of the entangled photon source, the information channel and the detectors. These models allowed us to take account of effects such as transmission losses, cross talk, detector inefficiencies, and dark counts. After developing the general theory in Secs. III and IV, the formalism was illustrated by looking at systems where the photon pairs are generated by spontaneous parametric down conversion. An explicit expression for the mutual information, Eq. (17), was given for this case. This represented one of the main results of the paper. Within a QKD scheme the quantity we have calculated corresponds to the shared information in Alice and Bob's keys, before privacy amplification. Our results can thus be used in the design of QKD experiments to choose parameters that maximize both the mutual information and the average information per photon. As an example, Fig. 4 shows the optimal amount of information per photon that two parties can share as a function of the efficiency.

Our findings have applications out with quantum key distribution. This was demonstrated by two examples. The first was using the mutual information as a basis for an experimental protocol to quantify photonic entanglement [48]. The second application was in characterizing the efficiency of an optical array in terms of how well it transmits information. This provides a useful, experimentally accessible, figure of merit for how well an optical array can sort and transmit optical signals.

ACKNOWLEDGMENTS

We would like to thank Daniel Gauthier, Paul Kwiat, and Kevin McCusker for very useful discussions. This research was supported by the DARPA InPho program through the US Army Research Office award W911NF-10-0395. SMB also acknowledges the Royal society and the Wolfson Foundation for support.

[1] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[2] C. H. Bennett, H. J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
[3] S. M. Barnett and S. J. D. Phoenix, Phys. Rev. A **40**, 2404 (1989); **44**, 535 (1991).
[4] M. J. W. Hall, E. Andersson, and T. Brougham, Phys. Rev. A **74**, 062308 (2006).
[5] C. H. Bennett and P. W. Shor, IEEE Trans. Inf. Theory **44**, 2724 (1998).
[6] S. M. Barnett, *Quantum Information* (Oxford University Press, Oxford, 2009).
[7] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[8] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[9] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[10] S. J. D. Phoenix, S. M. Barnett, and A. Chefles, J. Mod. Opt. **47**, 507 (2000).
[11] V. Scarani, F. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütheнaus and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[12] G. M. Nikolopoulos and G. Alber, Phys. Rev. A **72**, 032320 (2005).
[13] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[14] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[15] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).
[16] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, Phys. Rev. Lett. **98**, 060503 (2007).
[17] C. H. Bennett, G. Brassard, and J. M. Robert, SIAM J. Comput. **17**, 210 (1988).
[18] G. Berlín, G. Brassard, F. Bussières, N. Godbout, J. A. Slater, and W. Tittel, Natl. Commun. **2**, 561 (2011).
[19] X. Ma, Chi-Hang Fred Fung, H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).
[20] A. Scherer, B. Sanders, and W. Tittel, Opt. Express **19**, 3004 (2011).
[21] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin, Phys. Rev. A **66**, 062308 (2002).
[22] H. de Riedmatten, I. Marcikic, V. Scarani, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **69**, 050304 (2004).
[23] D. Stucki, H. Zbinden, and H. Gisin, J. Mod. Opt. **52**, 2637 (2005).
[24] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, J. Mod. Opt. **56**, 516 (2009).
[25] P. G. Kwiat, J. Mod. Opt. **44**, 2173 (1997).
[26] J. T. Barreiro, N. K. Langford, N. A. Peters, and P. G. Kwiat, Phys. Rev. Lett. **95**, 260501 (2005).
[27] A. Joobeur, B. E. A. Saleh, and M. C. Teich, Phys. Rev. A **50**, 3349 (1994).

[28] R. Loudon, *The Quantum Theory of Light*, 3rd ed. (Oxford University Press, Oxford, 2000).
[29] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, Nature (London) **412**, 3123 (2001).
[30] J. B. Götte, S. Franke-Arnold, and S. M. Barnett, J. Mod. Opt. **53**, 627 (2007).
[31] J. Leach, B. Jack, J. Romero, A. K. Jha, A. M. Yao, S. Franke-Arnold, D. G. Arnold, D. G. Ireland, R. W. Boyd, S. M. Barnett, and M. J. Padgett, Science **329**, 662 (2010).
[32] M. M. Haget, A. Joobeur, and B. E. A. Saleh, J. Opt. Soc. Am. A **16**, 348 (1999).
[33] R. E. Warburton, F. Izdebski, C. Reimer, J. Leach, D. G. Ireland, M. Padgett, and G. S. Buller, Opt. Express **19**, 2670 (2011); J. Leach, R. E. Warburton, D. G. Ireland, F. Izdebski, S. M. Barnett, A. M. Yao, G. S. Buller, and M. J. Padgett, Phys. Rev. A **85**, 013827 (2012).
[34] F. M. Miatto, T. Brougham, and A. M. Yao, e-print arXiv:1111.6449 [quant-ph] (2012).
[35] J. Jeffers, New J. Phys. **8**, 268 (2006).
[36] P. P. Rohde and T. C. Ralph, J. Mod. Opt. **53**, 1589 (2005).
[37] S. M. Barnett and P. M. Radmore, *Methods in Theoretical Quantum Optics* (Oxford University Press, Oxford, 1997).
[38] W. Weaver and C. E. Shannon, *The Mathematical Theory of Communication* (University of Illinois Press, Urbana, Illinois, 1949).
[39] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, (John Wiley and Sons, New York, 1991).
[40] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, Phys. Rev. Lett. **75**, 4337 (1995).
[41] J. P. Torres, A. Alexandrescu and Lluis Torner, Phys. Rev. A **68**, 050301 (2003).
[42] F. M. Miatto, A. M. Yao, and S. M. Barnett, Phys. Rev. A , **83**, 033816 (2011).
[43] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[44] A. M. Yao, New J. Phys. **13**, 053048 (2011).
[45] L. Allen, S. M. Barnett, and M. J. Padgett, *Optical Angular Momentum* (Institute of Physics, Bristol, 2003).
[46] A. Ling, A. Lamas-Linares, and C. Kurtsiefer, Phys. Rev. A **77**, 043834 (2008).
[47] M. J. W. Hall, Phys. Rev. A **55**, 100 (1997).
[48] P. B. Dixon, G. A. Howland, J. Schneeloch, and J. C. Howell, e-print arXiv:1107.5245 [quant-ph] (2011).
[49] D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, I. A. Walmsley, M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, J. Mod. Opt. **51**, 1499 (2004).