Multimode states in decoy-based quantum-key-distribution protocols

Wolfram Helwig,* Wolfgang Mauerer, and Christine Silberhorn
Max Planck Institute for the Science of Light, 91058 Erlangen, Germany
(Received 30 January 2009; published 19 November 2009)

Every security analysis of quantum-key distribution (QKD) relies on a faithful modeling of the employed quantum states. Many photon sources, such as for instance a parametric down-conversion (PDC) source, require a multimode description but are usually only considered in a single-mode representation. In general, the important claim in decoy-based QKD protocols for indistinguishability between signal and decoy states does not hold for all sources. We derive bounds on the single-photon transmission probability and error rate for multimode states and apply these bounds to the output state of a PDC source. We observe two opposing effects on the secure key rate. First, the multimode structure of the state gives rise to a new attack that decreases the key rate. Second, more contributing modes change the photon number distribution from a thermal toward a Poissonian distribution, which increases the key rate.

DOI: 10.1103/PhysRevA.80.052326 PACS number(s): 03.67.Dd

I. INTRODUCTION

The security of classical cryptography is based on the high computational complexity of the decryption process combined with the condition that the adversary only has a limited amount of computational power. In contrast, quantum-key distribution (QKD) allows two parties, Alice and Bob, to share a secret key that is inaccessible to an eavesdropper Eve whose power is only limited by the laws of quantum physics. In 1984, Bennett and Brassard introduced the first QKD protocol BB84 [1]. It is still the most commonly used protocol, although many more have been proposed since then [2–4].

This first theoretical proposal assumed perfect devices, namely, single-photon sources and error-free transmission and detection. With the development of sophisticated security proofs, these restrictions could gradually be lessened. First, security has been proved in the presence of noise [5,6]. In the next step, the necessity of single-photon sources has been taken out of the equation [7]. This, however, reduced the achievable key rate drastically because multiphoton events gave rise to the photon number splitting (PNS) attack [8–10], which Alice and Bob were not able to distinguish from natural losses.

This issue has been resolved with the decoy method, which was introduced by Hwang [11] and has been further developed to a practically realizable form by several researchers [12–15]. In this method, additional *decoy* states with a different photon number distribution than the primary signal states are randomly introduced. It is crucial that decoy states share all other physical characteristics of the signal so that Eve cannot distinguish between decoy and signal. Consequently, the decoys are affected by the PNS attack in the same way as the signal states, and this perturbation of the system reveals Eve's presence. Since Eve has to design her attack in a way that cannot be detected by Alice and Bob (otherwise the protocol is aborted), her attack possibilities are drastically limited when she is confronted with a decoy protocol. This enables Alice and Bob to achieve an improved key rate.

The important assumption that Eve cannot distinguish between photons arising from signal and decoy states is trivially fulfilled for a single-mode description where all photons are created by the same creation operator. However, this model does not match experimental reality well. Hence, in this paper, we treat the scenario where photons are excited into many different modes and the excitation probability for each mode differs between signal and decoy states. This multimode description is, for instance, necessary for a realistic representation of the states created by a parametric down-conversion (PDC) source, in which case the different modes correspond to different spectral modes [16].

This paper is organized as follows. In Sec. II, we review the decoy method and introduce the notation necessary for the subsequent analysis. Section III presents the description of a multimode state with special emphasis on spectral modes for the description of a PDC state. In Secs. IV and V, we describe attack possibilities when multimode states are used and derive bounds that allow us to calculate the achievable key rate in this scenario. Section VI finally applies the analysis to the multimode PDC state and gives bounds on the achievable key rate.

II. DECOY METHOD

The security of the BB84 protocol is based on the no-cloning theorem [17], which prevents Eve from making a copy of a transmitted single photon. However, the security argument is not applicable to multiphoton events because for these events Alice implicitly encodes the same information on all photons in the pulse. This, in turn, allows Eve to obtain an identical copy of Bob's state by splitting away one of the photons. Hence only detection events arising from single photons give a positive contribution to the secure key rate. With current technology, Alice is not able to determine the number of photons her source emitted. Thus Alice and Bob cannot simply ignore multiphoton events. In this scenario, a lower bound on the secure key rate S is given by [7,12]

*wolfram.helwig@physik.uni-erlangen.de

$$S \geq q\{Y_1^{(s)} p_1^{(s)}[1 - H(e_1^{(s)})] - Q^{(s)} f(E^{(s)}) H(E^{(s)})\}. \quad (1)$$

Here $p_n^{(s)}$ ($n \in \mathbb{N}_0$) denotes the photon number distribution of Alice's source, $f(E^{(s)})$ is the error correction efficiency, $H(x) = -x \log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy, and q accounts for incompatible basis choices of Alice and Bob. In the standard BB84 protocol, $q = 1/2$. The overall detection probability is given by the *gain*

$$Q^{(s)} = Y_0 p_0^{(s)} + Y_1^{(s)} p_1^{(s)} + Y_M^{(s)} p_M^{(s)}, \quad (2)$$

where the *yields* $Y_0^{(s)}$, $Y_1^{(s)}$, and $Y_M^{(s)}$ are the detector click probabilities conditioned on emitted zero-, one-, and multiphoton events of Alice's source, respectively. Analogously, the zero-, one-, and multiphoton error rates, e_0, e_1 and e_M, are defined as the error rates conditioned on emitted zero-, one-, and multiphoton events, respectively. The relation to the total quantum bit error rate (QBER) $E^{(s)}$ is given by

$$Q^{(s)} E^{(s)} = e_0 Y_0 p_0^{(s)} + e_1^{(s)} Y_1^{(s)} p_1^{(s)} + e_M^{(s)} Y_M^{(s)} p_M^{(s)}. \quad (3)$$

The QBER and the gain $Q^{(s)}$ are directly accessible from the recorded data of the QKD protocol. However, since Alice and Bob do not know when a single photon was sent, they cannot determine the exact values of $Y_1^{(s)}$ and $e_1^{(s)}$ but need to estimate them using worst-case assumptions. Prior to the decoy method, they had to assume that all multiphoton events produce a click at Bob's detector. This corresponds to $Y_M^{(s)} = 1$, and a lower bound on $Y_1^{(s)}$ can be calculated with Eq. (2). This estimate, however, lies well below the single-photon transmission probability caused by natural losses. In addition, Alice and Bob have to assume that all errors arise from single-photon events, resulting in a very high estimate of $e_1^{(s)}$. These values are actually achieved if Eve performs a PNS attack [8–10] and lead to a drastically reduced key rate [7].

The decoy method enables Alice and Bob to attain better estimates of $Y_1^{(s)}$ and $e_1^{(s)}$. This is achieved by randomly introducing decoy states with independent photon number distributions. For each photon number distribution, the gain and QBER can be determined individually, resulting in better bounds on $Y_1^{(s)}$ and $e_1^{(s)}$.

In this paper, we base our analysis on the so-called *vacuum+weak decoy method* [13,14], which uses two decoy states. Deliberately interspersing the signal stream with vacuum states ($p_n = \delta_{n0}$, gain $Q = Y_0$) allows Alice and Bob to determine the dark count probability Y_0. The second decoy state is of low intensity and features a photon number distribution $p_n^{(d)}$ that differs from the photon number distribution $p_n^{(s)}$ of the regular signal. In the following, we will refer to this state as the decoy state and to the state with photon number distribution $p_n^{(s)}$ as the signal state. The gain for the decoy state is given by

$$Q^{(d)} = Y_0 p_0^{(d)} + Y_1^{(d)} p_1^{(d)} + Y_M^{(d)} p_M^{(d)}, \quad (4)$$

with the yields defined equivalently to the signal yields. The yield Y_0 for an emitted zero-photon state has to be the same for all states because Eve cannot distinguish between vacua arising from different states. However, there is no *a priori* reason for the single- and multiphoton yields to be the same for signal and decoy. In the analyses up to now, it was assumed that Eve cannot distinguish between n-photon events arising from signal and decoy state, resulting in $Y_n^{(s)} = Y_n^{(d)}$ ($n \in \mathbb{N}_0$). Note that this is the assumption we will loosen in Sec. IV, as it is generally not justified in a multimode description of the states. However, proceeding with $Y_n^{(s)} = Y_n^{(d)}$, from Eqs. (2) and (4) the lower bound

$$Y_{1,LB} = \frac{p_2^{(s)}}{p_2^{(s)} p_1^{(d)} - p_1^{(s)} p_2^{(d)}} \times \left(Q^{(d)} - \frac{p_2^{(d)}}{p_2^{(s)}} Q^{(s)} - \frac{p_2^{(s)} p_0^{(d)} - p_0^{(s)} p_2^{(d)}}{p_2^{(s)}} Y_0 \right) \quad (5)$$

on the signal single-photon yield can be derived if the additional condition

$$\frac{Y_M^{(d)}}{Y_M^{(s)}} \leq \frac{p_2^{(d)}/p_M^{(d)}}{p_2^{(s)}/p_M^{(s)}} \quad (6)$$

is satisfied. This is, for instance, fulfilled if both signal and decoy have a Poissonian or thermal distribution with a lower mean photon number for the decoy distribution.

With a similar equation to Eq. (3) for the decoy QBER [i.e., $(\cdot)^{(s)} \to (\cdot)^{(d)}$], an upper bound on the single-photon error rate of the decoy state can be calculated as

$$e_1^{(d)} \leq e_{1,ub}^{(d)} = \frac{1}{p_1^{(d)} Y_{1,LB}^{(d)}} [E^{(d)} Q^{(d)} - e_0 Y_0 p_0^{(d)}]. \quad (7)$$

The postulated indistinguishability of n-photon states for signal and decoy gives $e_{1,ub}^{(s)} = e_{1,ub}^{(d)}$ and $Y_{1,LB}^{(d)} = Y_{1,LB}^{(s)}$, because $Y_1^{(d)} = Y_1^{(s)}$ and $e_0 = 1/2$, since a dark count gives the wrong result 50% of the time.

The derived bounds [Eqs. (5) and (7)] are much tighter than the worst-case assumptions without decoy states. Therefore using them in Eq. (1) results in a significant improvement in the achievable secure key rate [12].

III. MULTIMODE STATE

QKD analyses generally assume that Alice's output states are accurately represented by a single-mode description as

$$\rho^{(s/d)} = \sum_n p^{(s/d)}(n) |n\rangle\langle n|, \quad (8)$$

where $p^{(s/d)}(n)$ denotes the signal and decoy photon number distributions.

This form intrinsically implies that all emitted photons have identical properties, and hence the method presented in Sec. II may be applied. A restriction to output states of this form can, however, be a very strong requirement that is hard to meet in the laboratory. For a PDC source, for instance, this requires the production of two output beams with independent spatiospectral mode structures, which is known to be a very demanding task [18].

In this paper, we extend the decoy method to deal with multimode states of the form

$$\rho^{(s/d)} = \bigotimes_{k=1}^{N} \sum_n p^{(s/d)}(k,n) |n;k\rangle\langle n;k|. \quad (9)$$

Here $|n;k\rangle$ describes a state with n photons in the kth mode and $p^{(s/d)}(k,n)$ is the photon number distribution for the kth

mode for signal or decoy. All the N modes are mutually orthogonal, $\langle n;k|m;l\rangle=\delta_{nm}\delta_{kl}$. The modes can be spectral modes, spatial modes, or embedded into any other degree of freedom the information carrier under consideration might have. For instance, in the case of spectral mode, the states $|n;k\rangle$ are of the form

$$|n;k\rangle=\frac{1}{\sqrt{n!}}(A_{\xi_k}^{\dagger})^n|0\rangle, \tag{10}$$

$$A_{\xi_k}^{\dagger}\equiv\int d\omega\xi_k(\omega)a^{\dagger}(\omega), \tag{11}$$

where $\{\xi_k(\omega)\}$ are a set of orthonormal functions. For a detailed description of this notation, see [19].

In Secs. IV and V, we extend the decoy method to states of the form given by Eq. (9). This means we derive bounds on $Y_1^{(s)}$ and $e_1^{(s)}$ for such a state. In the analysis it is assumed that Alice and Bob, as well as Eve, know all the parameters of the source, in particular the photon number distributions $p^{(s/d)}(k,n)$, precisely. In addition, Eve is able to distinguish between photons in different modes without disturbing the states, as this is possible in principle for orthogonal modes. However, Alice and Bob are not able to discriminate between photons in different modes owing to current technological limitations. In Sec. VI, the results are then applied to the aforementioned PDC source.

IV. BOUND ON $Y_1^{(s)}$

Recall that in a single-mode description, the yields for n-photon signal and decoy states are identical and thus a lower bound on $Y_1^{(s)}$ can be computed by Eq. (5) from the known gains and photon number distributions.

In this section, we develop a means of computing a lower bound on $Y_1^{(s)}$ for multimode states as defined in Eq. (9). For states of this type, $Y_n^{(s)}=Y_n^{(d)}$ is no longer valid for $n\geq 1$. Note, however, that Y_0 is still the same for signal and decoys because for zero emitted photons the resulting state is always described by the same vacuum state and thus Eve cannot treat these pulses differently for signal and decoys. The derivation of the lower bound on $Y_1^{(s)}$ proceeds in three steps. First, we derive a lower bound on the signal single-photon yield $Y_1^{(s)}$ for a given decoy single-photon yield $Y_1^{(d)}$. Then, we determine an upper bound on the decoy multiphoton yield $Y_M^{(d)}$ for a given signal multiphoton yield $Y_M^{(s)}$. Finally, with these two relations, we are able to calculate a lower bound on $Y_1^{(s)}$ for given signal and decoy gains, $Q^{(s)}$ and $Q^{(d)}$.

Step 1: Lower bound on $Y_1^{(s)}$ for a given $Y_1^{(d)}$. Assume Eve has to let a certain fraction $Y_1^{(d)}$ of the decoy single-photon events pass to achieve the desired decoy gain. In this step, we are seeking the lowest possible value for the signal single-photon yield $Y_1^{(s)}$ that is compatible with the given $Y_1^{(d)}$. Using Eq. (9), we find the conditioned one-photon state to be

$$\rho_1^{(s/d)}=\sum_k m_k^{(s/d)}|1;\xi_k\rangle\langle 1;\xi_k|, \tag{12}$$

where we define the mode occupation probabilities by

FIG. 1. (Color online) Eve blocks all photons in the second mode. This results in different single-photon yields for signal and decoy state.

$$m_k^{(s/d)}=\frac{p^{(s/d)}(k,1)\prod_{i\neq k}p^{(s/d)}(i,0)}{P_1^{(s/d)}}, \tag{13}$$

and the single-photon probability is given by

$$P_1^{(s/d)}=\sum_k p^{(s/d)}(k,1)\prod_{i\neq k}p^{(s/d)}(i,0). \tag{14}$$

We have to assume that Alice does not have the technology to determine in which mode a photon resides. Remember that she cannot even determine the total number of emitted photons for a given event. However, an apparatus that measures the number of photons in each mode individually is possible in principle because all modes are orthogonal. Therefore, if we want to claim unconditional security, we have to give Eve knowledge about how many photons each mode contains. For the single-photon case, this means that she knows in which mode the photon is. This, in turn, allows Eve to reach different single-photon yields for signals and decoys by selectively blocking modes if the mode occupation probabilities m_k differ for signal and decoy state.

Figure 1 illustrates how this can be accomplished for the case of two different modes with $m_1^{(d)}=0.7$, $m_2^{(d)}=0.3$, $m_1^{(s)}=0.6$, and $m_2^{(s)}=0.4$. If Eve blocks all photons in the second mode, 70% of the decoy single photon events are transmitted, but only 60% of the signal single photons pass through the channel. This results in the yields $Y_1^{(s)}=0.6$ and $Y_1^{(d)}=0.7$.

For a given decoy single-photon yield $Y_1^{(d)}$, we denote the smallest possible value Eve can achieve for $Y_1^{(s)}$ as $Y_{1,\mathrm{lb}}^{(s)}(Y_1^{(d)})$. In our example above, we have $Y_{1,\mathrm{lb}}^{(s)}=6/7Y_1^{(d)}$ for $Y_1^{(d)}\leq 0.7$ because in this case the photons of the first mode are sufficient to reach $Y_1^{(d)}$. Thus Eve can completely block the second mode and let only photons of the first mode pass. For $Y_1^{(d)}>0.7$, Eve additionally has to let a fraction $(Y_1^{(d)}-0.7)/0.3$ of the photons in the second mode pass to reach $Y_1^{(d)}$, resulting in $Y_{1,\mathrm{lb}}^{(s)}=0.6+(Y_1^{(d)}-0.7)/0.3\times 0.4$.

This concept is easily extended to all N modes that contribute to the state of Eq. (12). Without loss of generality, we take $m_1^{(s)}/m_1^{(d)}\leq m_2^{(s)}/m_2^{(d)}\leq\ldots\leq m_N^{(s)}/m_N^{(d)}$. To achieve the smallest possible ratio between signal and decoy single-photon yield, Eve has to let photons from the mode with the smallest possible ratio between the mode occupation probabilities, mode 1, pass. However, if all photons from this mode are not enough to reach the given decoy yield $Y_1^{(d)}$, Eve has to let photons from additional modes pass. To achieve the smallest possible ratio $Y_1^{(s)}/Y_1^{(d)}$, they have to be chosen from the modes with the next smallest ratio between the mode

occupation probabilities, which are modes $2,3,\ldots,K$. Here the number K of required modes is implicitly defined by

$$\sum_{k=1}^{K-1} m_k^{(\mathrm{d})} \leq Y_1^{(\mathrm{d})} < \sum_{k=1}^{K} m_k^{(\mathrm{d})}, \tag{15}$$

such that both inequalities hold. If Eve lets all photons from the first $K-1$ modes and a fraction $(Y_1^{(\mathrm{d})}-\Sigma_{k=1}^{K-1} m_k^{(\mathrm{d})})/m_K^{(\mathrm{d})}$ of the photons in the Kth mode pass, she achieves the desired decoy single-photon yield,

$$Y_1^{(\mathrm{d})} = \sum_{k=1}^{K-1} m_k^{(\mathrm{d})} + \frac{Y_1^{(\mathrm{d})} - \sum_{k=1}^{K-1} m_k^{(\mathrm{d})}}{m_K^{(\mathrm{d})}} m_K^{(\mathrm{d})}. \tag{16}$$

Since the photons are chosen from the modes that have the smallest ratio between the number of signal photons and decoy photons, this mode selection gives the smallest possible value,

$$Y_{1,\mathrm{lb}}^{(\mathrm{s})}(Y_1^{(\mathrm{d})}) = \sum_{k=1}^{K-1} m_k^{(\mathrm{s})} + \frac{Y_1^{(\mathrm{d})} - \sum_{k=1}^{K-1} m_k^{(\mathrm{d})}}{m_K^{(\mathrm{d})}} m_K^{(\mathrm{s})}, \tag{17}$$

for the signal single-photon yield for a given $Y_1^{(\mathrm{d})}$.

Step 2: Upper bound on $Y_{\mathrm{M}}^{(\mathrm{d})}$ for a given $Y_{\mathrm{M}}^{(\mathrm{s})}$. In this step, we want to find the highest possible decoy multiphoton yield that is compatible with a given signal multiphoton yield. With minor modifications, this works out analogously to step 1, the only difference being that we have to keep track of all possible distributions of the photons among the modes. For this purpose, we introduce the set $Q=\{\mathbf{l}\in\mathbb{N}_0^N | \Sigma_{k=1}^N l_k \geq 2\}$. Each member of this set represents a multiphoton event with l_i photons in the ith mode.

Similarly to m_k for the single-photon case, we define $h_{\mathbf{l}}$ as the probability that a multiphoton event possesses the photon distribution specified by $\mathbf{l}\in Q$. It is given by

$$h_{\mathbf{l}}^{(\mathrm{s/d})} = \frac{1}{P_{\mathrm{M}}^{(\mathrm{s/d})}} \prod_{k=1}^{N} p^{(\mathrm{s/d})}(k,l_k) \tag{18}$$

with the multiphoton probability

$$P_{\mathrm{M}}^{(\mathrm{s/d})} = \sum_{n\geq 2} P_2^{(\mathrm{s/d})} = 1 - P_0^{(\mathrm{s/d})} - P_1^{(\mathrm{s/d})}, \tag{19}$$

where $P_n^{(\mathrm{s/d})}$ denotes the convoluted photon number distribution of all modes. Accordingly, $P_0^{(\mathrm{s/d})}=\Pi_{k=1}^N p^{(\mathrm{s/d})}(k,0)$ and $P_1^{(\mathrm{s/d})}$ is given by Eq. (14). Employing the mode distribution probabilities of Eq. (18), the states of Eq. (9) conditioned on a multiphoton event can be written as

$$\rho_{\mathrm{M}}^{(\mathrm{s/d})} = \sum_{\mathbf{l}\in Q} h_{\mathbf{l}}^{(\mathrm{s/d})} \bigotimes_{k=1}^{N} |l_k;\xi_k\rangle\langle l_k;\xi_k|. \tag{20}$$

Again, Eve is not only allowed to make a photon number measurement but can also determine the mode distribution $\mathbf{l}$ of a multiphoton event. Thus she can selectively block multiphoton events with certain mode distributions. The highest possible $Y_{\mathrm{M}}^{(\mathrm{d})}$ for a given $Y_{\mathrm{M}}^{(\mathrm{s})}$ is achieved if Eve lets only events with the highest ratio between $h_{\mathbf{l}}^{(\mathrm{d})}$ and $h_{\mathbf{l}}^{(\mathrm{s})}$ pass. To sort the mode distributions accordingly, we define $L_1 = \arg\max_{L\in Q} h_L^{(\mathrm{d})}/h_L^{(\mathrm{s})}$ and recursively

$$L_i = \underset{L\in Q\setminus\{L_1,\ldots,L_{i-1}\}}{\arg\max} \frac{h_L^{(\mathrm{d})}}{h_L^{(\mathrm{s})}} \quad \text{for } i\geq 2. \tag{21}$$

With that definition, we can apply the same method as in step 1. For a given $Y_{\mathrm{M}}^{(\mathrm{s})}$, we define K implicitly by

$$\sum_{i=1}^{K-1} h_{L_i}^{(\mathrm{s})} \leq Y_{\mathrm{M}}^{(\mathrm{s})} < \sum_{i=1}^{K} h_{L_i}^{(\mathrm{s})}. \tag{22}$$

The highest possible $Y_{\mathrm{M}}^{(\mathrm{d})}$, compatible with a given $Y_{\mathrm{M}}^{(\mathrm{s})}$, is achieved if all multiphoton events with mode distributions L_1 to L_{K-1} and the remaining fraction $(Y_{\mathrm{M}}^{(\mathrm{s})}-\Sigma_{i=1}^{K-1} h_{L_i}^{(\mathrm{s})})/h_{L_K}$ with mode distribution L_K are transmitted to Bob's side. As a result we have the upper bound

$$Y_{\mathrm{M,ub}}^{(\mathrm{d})}(Y_{\mathrm{M}}^{(\mathrm{s})}) = \sum_{i=1}^{K-1} h_{L_i}^{(\mathrm{d})} + \frac{Y_{\mathrm{M}}^{(\mathrm{s})} - \sum_{i=1}^{K-1} h_{L_i}^{(\mathrm{s})}}{h_{L_K}^{(\mathrm{s})}} h_{L_K}^{(\mathrm{d})} \tag{23}$$

on the decoy multiphoton yield $Y_{\mathrm{M}}^{(\mathrm{d})}$ for a given signal multiphoton yield $Y_{\mathrm{M}}^{(\mathrm{s})}$.

Step 3: The bound on $Y_1^{(\mathrm{s})}$ for given gains $Q^{(\mathrm{s})}$ and $Q^{(\mathrm{d})}$. With the derived relations between the yields of signal and decoy events, we are now able to calculate a lower bound on $Y_1^{(\mathrm{s})}$ for given signal and decoy gains. If the relations were just given by a constant ratio, this would be in direct analogy to the single-mode case where the ratio of signal and decoy yields was fixed. This means we could plug the relations into Eq. (4) and solve Eqs. (2) and (4) for a lower bound on $Y_1^{(\mathrm{s})}$. However, the derived relations [Eqs. (17) and (23)] do not have a simple functional form. Hence an iterative approach is required to determine the lower bound on $Y_1^{(\mathrm{s})}$ from the set of nonlinear equations [Eqs. (2), (4), (17), and (23)].

We first solve Eqs. (2) and (4) for $Y_{\mathrm{M}}^{(\mathrm{s})}$ and $Y_1^{(\mathrm{d})}$, respectively,

$$Y_{\mathrm{M}}^{(\mathrm{s})} = \frac{1}{P_{\mathrm{M}}^{(\mathrm{s})}}[Q^{(\mathrm{s})} - P_0^{(\mathrm{s})}Y_0 - P_1^{(\mathrm{s})}Y_1^{(\mathrm{s})}], \tag{24}$$

$$Y_1^{(\mathrm{d})} = \frac{1}{P_1^{(\mathrm{d})}}[Q^{(\mathrm{d})} - P_0^{(\mathrm{d})}Y_0 - P_{\mathrm{M}}^{(\mathrm{d})}Y_{\mathrm{M}}^{(\mathrm{d})}]. \tag{25}$$

Alice and Bob know Y_0 from the vacuum decoy state. They can measure $Q^{(\mathrm{s})}$ and $Q^{(\mathrm{d})}$, and they know P_0, P_1, and P_M for both signal and decoy because they know the properties of their source. In addition, a trivial lower bound on $Y_1^{(\mathrm{s})}$ is given by $Y_1^{(\mathrm{s})}\geq Y_{1,\mathrm{LB}}^{(\mathrm{s})}=0$. Starting with that value, a tighter bound can be calculated by the following algorithm:

(1) Start by calculating an upper bound on $Y_{\mathrm{M}}^{(\mathrm{s})}$ from $Y_{1,\mathrm{LB}}^{(\mathrm{s})}$ using Eq. (24),

$$Y_{\mathrm{M,UB}}^{(\mathrm{s})} = \frac{1}{P_{\mathrm{M}}^{(\mathrm{s})}}[Q^{(\mathrm{s})} - P_0^{(\mathrm{s})}Y_0 - P_1^{(\mathrm{s})}Y_{1,\mathrm{LB}}^{(\mathrm{s})}]. \tag{26}$$

(2) Next, use $Y_{\mathrm{M,UB}}^{(\mathrm{s})}$ to derive an upper bound on $Y_{\mathrm{M}}^{(\mathrm{d})}$ with Eq. (23),

$$Y_{\mathrm{M,UB}}^{(\mathrm{d})} = Y_{\mathrm{M,ub}}^{(\mathrm{d})}(Y_{\mathrm{M,UB}}^{(\mathrm{s})}). \tag{27}$$

(3) Obtain a lower bound on $Y_1^{(\mathrm{d})}$ from $Y_{\mathrm{M,UB}}^{(\mathrm{d})}$ with Eq. (25),

$$Y_{1,\mathrm{LB}}^{(\mathrm{d})} = \frac{1}{P_1^{(\mathrm{d})}}[Q^{(\mathrm{d})} - P_0^{(\mathrm{d})} Y_0 - P_{\mathrm{M}}^{(\mathrm{d})} Y_{\mathrm{M,UB}}^{(\mathrm{d})}]. \tag{28}$$

(4) Finally, determine a lower bound on $Y_1^{(\mathrm{s})}$ from $Y_{1,\mathrm{LB}}^{(\mathrm{d})}$, using Eq. (17),

$$Y_{1,\mathrm{LB}}^{(\mathrm{s})} = Y_{1,\mathrm{lb}}^{(\mathrm{s})}(Y_{1,\mathrm{LB}}^{(\mathrm{d})}). \tag{29}$$

The value obtained in Eq. (29) can iteratively be plugged into the previously described steps as initial value, which results in an even tighter bound. After each iteration step, the final value for $Y_{1,\mathrm{LB}}^{(\mathrm{s})}$ is at least as large as the starting value, so the iteratively obtained values are monotonically increasing. As $Y_{1,\mathrm{LB}}^{(\mathrm{s})} \leq 1$ is bounded from above (not more than 100% of the events can result in a click of Bob's detector), the series converges, giving the final lower bound on the single-photon yield of the signal state.

V. BOUND ON $e_1^{(\mathrm{s})}$

We also need to bound the error rate of the single-photon events of the signal state from above. In this case, Eve wants to introduce as many errors as possible into the single-photon events of the signal state while leaving the measured QBERs as expected because this way she can gain the maximal amount of information from the signal single-photon events. An upper bound on the decoy single-photon events is given by Eq. (7) if we use $Y_{1,\mathrm{LB}}^{(\mathrm{d})}$ given by the value [Eq. (28)] obtained in the iteration for determining $Y_{1,\mathrm{LB}}^{(\mathrm{s})}$. Since the errors also have to be assumed to be under Eve's control, she is free to choose the modes into which the errors occur. The highest error rate of the signal single-photon events compared to the error rate of the decoy single-photon events is obtained if the errors are introduced into modes with a large $m_k^{(\mathrm{s})}/m_k^{(\mathrm{d})}$ ratio. Hence, if we again define K implicitly by

$$\sum_{k=K}^{N} m_k^{(\mathrm{d})} \leq e_{1,\mathrm{ub}}^{(\mathrm{d})} < \sum_{i=K-1}^{N} m_k^{(\mathrm{d})}, \tag{30}$$

the worst-case assumption is that all photons in modes $N, N-1, \ldots, K$ and a fraction $(e_{1,\mathrm{ub}}^{(\mathrm{d})} - \Sigma_{k=K}^{N} m_k^{(\mathrm{d})})/m_{K-1}^{(\mathrm{d})}$ of the photons in mode $K-1$ are erroneous. This gives the upper bound on the signal single-photon error rate,

$$e_{1,\mathrm{ub}}^{(\mathrm{s})} = \sum_{k=K}^{N} m_k^{(\mathrm{s})} + \frac{e_{1,\mathrm{ub}}^{(\mathrm{d})} - \sum_{k=K}^{N} m_k^{(\mathrm{d})}}{m_{K-1}^{(\mathrm{d})}} m_{K-1}^{(\mathrm{s})}. \tag{31}$$

VI. NUMERICAL SIMULATIONS

With the lower bound on $Y_1^{(\mathrm{s})}$, obtained by Eq. (29) in the iteration, and the upper bound on $e_1^{(\mathrm{s})}$ given by Eq. (31), we can determine a lower bound on the achievable key rate for states of form (9) with Eq. (1).

In the following simulations, we consider the simplest example for the use of a type-II PDC source in a QKD protocol. A type-II PDC process emits photons in two different polarization modes, called signal and idler. (This signal in the signal or idler beam distinction is not to be confused with the signal in the signal or decoy distinction. This standard terminology is somewhat unfortunate for PDC sources in QKD protocols.) In the scenario under consideration, the idler photons are ignored and the signal photons are used as information carriers. In addition to the polarization modes, a realistic model of the PDC output state has to take spectral modes into account. Thus the output state has to be described as follows [16]:

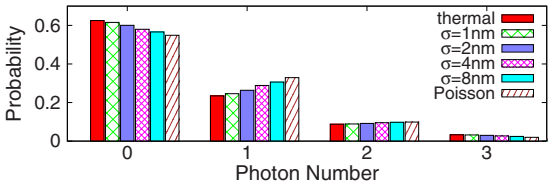

FIG. 2. (Color online) The photon number distributions for different pump widths σ.

$$|\Psi^{(\mathrm{s/d})}\rangle = \bigotimes_{k=1}^{N} \sum_{n} c^{(\mathrm{s/d})}(k,n)|n;k\rangle_{\mathrm{s}}|n;k\rangle_{\mathrm{i}}, \tag{32}$$

where $|n;k\rangle_{\mathrm{s/i}}$ describes a state with n photons in the kth spectral modes as introduced in Eq. (10) (with in general different sets of orthogonal functions for signal and idler). Signal and decoy are created with different pump intensities, $I^{(\mathrm{s})}$ and $I^{(\mathrm{d})}$, which are reflected in the photon number distributions for the spectral modes

$$p^{(\mathrm{s/d})}(k,n) = |c^{(\mathrm{s/d})}(k,n)|^2 = \mathrm{sech}^2\, r_k^{(\mathrm{s/d})} \tanh^{2n} r_k^{(\mathrm{s/d})}, \tag{33}$$

with the squeezing parameters $r_k^{(\mathrm{s/d})} \propto \lambda_k \sqrt{I^{(\mathrm{s/d})}}$. Here λ_k depends on the PDC crystal and the pump and indicates how prominent the kth mode is (see [16] for more details). Since we are only interested in the signal photons, we have to trace over the idler modes, which give the state

$$\rho^{(\mathrm{s/d})} = \mathrm{tr}_{\mathrm{i}} |\Psi^{(\mathrm{s/d})}\rangle\langle\Psi^{(\mathrm{s/d})}| \tag{34}$$

$$= \bigotimes_{k=1}^{N} \sum_{n} p^{(\mathrm{s/d})}(k,n)|n;k\rangle\langle n;k|. \tag{35}$$

This state has the form of Eq. (9), and we can therefore apply the decoy analysis of the previous sections.

The photon number distribution for each spectral mode [Eq. (33)] is a thermal distribution. Thus the single-mode case ($\lambda_k = \delta_{k1}$) corresponds to thermal photon number distribution. With more contributing modes, the distribution is changed from thermal toward a Poissonian distribution (for an explanation of this effect see [16]). This is shown in Fig. 2 for the values of Table I and a mean photon number of 0.6.

Let us first illustrate, by means of a simple example, how different mode occupation probabilities arise for signal and decoy state. Consider a PDC state with just two spectral modes that have $\lambda_1 = \sqrt{0.75}$ and $\lambda_2 = \sqrt{0.25}$. The mode occupation probabilities for a single-photon event are then given by

TABLE I. λ_k for the KTP crystal for different pump widths.

Width σ (nm)	λ_k
1	0.959, 0.194, 0.152, 0.098, 0.088, 0.033, 0.032, 0.014
2	0.871, 0.463, 0.140, 0.064, 0.054, 0.028, 0.001
4	0.690, 0.555, 0.383, 0.222, 0.107, 0.054, 0.050 0.044, 0.023, 0.012, 0.004, 0.003, 0.001
8	0.511, 0.478, 0.427, 0.364, 0.296, 0.228, 0.167 0.117, 0.078, 0.056, 0.047, 0.037, 0.023, 0.015 0.014, 0.011, 0.006, 0.003, 0.001

$$m_1(I) = \frac{p(1,1)p(2,0)}{p(1,1)p(2,0)+p(1,0)p(2,1)} = \frac{\tanh^2 r_1}{\tanh^2 r_1 + \tanh^2 r_2}, \tag{36}$$

$$m_2(I) = \frac{\tanh^2 r_2}{\tanh^2 r_1 + \tanh^2 r_2}. \tag{37}$$

They inherit the intensity dependence from the squeezing parameters r_1 and r_2. This intensity dependence is shown in Fig. 3 along with chosen decoy and signal intensities such that we end up exactly with the states shown in Fig. 1.

Now, we focus on a physically realistic case. Our source is a waveguided periodically poled potassium titanyl phosphate (KTP) crystal with a grating period of $\Lambda=68.40$ μm, length of 5 mm, and waveguide width and height both 4 μm. The pump laser spectrum is centered at a wavelength of 775 nm and the signal and idler are frequency degenerate around 1550 nm. We study four different pump bandwidths σ, which lead to different values for λ_k [16]. They are shown in Table I.

We first consider the case of $\sigma=4$ nm. For given pump intensities for signal and decoy state, the mode occupation probabilities can be calculated with Eqs. (13) and (18) for the single-photon and multiphoton states, respectively. We assume that Eve designs her attack such that her presence cannot be detected. This implies that the measured gains and error rates for signal and decoy state have the values that are expected from natural losses and detection errors. According to [12], they are given by

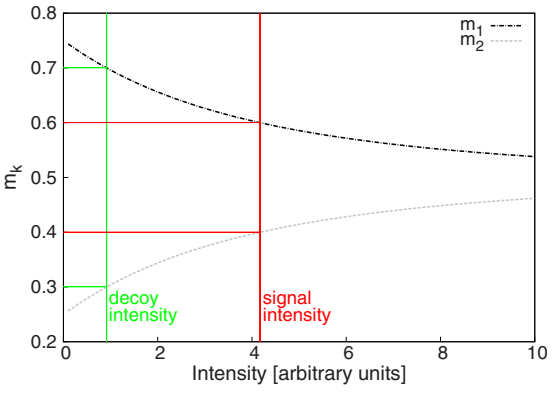

FIG. 3. (Color online) The mode occupation probabilities m_1 and m_2 for a single-photon event in dependence of the pump intensity.

TABLE II. Characteristics of Bob's detector.

Dark count probability	1.7×10^{-6}
Detection error	3.3%
Detector efficiency	4.5%

$$Q^{(s/d)} = \sum_n Y_n P_n^{(s/d)}, \tag{38}$$

$$E^{(s/d)} = \frac{1}{Q^{(s/d)}} \sum_n e_n Y_n P_n^{(s/d)}, \tag{39}$$

with the overall (i.e., convoluted) photon number distributions $P_n^{(s/d)}$ and

$$Y_n \approx \eta_n + p_{\text{dark}}, \tag{40}$$

$$e_n = \frac{1}{Y_n}\left(e_{\text{det}}\eta_n + \frac{1}{2}p_{\text{dark}}\right). \tag{41}$$

In these equations, p_{dark} is the dark count probability of Bob's detector, e_{det} is the detection error [i.e., the probability that Alice prepares a 0 (1), but Bob detects a 1 (0)], and $\eta_n=1-(1-\eta)^n$ is the probability that at least one of n photons arrives at Bob's side and is detected. The overall detection probability $\eta=10^{-\alpha/10}\eta_{\text{det}}$ of each photon is determined by the channel attenuation α in dB and the detector efficiency η_{det}. We use the experimental parameters in Ref. [20] in the simulations, which are shown in Table II.

With the gains and QBER for signal and decoy states [Eqs. (40) and (41)], a lower bound on the signal single-photon yield $Y_1^{(s)}$ and an upper bound on the signal single-photon error rate $e_1^{(s)}$ can be calculated as described in Secs. IV and V. This allows us to compute a lower bound on the achievable key rate according to Eq. (1). We compare this key rate to the key rate for a single-mode source with the same photon number distribution. In other words, the secure key rate one would falsely expect to be achievable if the multimode structure of the PDC state is ignored. It is calculated by Eq. (1) with the bounds on $Y_1^{(s)}$ and $e_1^{(s)}$ given by Eqs. (5) and (7). The corresponding key rates are both plotted in Fig. 4 against the channel attenuation. We find that the key rate drops about 10% when Eve's new possible attack is taken into account by adjusting the bounds on $Y_1^{(s)}$ and $e_1^{(s)}$ accordingly. In both scenarios, the mean photon number of the decoy state is 0.1, and the mean photon number of the signal state is optimized to give the highest key rate.

Figure 5 shows the secure key rate for all different pump widths given in Table I. One can see that the secure key rate is higher when more modes contribute to the PDC process. This effect is explained by the change in the photon number distribution. With more contributing modes, the photon number distribution is shifted from a thermal distribution to a

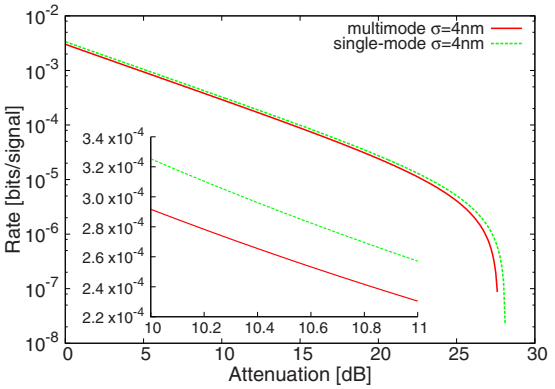

FIG. 4. (Color online) Solid (red) line: lower bound on the secure key rate for the KTP crystal with a pump width of 4 nm. Dashed (green) line: lower bound on secure key rate for the same photon number distribution, but with all photons in the same spectral mode. The inset shows a zoom of the 10–11 dB region. The weak decoy mean photon number is 0.1 in both cases, and the signal mean photon number is optimized to result in the largest possible rate.

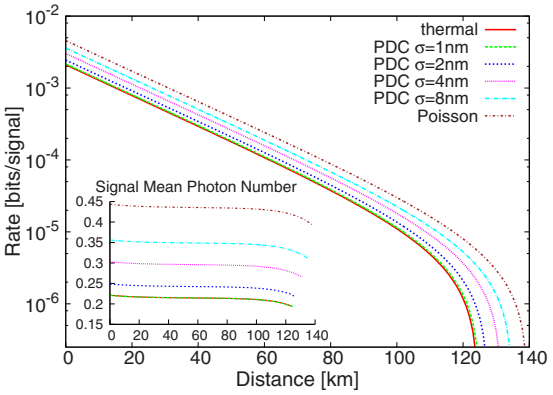

FIG. 5. (Color online) Lower bound on the secure key rate for different pump widths and therefore different mode contributions. The asymptotic cases are the rates for thermal and Poissonian distribution. The inset shows the optimized mean photon number of the signal state. The weak decoy mean photon number is fixed to 0.1 for all scenarios.

Poissonian distribution (see Fig. 2). The Poissonian distribution is favorable in comparison to the thermal distribution because the ratio between single-photon and multiphoton events increases. This permits a higher mean photon number for the signal state, which in turn increases the achievable key rate and distance. The resulting optimal mean photon numbers in dependence of the channel attenuation are depicted in the inset of Fig. 5.

VII. CONCLUSION

In summary, we have pointed out the necessity to carefully pay attention to the output states of the utilized sources but likewise demonstrated that the demand for perfect indistinguishability of the signal and decoy photons, which is hard to implement in practice, can be loosened for only a small cost in the key rate.

The analysis was applied to a parametric down-conversion (PDC) source, where the weak decoy state is created by pumping the crystal with a lower pump intensity. For about ten effectively contributing modes, we observed a drop of the key rate to roughly 90% of the corresponding value in the single-mode case with the same photon number distribution. The simulation was performed for different numbers of effectively contributing modes, leading to the conclusion that the advantageous change in the photon number distribution, which occurs if more modes contribute, has a higher effect on the key rate than the aforementioned decrease due to the new attack possibility presented to Eve by the multimode structure of the states.

This analysis can also be used for a heralded PDC source, as long as the heralding detector is frequency independent, as the resulting states are also of the form of Eq. (9). For heralding with a frequency dependent detector, the analysis has to be extended to the case where the density matrices for signal and decoy state are diagonal in different bases contrary to our condition given by Eq. (9).

Another possibility to produce the decoy state is by passive decoy generation [21,22]. In this scheme, the complications that arise because of the multimode structure of the PDC state can be avoided if a frequency independent detector is available for the decoy generation, as the spectral properties of n-photon states would then be the same for signal and decoy state. This, however, is not the case for a frequency dependent detector because such a detector leads to signal and decoy states with different spectral properties. Again, the resulting states require an analysis for signal and decoy states that are diagonal in different bases.

We believe that this paper is a step toward allowing more general signal and decoy states, which will significantly simplify the design of QKD sources.

ACKNOWLEDGMENTS

This work was supported by the EC under the FET-Open grant agreement CORNER, Grant No. FP7-ICT-213681.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), pp. 175–179.

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[3] M. Dušek, N. Lütkenhaus, and M. Hendrych, Prog. Opt. **49**, 381 (2006).

[4] W. Mauerer, W. Helwig, and C. Silberhorn, Ann. Phys. **158**, 175 (2008).

[5] D. Mayers, J. ACM **3**, 35 (1998).

[6] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[7] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **5**, 325 (2004).
[8] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[9] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[10] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[11] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[12] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[13] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[14] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[15] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).
[16] W. Mauerer, M. Avenhaus, W. Helwig, and C. Silberhorn, Phys. Rev. A **80**, 053815 (2009).
[17] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[18] P. J. Mosley, J. S. Lundeen, B. J. Smith, P. Wasylczyk, A. B. U'Ren, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **100**, 133601 (2008).
[19] P. P. Rohde, W. Mauerer, and C. Silberhorn, New J. Phys. **9**, 91 (2007).
[20] D. Gobby, Z. Yuan, and A. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
[21] W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305(R) (2007).
[22] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007).