Effect of finite detector efficiencies on the security evaluation of quantum key distribution

Marcos Curty and Norbert Lütkenhaus
Institut für Theoretische Physik I, Institut für Optik, Information und Photonik (Max-Planck-Forschungsgruppe), Staudtstrasse 7/B3, Universität Erlangen-Nürnberg, 91058 Erlangen, Germany
(Received 19 December 2003; published 28 April 2004)

Quantum key distribution with the Bennett-Brassard 1984 protocol has been shown to be unconditionally secure even using weak coherent pulses instead of single-photon signals. The distances that can be covered by these methods are limited due to the loss in the quantum channel (e.g., loss in the optical fiber) and in the single-photon counters of the receivers. One can argue that the loss in the detectors cannot be changed by an eavesdropper in order to increase the covered distance. Here we show that the security analysis of this scenario is not as easy as is commonly assumed, since already two-photon processes allow eavesdropping strategies that outperform the known photon-number splitting attack. For this reason there is, so far, no satisfactory security analysis available in the framework of individual attacks.

DOI: 10.1103/PhysRevA.69.042321 PACS number(s): 03.67.Dd, 03.67.−a

I. INTRODUCTION

Quantum key distribution (QKD) [1,2] is a technique that allows two parties (Alice and Bob) to generate a secret key despite the computational and technological power of an eavesdropper (Eve) who interferes with the signals. Together with the Vernam cipher [3], QKD can be used for unconditionally secure data transmission.

The basic ingredient of any QKD protocol is the distribution of *effective* quantum states that can be proved to be entangled [4]. The first complete scheme for QKD is that introduced by Bennett and Brassard in 1984 (BB84 for short) [2]. In a quantum optical implementation of this protocol, Alice encodes each random bit into the polarization state of a single photon. She chooses for her encoding one of two mutually unbiased bases, e.g., either a linear or a circular polarization basis. On the receiving side, Bob measures each photon by selecting at random between two polarization analyzers, one for each possible basis. Once this phase is completed, Alice and Bob use an authenticated public channel to process their correlated data in order to obtain a secret key. This last procedure, called *key distillation*, involves, typically, postselection of data, error correction to reconcile the data, and privacy amplification to decouple the data from Eve [5]. A full proof of the security for the whole protocol has been given in Refs. [6–9].

After the first demonstration of the feasibility of this scheme [10], several long-distance implementations have been realized in the last years (see Ref. [11–14] and references therein). However, these practical approaches differ in many important aspects from the original theoretical proposal, since that demands technologies that are beyond our present experimental capability. Especially, the signals emitted by the source, instead of being single photons, are usually weak coherent pulses (WCP) with typical average photon numbers of 0.1 or higher. These pulses are described by coherent states in the chosen polarization mode. The quantum channel introduces considerable attenuation and errors that affect the signals even when Eve is not present. Finally, the detectors employed by the receiver have a low detection efficiency and are noisy. All these modifications jeopardize the security of the protocol, and lead to limitations of rate and distance that can be covered by these techniques [15,16]. A positive security proof against all individual particle attacks, even with practical signals, has been given in Ref. [17]. More recently, a complete proof of the unconditional security of this scheme in a realistic setting has been achieved [18]. This means that, despite practical restrictions, with the support of the classical information techniques used in the key distillation phase, it is still possible to obtain a secure secret key.

The main limitation of QKD based on WCP arises from the fact that some pulses contain more than one photon prepared in the same polarization state. Now Eve is no longer limited by the no-cloning theorem [19] since in these events the signal itself provides her with perfect copies of the signal photon. She can perform the so-called *photon-number splitting* (PNS) attack on the multiphoton pulses [15]. This attack provides Eve with full information about the part of the key generated with the multiphoton signals [20], without causing any disturbance in the signal polarization. Together with an optimal eavesdropping attack on the single-photon pulses, the PNS attack constitutes Eve's optimal strategy [17,18]. This result is stated for a conservative definition of security. In this paradigm, it is commonly assumed that some flaws in Alice and Bob's devices (e.g., the detection efficiency and the dark count probability of the detectors), together with the losses in the channel, are controlled by Eve, who exploits them to obtain maximal information about the shared key.

In this paper we analyze a different scenario. We impose constraints on Eve's capabilities, and we are interested in the influence that this effect has on her best strategy. It is necessary to distinguish this work from earlier ones: here we consider a more relaxed definition of security than the one in Refs. [17,18]. In particular, we study the situation where Eve is not able to manipulate Alice and Bob's devices at all, but she is limited to act exclusively on the quantum channel (See, e.g., Ref. [21]). The main motivation to consider this scenario is that from a practical point of view it constitutes a reasonable description of a realistic situation, where Alice and Bob can limit Eve's influence on their apparatus by some counterattack techniques. However, this scenario has not been analyzed thoroughly. See Appendix A for a discussion of the papers by Gilbert and Hamrick. In discussions within the scientific community one often hears the hope that it is sufficient to consider the PNS attack, but this time taking into account the finite detection efficiency of Bob's detectors. As a result the loss of a photon in the PNS attack reduces the probability to detect the remaining signal with the inefficient detectors and less multiphoton signals contribute to the final key. This suggests higher available rates. However, the analysis of this scenario is rather subtle, as we will show in this paper. Note that a first counterexample against that belief is contained in Ref. [22] showing that the unambiguous state discrimination attack of Ref. [21] can outperform the adaptation of the photon-number splitting attack of Refs. [16,17] in the discussed scenario of limited eavesdropping capabilities. This result applied to signals containing at least three photons. We show that already two-photon processes allow for improved eavesdropping in the restricted scenario.

With our paper, we point out the difficulty of analyzing the scenario where Bob's detection efficiency cannot be manipulated. For this we refer to the standard BB84 protocol, where in the first part only the raw bit rate (before the key distillation phase) is monitored but not the number of coincidence detections. We construct two specific eavesdropping strategies which do not subtract photons from all the multiphoton pulses, and that are more powerful than the PNS attack for some relevant regimes of the observed error rate. They are based on specifically chosen cloning attacks. The results obtained here do not constitute a complete analysis of Eve's optimal attack under these restrictions, they introduce a class of eavesdropping strategies that become relevant only in this scenario. Our results clearly show that a simple extension of the PNS attack in this scenario fails to deliver security. In an extended version of the protocol, where Alice and Bob can access the complete photon-number statistics of the arriving signal, we find that the advantage of the cloning attacks is not as evident, but requires a deeper analysis.

The paper is organized as follows. In Sec. II we describe in more detail the scenario we consider here. This includes the signal states and detection methods employed by Alice and Bob together with the technologies assumed for Eve. In Sec. III we introduce the complete PNS attack, and we analyze a particular process that is part of this attack and involves only single-photon signals and two-photon signals. In Sec. IV we introduce two more processes that do not subtract photons from the pulses. They are based on cloning machines operating only on two-photon pulses. In Sec. V, these two processes are compared with the PNS process. We show that, for some relevant regimes of the observed error rate in the sifted key and the loss in the channel, the two processes based on cloning machines provide Eve with more information than the PNS process. This happens, in particular, when the loss in the channel is high but the number of nonvacuum signals expected to arrive at Bob's detection device is still greater than the number of multiphoton signals. The extended version of the protocol, where Alice and Bob use the full statistics at their disposal to detect Eve, as introduced in Refs. [5,21,23] is briefly considered in Sec. VI. Finally, Sec. VII concludes the paper with a summary.

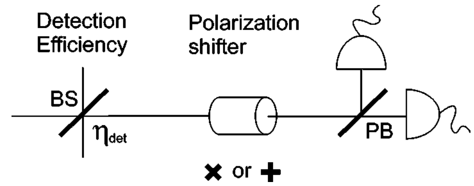

FIG. 1. The polarization shifter allows to change the polarization basis (+ and ×) of the measurement as desired. The polarization analyzer consists of a polarizing beam splitter (PB) and two ideal detectors. The PB discriminates the two orthogonal polarized modes. Detection efficiencies are modeled by a beam splitter (BS) of transmittance η_{det}.

II. TOOLBOX FOR ALICE, BOB, AND EVE

A. Alice

Alice uses WCP signal states that are described by coherent states with a small amplitude α. This corresponds to the description of a dimmed laser pulse. We consider otherwise a perfect implementation of the signal states. The coherent state is given by

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_{n=0}^{\infty}\frac{(\alpha a^{\dagger})^n}{n!}|0\rangle \tag{1}$$

with $a^{\dagger}$ being the creation operator for one of the four BB84 polarizations modes. However, usually there is no reference phase available outside Alice's lab, and the state that Bob and Eve see is not a coherent state $|\alpha\rangle$, but the phase-averaged form of the signal, $\rho=1/2\pi\int_{\phi}|e^{i\phi}\alpha\rangle\langle e^{i\phi}\alpha|d\phi$. This results in an effective signal state which is a mixture of Fock states with a Poissonian photon-number distribution of mean $\mu=|\alpha|^2$. It is described by the density matrix

$$\rho = e^{-\mu}\sum_{n=0}^{\infty}\frac{\mu^n}{n!}|n\rangle\langle n|, \tag{2}$$

where the state $|n\rangle$ denotes the Fock state with n photons in one of the four BB84 polarization states.

B. Bob

We consider that Bob employs the active detection setup shown in Fig. 1. It consists of a polarization analyzer and a polarization shifter which effectively changes the polarization basis of the subsequent measurement. The polarization analyzer has two detectors, each monitoring the output of a polarizing beam splitter. These detectors are characterized by their detection efficiency η_{det}. They can be described by a combination of beam splitters of transmittance η_{det} and ideal detectors [24]. This model can be simplified further by considering that both detectors are equal. In this situation, it is possible to attribute the losses of both detectors to a single-loss beam splitter which is located after the transmission channel. We assume that the detectors cannot distinguish the number of photons of arrival signals, but they provide only two possible outcomes: "click" (at least one photon is detected), and "no click" (no photon is detected in the pulse).

The action of Bob's detection device can be characterized by two positive operator value measures (POVM), one for each of the two polarization bases β used in the BB84 protocol [25]. Each POVM contains four elements [23]: F_{vac}^{β}, F_0^{β}, F_1^{β}, and F_D^{β}. The outcome of the first operator F_{vac}^{β} corresponds to no click in the detectors, the following two POVM operators, F_0^{β} and F_1^{β}, give precisely one detection click (these are the desired measurements), and the last one F_D^{β} gives rise to both detectors being triggered. If we denote by $|n,m\rangle_{\beta}$ the state which has n photons in one mode and m photons in the orthogonal polarization mode with respect to the polarization basis β, the elements of the POVM for this basis are given by

$$F_{vac}^{\beta}=\sum_{n,m=0}^{\infty}\overline{\eta}^{n+m}|n,m\rangle_{\beta}\langle n,m|,$$

$$F_0^{\beta}=\sum_{n,m=0}^{\infty}(1-\overline{\eta}^{n})\overline{\eta}^{m}|n,m\rangle_{\beta}\langle n,m|,$$

$$F_1^{\beta}=\sum_{n,m=0}^{\infty}(1-\overline{\eta}^{m})\overline{\eta}^{n}|n,m\rangle_{\beta}\langle n,m|,$$

$$F_D^{\beta}=\sum_{n,m=0}^{\infty}(1-\overline{\eta}^{n})(1-\overline{\eta}^{m})|n,m\rangle_{\beta}\langle n,m|, \tag{3}$$

where $\overline{\eta}=(1-\eta_{det})$.

The detectors show also noise in the form of dark counts which are, to a good approximation, independent of the signal. Note that the observed errors can be thought as coming from a two-step process: In the first step the signals are changed as they pass Eve's domain in the quantum channel, in the second step random noise from the detector dark counts is added. If we assume that the second step cannot be influenced by Eve, then Alice and Bob can infer the channel error rate, which is assumed to be due to eavesdropping, from their data and their knowledge of the detector performance. This means that only this reduced channel error rate needs to be taken into account in the privacy amplification step.

C. Eve

As discussed before, we allow Eve to have at her disposal all technology allowed by quantum mechanics, but she is limited to use it exclusively on the quantum channel. This assumption has two consequences on Eve's possible eavesdropping strategies that are vital for the security analysis of the next sections. In particular, the detection efficiency η_{det} of Bob's detectors is fixed and Eve cannot influence it to obtain extra information [26]. Moreover, since we consider that the noise of the detectors is independent of the signals entering them, Eve cannot make use of the dark counts to increase her information.

III. THE PNS ATTACK

In the photon-number splitting attack Eve performs a quantum nondemolition measurement of the *total* number of photons of each signal. Whenever she finds that a signal contains two or more photons, she deterministically takes one photon out. The remaining photons are then forwarded to Bob. The photons in Eve's hand will reveal their signal polarization to Eve if she waits with her measurement until she learns the polarization basis during the key distillation phase. If the loss of the channel is strong enough, Eve can block all the single-photon pulses and forward only the remaining photons of multiphoton signals by a lossless channel; on these signals she can obtain the whole information. In this situation no secure key can be generated. When the loss is not high enough for this, then Eve can block only a fraction of the single-photon signals, but she can perform some optimal eavesdropping attack on the remaining single-photon pulses. Moreover, the whole process can be adapted such that it mimics the photon-number statistics of a lossy channel in typical situations [27].

When Bob uses a detection setup with ideal detectors, or Eve can manipulate their efficiency such as $\eta_{det}=1$, then the PNS attack constitutes Eve's optimal strategy [17,18]. The reason is that in this case all signals that provide Eve with full information about the key (multiphoton pulses) contribute for the raw key. If the detectors have a detection efficiency $\eta_{det}<1$ which Eve cannot change, we find that with certain probability the multiphoton signals can also contribute to vacuum events in the detection process. In this situation, there are regimes where the PNS attack is still Eve's optimal eavesdropping strategy. This happens when the loss in the channel is sufficiently high such that the number of nonvacuum signals expected to *arrive* at Bob's detection device is smaller than the number of multiphoton signals. Here we consider the regime where this is not the case. This means that Eve needs to compensate the effect of the undetected multiphoton signals by increasing the number of single-photons signals that are sent to Bob. This fact reduces the effectiveness of the PNS attack, and one might consider the existence of better strategies for Eve.

We focus on a particular combination of processes that are contained in the extended PNS attack [27], now with imperfect detectors. This combination includes only some two-photon processes (with probability p) and some one-photon processes (probability $1-p$) from the whole eavesdropping strategy. It is represented in Fig. 2. The objective is to obtain Eve's maximum information on this combination of processes given a particular disturbance in the signals. For that, we employ the concept of mutual information given by Shannon. Under this definition, it has been proven that the optimal attack on single-photon signals (OA), i.e., the one that provides Eve maximum information about the raw key, coincides with the optimal individual attack on these signals [28]. This optimal individual attack has been introduced by Fuchs *et al.* in Ref. [29]. In the symmetric strategy, every qubit signal ρ_A sent by Alice is transformed into the mixed state $\rho_B=(1-2D)\rho_A+D\mathbb{1}$. The disturbance D represents the error rate in the sifted key within the chosen signals; it is not the overall observed error rate. The connection between the

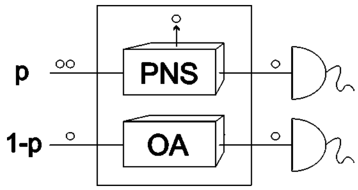

FIG. 2. Process included in the PNS attack. With probability p the pulse contains two photons, Eve takes one photon out of it, and she sends the remaining one photon to Bob. In the case of single-photon signals (probability $1-p$), Eve performs an optimal eavesdropping attack (OA) on these pulses.

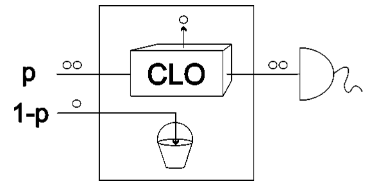

FIG. 3. When the pulse contains two photons, Eve employs an asymmetric cloning machine which produces three clones. She keeps one of the clones, and she sends the other two clones to Bob. This occurs with probability p. In the case of a single-photon pulse (probability $1-p$), she blocks it.

two error rates is made in Sec. V A. For a given value of D, Eve's maximum information in this attack is given by [29]

$$I_{AE} = \tfrac{1}{2}\Phi(2\sqrt{D(1-D)}), \tag{4}$$

where the function Φ is defined as $\Phi(x)=(1+x)\log_2(1+x)+(1-x)\log_2(1-x)$. With this result, now it is straightforward to obtain Eve's maximum information in the PNS process of Fig. 2, as a function of p and D,

$$I_{AE}^{PNS} = p + \frac{1-p}{2}\Phi(2\sqrt{D(1-D)}). \tag{5}$$

In the following section we introduce two more combinations of processes that have the same input signals as those of Fig. 2. Then, in Sec. V we show that these processes provide Eve more information than the PNS process, for some relevant regimes of D. Moreover, the raw bit rate of all the processes can be selected to be the same. This means that the substitution of the combination of processes of Fig. 2 by any of the new combinations leads to a better eavesdropping strategy in terms of Shannon information.

IV. CLONING ATTACKS

Another possible eavesdropping alternative for Eve is not to reduce the number of photons in the signal as in the PNS attack. Instead, she can interact with the signals via a photon-number conserving interaction of a probe system with the signal photons. Then, after the information about the polarization basis is publicly revealed, Eve can obtain information about the key by measuring her probe. In this attack, multiphoton signals maintain their photon number and can therefore contribute with higher probability to a "click" event. Therefore, the fraction of the single-photon signals in this attack can be decreased. In principle, one would like to optimize this type of attack over all possible probes and their interaction. However, for the sake of simplicity, we restrict our analysis to the case of two particular interactions representing cloning machines. This is motivated by the fact that the optimal individual attack for single-photon pulses coincides with the optimal phase-covariant cloning machine [30]. These cases already prove our point.

Consider the process represented in Fig. 3. The input signals are the same of the process of Fig. 2. But here Eve employs an asymmetric cloning machine for all two-photon pulses, while she blocks all the single-photon pulses. The parameter p can be selected such that the processes of Figs. 2 and 3 have the same raw key rate. This is done in Sec. V, when we compare them. We consider two particular asymmetric cloning machines that have been proposed by Acín *et al.* in Ref. [31]. They generalize the $1\rightarrow 2$ asymmetric cloning machines introduced in Refs. [32,33] to the $2\rightarrow 3$ case. But before discussing these cloning machines and studying the performance of the process of Fig. 3 for each of them (strategies A and B below), we introduce a qubit representation for the two-photon pulses emitted by Alice that is used in the next sections.

The set of two-photon signals employed in the BB84 protocol span a three-dimensional Hilbert space. They can be represented in the *symmetric* subspace of two qubits, which contains the signal states $|0\rangle^{\otimes 2}$, $|1\rangle^{\otimes 2}$, $|+\rangle^{\otimes 2}$, and $|-\rangle^{\otimes 2}$, where $|\pm\rangle = 1/\sqrt{2}(|0\rangle \pm |1\rangle)$.

A. Strategy A

In this attack Eve uses an asymmetric universal cloning machine. It takes as an input state two copies of an unknown one-qubit state, plus a two-qubit probe. Its unitary transformation is defined by [31]

$$U|\psi\rangle^{\otimes 2}|00\rangle = \alpha|\psi\rangle^{\otimes 2}|\phi^+\rangle + \beta(\tilde{\sigma}_z|\psi\rangle^{\otimes 2}|\phi^-\rangle + \tilde{\sigma}_x|\psi\rangle^{\otimes 2}|\psi^+\rangle + i\tilde{\sigma}_y|\psi\rangle^{\otimes 2}|\psi^-\rangle), \tag{6}$$

where the operator $\tilde{\sigma}_k = \sigma_k \otimes \mathbb{1} + \mathbb{1} \otimes \sigma_k$ (for $k=x,y,z$) with the usual Pauli operators σ_k, the states $|\psi^\pm\rangle = 1/\sqrt{2}(|01\rangle \pm |10\rangle)$, $|\phi^\pm\rangle = 1/\sqrt{2}(|00\rangle \pm |11\rangle)$, and $\alpha^2 + 8\beta^2 = 1$. In the output, the state of the first two qubits belong to the symmetric subspace of two-qubits signals, and correspond to the two photons that are sent to Bob. The third and fourth qubits constitute the probe that is kept by Eve. Next we calculate the information that Eve can obtain on Alice's signal as part of a sifted key by measuring her probe after the public announcement of basis.

Eve's probe for the signals $|+\rangle^{\otimes 2}$ and $|-\rangle^{\otimes 2}$, after applying the cloning machine, is given by

$$\rho_+ = 2D|-+\rangle\langle -+| + (1-2D)|\varphi_+\rangle\langle\varphi_+| \tag{7}$$

and

$$\rho_- = 2D|+-\rangle\langle +-| + (1-2D)|\varphi_-\rangle\langle\varphi_-|, \tag{8}$$

respectively, where $|\varphi_\pm\rangle = 1/\sqrt{1-2D}(\sqrt{1-4D}|\phi^+\rangle \pm \sqrt{2D}|\psi^+\rangle)$ [34]. Note that in the subspace spanned by the two-qubit states $|-+\rangle$ and $|+-\rangle$ Eve can discriminate between ρ_+ and ρ_- perfectly. In the orthogonal subspace spanned by $|\phi^+\rangle$ and $|\psi^+\rangle$, however, the states ρ_+ and ρ_- present a nonvanishing overlap $x=\langle\varphi_+|\varphi_-\rangle=(1-6D)/(1-2D)$. In this subspace, Eve's maximum information is given by $I_{AE}=1/2\Phi(\sqrt{1-x^2})$ [35,36]. This means that Eve's maximum information in this cloning machine can be written as a function of D as

$$I_{AE}^{A}=2D+\frac{1-2D}{2}\Phi\left(\frac{\sqrt{8D(1-4D)}}{1-2D}\right). \tag{9}$$

This expressions holds also for the signals of the other polarization basis, so that it denotes also the total Shannon information over all signals.

Here, and also in the following section, we consider that double click events are not discarded by Bob, but they contribute to the raw key. Every time Bob obtains a double click, he just decides randomly the bit value [5].

B. Strategy B

The second cloning machine we consider is a phase-covariant cloning machine. The unitary transformation of this cloning machine is given by [31]

$$U|\varphi\rangle|00\rangle=(V|\varphi\rangle|0\rangle)|0\rangle+(\tilde{V}|\varphi\rangle|0\rangle)|1\rangle, \tag{10}$$

where $|\varphi\rangle$ can be any state in the symmetric two-qubit Hilbert space, and V is the unitary transformation:

$$V|00\rangle|0\rangle=|000\rangle,$$

$$V|\psi^+\rangle|0\rangle=\frac{\cos\gamma(|010\rangle+|100\rangle)+\sin\gamma|001\rangle}{\sqrt{1+\cos^2\gamma}},$$

$$V|11\rangle|0\rangle=\frac{\cos\gamma|110\rangle+\sin\gamma(|011\rangle+|101\rangle)}{\sqrt{1+\sin^2\gamma}}. \tag{11}$$

$\tilde{V}$ has the same form as V but interchanging zeros and ones on the right-hand side of Eq. (11), and $0\leqslant\gamma\leqslant\pi$. The first two output qubits of this cloning machine belong again to the symmetric subspace of two-qubit signals and correspond with the two photons which are sent to Bob, while the other two qubit constitute Eve's probe.

Following the same argumentation used in strategy A, when Alice sends the signals $|+\rangle^{\otimes 2}$, $|-\rangle^{\otimes 2}$ [37], the state of Eve's probe is given by ρ_+ or ρ_-, depending on the particular state chosen by Alice. The states ρ_+ and ρ_- can be written in the basis $|+\rangle|+\rangle$, $|+\rangle|-\rangle$, $|-\rangle|+\rangle$, $|-\rangle|-\rangle$ as

$$\rho_+=\frac{1}{16}\begin{pmatrix} a & 0 & 0 & b\\ 0 & d & e & 0\\ 0 & e & f & 0\\ b & 0 & 0 & c\end{pmatrix} \text{ and } \rho_-=\frac{1}{16}\begin{pmatrix} c & 0 & 0 & b\\ 0 & f & e & 0\\ 0 & e & d & 0\\ b & 0 & 0 & a\end{pmatrix}, \tag{12}$$

respectively, where the coefficients a, b, c, d, e, and f are complicated functions of the parameter γ. The exact expression of these coefficients is given in Appendix B. To calculate Eve's maximum information in this case, we can decompose Eve's optimal measurement again in two steps. First, she performs a projection measurement onto the two orthogonal subspaces spanned by $|+\rangle|+\rangle$ $|-\rangle|-\rangle$ and $|+\rangle|-\rangle$, $|-\rangle|+\rangle$, respectively. This measurement reduces the optimization problem in the whole space, to discriminate in each subspace between two equiprobable one-qubit states whose density matrices have the same invariants. This problem was solved by Levitin in Ref. [35]. The maximum of the mutual information in each subspace is given by $I=1/2\Phi(\sqrt{1-r-2d})$, where r represents the trace of the product of the two states, and d is the determinant of their density matrices. Using the expressions for Eve's maximum information in each subspace one can obtain Eve's maximum information in the cloning machine as a function of the coefficients a, c, d, and f. It is given implicitly by

$$I_{AE}^{B}=\frac{1}{32}\left\{(a+c)\Phi\left(\frac{a-c}{a+c}\right)+(d+f)\Phi\left(\frac{d-f}{d+f}\right)\right\}. \tag{13}$$

The disturbance D in this case has the form

$$D=\frac{1}{2}\left\{1-\frac{1}{\sqrt{2(1+\cos^2\gamma)}}\left(\cos\gamma+\frac{1}{\sqrt{1+\sin^2\gamma}}\right)\right\}. \tag{14}$$

Again, due to symmetry with respect to the polarization bases, Eq. (13) holds also for the total average Shannon information.

V. PNS ATTACK VERSUS CLONING ATTACKS

The processes represented in Figs. 2 and 3, for both cloning machines, give a symmetric detection pattern. That is, if Bob measures the signals in the same basis chosen by Alice when preparing the states, then the probability of obtaining a correct result, a wrong result, or a double click is the same for all the signals. Otherwise the outcomes corresponding to events with one detection click are completely random. For a fair comparison of the PNS process and the two cloning processes, we need to assure that the raw bit rate in Bob's detectors is the same for all of them, $p\eta_{det}+(1-p)\eta_{det}=p\eta_{det}(2-\eta_{det})$. The left-hand-side of the equation is the number of clicks of the PNS process, while the right-hand side is the number of clicks expected in Fig. 3 for both cloning machines. This means that $p=1/(2-\eta_{det})$. If we include this value in Eq. (5), Eve's maximum information in the PNS process is now written as

$$I_{AE}^{PNS}=\frac{1}{2-\eta_{det}}\left\{1+\frac{1-\eta_{det}}{2}\Phi(2\sqrt{D(1-D)})\right\}. \tag{15}$$

This expression can now be directly compared with Eq. (9) and (13). The results are plotted in Fig. 4 and show regimes of D for which the process based on cloning machines provides Eve with more information than the PNS process. Note that Eve's maximum information in the cloning processes is independent of η_{det}. This fact comes from the matching con-

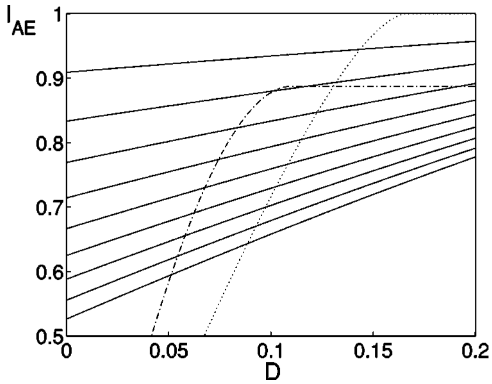

FIG. 4. Eve's maximum information vs the disturbance D: PNS process for increasing, equally spaced values of η_{det} (solid). The lower line corresponds to $\eta_{det}=0.1$, while the upper line corresponds to $\eta_{det}=0.9$. Universal cloning machine, strategy A (dotted). Phase-covariant cloning machine, strategy B (dashdot).

dition for the raw bit rate. In the PNS process, as expected, when η_{det} approaches 1, I_{AE}^{PNS} also approaches 1, since the PNS attack is the optimal strategy for Eve's in the case of ideal detectors. In the phase-covariant cloning machine of strategy B, Eve's maximum information never reaches 1. The reason is that in this particular cloning machine, none of the two qubits kept by Eve can reach a fidelity 1 with respect to the input state. For low values of D, this cloning machine gives Eve more information than the universal cloning machine of strategy A. From the perspective of cloning machines this fact is not surprising. The fidelity achievable in the clones depends always on the set of allowed input states. As more information about the input set is known, better the input states can be cloned. The phase-covariant cloning machine exploits the fact that the input states are *equatorial* qubits. That is, the z component of their Bloch vector is zero. The cloning machine of strategy A, however, is designed to clone *any* input qubit with the same fidelity.

A. Observed error rate

In this section we obtain the relationship between the disturbance D, which appears in Fig. 4, and the overall observed error rate e which is measured in the experiment. This relationship can be established by an analysis of the PNS attack alone, which includes here the optimal eavesdropping on single-photon signals, as before.

The probability that a multiphoton signal undergoes the PNS attack and then is detected by Bob's detection device is given by

$$P_{arr}^{multi} = \sum_{n=2}^{\infty} P(n,\mu)[1-\overline{\eta}^{n-1}], \tag{16}$$

where $P(n,\mu)=e^{-\mu}\mu^n/n!$ is the photon-number distribution of the signal states emitted by Alice, given by Eq. (2). On the other hand, the expected click rate at Bob's side has the form

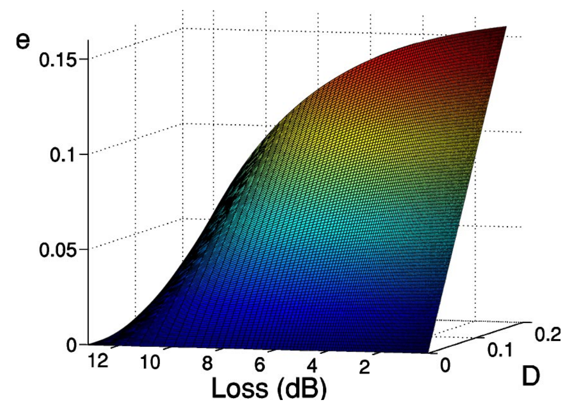

FIG. 5. Observed error rate e vs the disturbance D as a function of the loss in decibel of the quantum channel. The mean photon number μ is 0.1 and η_{det} is 0.2 in this example.

$$P_{exp} = 1 - e^{-\mu\eta_{det}\eta_t}, \tag{17}$$

where η_t is the transmission efficiency of the quantum channel. The total loss in decibel of the quantum channel is given by $-10\log_{10}\eta_t$. From P_{arr}^{single} and P_{exp} one can obtain the probability that single-photon signals contribute to the raw key. It is given by

$$P_{arr}^{single} = P_{exp} - P_{arr}^{multi}. \tag{18}$$

The multiphoton pulses do not introduce any error in the sifted key. This means that

$$e = \frac{P_{arr}^{single}}{P_{exp}} D. \tag{19}$$

After substituting the values of P_{exp} and P_{arr}^{single} into Eq. (19) we finally obtain

$$e = \frac{e^{-\mu}[\eta_{det}e^{\mu\eta_{det}\eta_t} + e^{\mu}(1-\eta_{det}) - e^{\mu[1-\eta_{det}(1-\eta_t)]}]}{(1-\eta_{det})(1-e^{\mu\eta_{det}\eta_t})} D. \tag{20}$$

This result is illustrated in Fig. 5 for some typical values of μ and η_{det}. When the loss in the channel increases, the observed error rate e for each value of D, as expected, decreases. The regime that we consider here corresponds with a value of the loss in the channel such as Eve can perform a PNS attack on all the multiphoton pulses, but $P_{exp} > P_{arr}^{multi}$. The first condition requires

$$P_{exp} \leqslant \eta_{det} P(1,\mu) + P_{arr}^{multi}, \tag{21}$$

which provides an upper bound for the transmission efficiency of the channel

$$\eta_t \leqslant -\frac{\ln\left[\dfrac{e^{-\mu}\{e^{\mu(1-\eta_{det})} - \eta_{det}[1+\mu(1-\eta_{det})]\}}{1-\eta_{det}}\right]}{\mu\eta_{det}}. \tag{22}$$

The second constraint $P_{exp} > P_{arr}^{multi}$ implies a lower bound for η_t

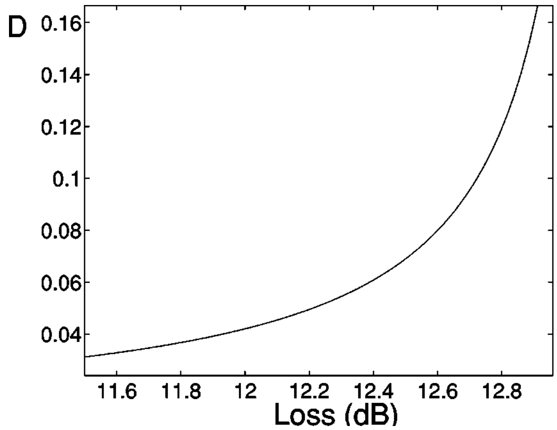

FIG. 6. The disturbance D as a function of the loss in decibel of the quantum channel for a fixed value of the observed error rate $e=0.01$. The mean photon number μ is 0.1 and η_{det} is 0.2.

$$\eta_t > - \frac{\ln\left[\dfrac{e^{-\mu\eta_{det}} - \eta_{det}e^{-\mu}}{1-\eta det}\right]}{\mu\eta_{det}}. \tag{23}$$

The meaning of this condition is to guarantee that we are not in a regimen where the PNS attack is still Eve's optimal strategy. When $\mu=0.1$ and $\eta_{det}=0.2$, we obtain for the lower and upper bounds 0.17 dB and 13.2 dB, respectively.

The process based on cloning machines becomes more powerful than the PNS process for lower values e when the loss is high. The typical value of the observed error rate in the experiments is around 1% if we consider only errors in the quantum channel. Therefore, it is interesting to see how the value of the disturbance D changes as a function of the loss in the channel when we impose e to be 1%. This is illustrated in Fig. 6. We find, in combination with Fig. 4, that for losses higher than 12.5 dB the PNS attack is clearly no longer optimal for these typical parameters.

It is worth to point out that when the losses in the channel are small, but still inside the interval imposed by Eqs. (22) and (23), the eavesdropping attack which includes the cloning machine can be made more powerful than the PNS attack even for a lower value of e than the one given in Eq. (20). The reason is that, although in this situation Eve cannot discard too many single-photon pulses, she can redistribute the errors from the single-photon processes into the two-photon processes. To this end, she increases her intrusion via the cloning attack on the two-photon signals, while she reduces her intrusion on the single-photon signals. The exploitation of this effect is beyond the scope of this paper.

VI. PHOTON STATISTICS

In the previous sections, we consider the case of the standard BB84 protocol, where only the raw bit rate is monitored. Here, we briefly discuss the case of the extended version of the protocol, where Alice and Bob use the full statistics at their disposal to detect Eve.

In this scenario, it is straightforward to see that the processes of Figs. 2 and 3 are not equivalent. The PNS process of Fig. 2 can never produce a double click in Bob's detectors, while the process of Fig. 3 presents always a nonvanishing probability of producing a double click, independently of the basis that Bob uses for his measurement. In fact, the PNS attack never produces a double click event when Bob chooses for his measurement the same basis that Alice used when preparing the signals. This means that, in principle, Alice and Bob might employ this information to discard any eavesdropping strategy that includes the cloning process. However, if we consider a real implementation of the protocol, then the situation is not so simple. The reason is that the quantum channel is not just lossy, but presents a misalignment that introduces errors in the signals [38]. As a result we have that any multiphoton signal has a nonzero probability of providing a double click, independently of the basis used by Bob in his measurement. This means that Eve must adapt the PNS attack such that it reproduces the expected misalignment in the channel. Otherwise her attack would be detected. In particular, Eve has to introduce some noise in the signals that are sent to Bob. In the case of single-photon pulses, this can be achieved by sending the signals through a depolarizing channel of appropriate parameters. This is precisely the effect of the symmetric OA introduced in Sec. III. Therefore, in these pulses, Eve can always get information from this extra noise. The multiphoton pulses, however, gives already Eve full information about the key, and she cannot exploit the noise she needs to introduce to get more information from the single-photon pulses.

The eavesdropping attack which includes the cloning machine can also be adapted such that it reproduces the statistics that is expected from a realistic channel. However, the question whether it remains more powerful than the PNS attack, in this scenario, requires a deeper analysis. If we consider the situation where Eve performs a PNS attack on the pulses that contain more than two photons, and the misalignment in the channel is sufficiently strong for Eve to get full information from the cloning process, then Eve can obtain as much information as with the PNS attack. If the misalignment is smaller, it seems that the strategy that combines the cloning process with the PNS attack on the remaining multiphoton pulses cannot be more powerful than the PNS attack. The reason is that the adapted version of the PNS attack still contains processes that do not produce any double click in Bob's detectors, independently of the basis that Bob uses for his measurement. To compensate this effect, Eve has to subtract more than one photon from the multiphoton pulses, such that she creates processes that do not produce double clicks. But now the effectiveness of the complete strategy decreases, since the probability that the signals which provide Eve full information about the key (multiphoton pulses) contribute to the raw key decreases.

Although this fact constitutes a handicap of the eavesdropping strategy that combines the cloning process of Fig. 3 with the PNS attack on the rest of the pulses, it might be of relative importance in practice. Double clicks are rare events that have a very small probability to occur, and the statistical fluctuations in the channel, together with the effect of dark counts in Bob's detectors, make the detection of Eve's presence not easy. Moreover, Eve might also use a mixed strategy that combines probabilistically the PNS process of Fig. 2 and the cloning process of Fig. 3, such as her attack remains still more powerful than the PNS attack, while making her detection even more difficult.

VII. CONCLUSION

In an ideal quantum optical implementation of QKD, the sender uses single photons to encode the information he transmits. However, current experiments are not based on single-photon sources, but they are usually based on WCP with a low average photon number. Also the detectors employed by the receiver are not perfect, but have a low detection efficiency and are noisy. This fact, together with the loss in the quantum channel, limits the distances that can be covered by these methods. In this scenario, it is tempting to assume that the loss in the detectors cannot be changed by Eve in order to increase the covered distance, while the PNS attack, like in the case of a conservative definition of security, still constitutes Eve's optimal strategy. In this paper we disprove this belief for the case of the standard BB84 protocol, where only the raw bit rate (before the key distillation phase) is monitored. We constructed two specific eavesdropping strategies which include processes that do not subtract photons from the pulses, and that are more powerful than the PNS attack for some relevant regimes of the observed error rate and the loss in the channel. This happens, in particular, when the loss in the channel is high but the number of nonvacuum signals expected to arrive at Bob's detection device is still greater than the number of multiphoton signals. These strategies are based on the use of cloning machines. A complete analysis of Eve's optimal attack in this situation is still missing. In the extended version of the BB84 protocol, where Alice and Bob consider the full statistics at their disposal, the situation is not as straightforward, and a deeper security analysis of this scenario is required.

ACKNOWLEDGMENTS

The authors wish to thank A. Acín, A. Dolinska, P. van Loock, and Ph. Raynal for very useful discussions, and especially K. Tamaki for his critical discussion of this paper. We would also like to thank Gerald Gilbert for the clarifying discussion of his investigations. This work was supported by the DFG under the Emmy Noether programme and the network of competence QIP of the state of Bavaria.

APPENDIX A: RELATED WORK

An investigation of the scenario where Eve cannot improve Bob's detectors has been undertaken in Ref. [22]. We believe that this investigation is incomplete so far. The authors claim that they have performed a thorough analysis of the situation where Bob's detection efficiency cannot be manipulated by Alice, together with the restriction of an "individual attack." The authors define individual attack radically different from the usual terminology that is used in the analysis of quantum key distribution: they refer to attacks that act on *photons* individually, rather than *signals*. In practice, this means that the authors consider optimal attacks on single-photon signals, which can be implemented by attaching a probe to a single-photon; on the other hand, they disallow attaching a probe to a two-photon signal, since that would mean to interact with the two photons "coherently". In fact, they state [22] that such manipulations would be possible only when quantum computers become available.

Of course, it is not unusual to start with some assumptions about restrictions of eavesdropping strategies. For example, investigation of an individual attack scenario (now referring to the standard definition that relates to the signal pulses) has proven to be very powerful since the analysis can be performed easily and the resulting parameters for privacy amplification and the secure key rate correspond roughly to the subsequently derived values that assure security against all attacks, including coherent attacks on all signals. From this experience the individual attack derives its role as a first step investigation of the performance and security analysis of QKD schemes. The relationship between individual and coherent attacks has been strengthened by the results of Wang [28].

In the scenario considered in Ref. [22] we cannot see an equivalent role. Another motivation to investigate restricted scenarios might be the technological challenge of different eavesdropping strategies. However, the technological difference between attaching a probe to a single photon as compared to attaching a probe to a two-photon signal is not evident. Clearly, these questions do not invalidate the obtained results. However, in our point of view, the authors of Ref. [22] are inconsistent in describing the restrictions of their considered eavesdropping attacks. They claim that as a consequence of their restriction they need to consider only three types of attacks.

(1) "Direct attacks" in which Eve can unambiguously determine the signal state by a direct measurement of the signal. This corresponds to the unambiguous state discrimination attack in Ref. [21]. (Requires at least three photons.)

(2) "Indirect attacks," which is precisely the PNS attack [15–17] that extracts one photon from the signal. (Requires at least two photons.)

(3) "Combined attacks" which perform the indirect and the direct attack. (Requires therefore at least five photons, and is in the analysis later on shown to be an inferior attack.)

It is left open how these categories emerge and why this should be a complete description. As first point of criticism note that the authors apply for the direct attack the results of Ref. [21] that provide the performance for optimal unambiguous state discrimination measurements. Can we implement this attack by acting "individually" on photons? A second point of criticism is that to perform these attacks Eve needs to know the number of photons in each pulse. If one thinks of photons as distinguishable particles in a pulse, this might be easy. In a proper quantum optical description, however, these type of counting mechanisms, which do not disturb the signal, will require in all experience the same level of interaction between a probe and the total signal, as does a general eavesdropping attack on the signal.

So far, we pointed at inconsistencies that do not endanger the security statement derived in Ref. [22]. These attacks overestimate Eve's capabilities as compared to the initial restriction that require "individual" attacks on photons. However, the categorization by Gilbert and Hamrick left out possible attacks. Those attacks still operate on individual photons only. As an example let us consider a two-photon pulse. According to Ref. [22] the only attack we need to consider is the PNS attack. Instead, let Eve perform a direct measurement on the photons, for example, in the sense of a minimum-error measurement. Of course, the error will be nonzero, since on a two-photon state in the BB84 polarizations one cannot perform successfully unambiguous state discrimination. However, optimal eavesdropping on single-photon signals also results in some errors. Another attack would be to separate the two photons. Then one can attack probes to both photons and try to combine the photons again in Bob's detection apparatus, e.g., by sending them to Bob in close sequence so that Bob does not notice that they have been separated. Moreover, similar attacks are omitted for higher photon numbers.

These examples question the completeness of the proposed classification of eavesdropping attacks in Ref. [22]. Note that after receiving an advance copy of this manuscript the authors of Ref. [22] revised their work, acknowledging the incompleteness of their analysis. This means that we have to treat the classification as an assumption that only those three classes are of relevance. This includes the assumption that for the two-photon pulse the PNS attack is optimal in their restricted scenario. As a consequence, a security claim for an experimental implementation of QKD should not be based on this analysis, as done in Refs. [22,39,40], since it underestimates Eve's ability. Nevertheless, within the three investigated classes of eavesdropping attacks, Gilbert and Hamrick have been able to show that the unambiguous state discrimination attack can be more effective for Eve than the photon-number splitting attack for signals containing three or more photons.

APPENDIX B. EXPLICIT EXPRESSIONS

In this appendix we provide the exact expressions for the coefficients a, b, c, d, e, and f that are introduced in Eq. (12), as a function of the angle γ:

$$a = 1 + \frac{4\sin\gamma}{\sqrt{3+\cos(2\gamma)}} + \frac{10\sin(2\gamma)}{\sqrt{3+\cos(2\gamma)}\sqrt{1+\sin^2\gamma}} + \frac{2\cos\gamma}{\sqrt{1+\sin^2\gamma}} + \cos^2\gamma\left(\frac{8}{1+\cos^2\gamma} + \frac{1}{1+\sin^2\gamma}\right) + 4\sin^2\gamma\left(\frac{1}{3+\cos(2\gamma)} + \frac{1}{1+\sin^2\gamma}\right),$$

$$b = 1 + \frac{2\cos\gamma}{\sqrt{1+\sin^2\gamma}} + \frac{8\sin^2\gamma[9+\cos(2\gamma)]}{-17+\cos(4\gamma)} + \cos^2\gamma\left(\frac{8}{1+\cos^2\gamma} + \frac{1}{1+\sin^2\gamma}\right),$$

$$c = 1 - \frac{4\sin\gamma}{\sqrt{3+\cos(2\gamma)}} - \frac{10\sin(2\gamma)}{\sqrt{3+\cos(2\gamma)}\sqrt{1+\sin^2\gamma}} + \frac{2\cos\gamma}{\sqrt{1+\sin^2\gamma}} + \cos^2\gamma\left(\frac{8}{1+\cos^2\gamma} + \frac{1}{1+\sin^2\gamma}\right) + 4\sin^2\gamma\left(\frac{1}{3+\cos(2\gamma)} + \frac{1}{1+\sin^2\gamma}\right),$$

$$d = 1 + \frac{4\sin^2\gamma}{3+\cos(2\gamma)} + \frac{\cos^2\gamma}{1+\sin^2\gamma} - \frac{2\cos\gamma}{\sqrt{1+\sin^2\gamma}} + \frac{4\sin\gamma(-\cos\gamma + \sqrt{1+\sin^2\gamma})}{\sqrt{3+\cos(2\gamma)}\sqrt{1+\sin^2\gamma}},$$

$$e = 1 - \frac{4\sin^2\gamma}{3+\cos(2\gamma)} + \frac{\cos^2\gamma}{1+\sin^2\gamma} - \frac{2\cos\gamma}{\sqrt{1+\sin^2\gamma}},$$

and

$$f = 1 - \frac{4\sin\gamma}{\sqrt{3+\cos(2\gamma)}} + \frac{4\sin^2\gamma}{3+\cos(2\gamma)} + \frac{\cos^2\gamma}{1+\sin^2\gamma} - \frac{2\cos\gamma}{\sqrt{1+\sin^2\gamma}} + \frac{2\sin(2\gamma)}{\sqrt{3+\cos(2\gamma)}\sqrt{1+\sin^2\gamma}},$$

[1] S. Wiesner, SIGACT News **15**, 78 (1983).

[2] C. H. Bennett and G. Brassard, in *Proceeding IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE Press, New York, 1984), p. 175.

[3] G. S. Vernam, J. Am. Inst. Electr. Eng. **45**, 109 (1926).

[4] M. Curty, M. Lewenstein, and N. Lütkenhaus, e-print quant-ph/0307151.

[5] N. Lütkenhaus, Appl. Phys. B: Lasers Opt. **69**, 395 (1999).

[6] D. Mayers, J. ACM **48**, 351 (2001).

[7] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[8] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, in *Proceedings of the Thirty Second Annual ACM Symposium on Theory of Computing, New York, USA* (ACM Press, New York, 2000), 715 (2000).

[9] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).

[10] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).

[11] C. Marand and P. D. Townsend, Opt. Lett. **20**, 1695 (1995).

[12] D. S. Bethune, M. Navarro, and W. P. Risk, Appl. Opt. **41**, 1640 (2002).

[13] R. J. Hughes, J. E. Nordholt, D. Derkacs, and C. G. Peterson, New J. Phys. **4**, 43 (2002).

[14] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, New J. Phys. **4**, 41 (2002).

[15] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).

[16] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[17] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[18] H. Inamori, N. Lütkenhaus, and D. Mayers, e-print quant-ph/0107017.
[19] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[20] Note that by a public communication protocol that differs from the BB84 announcement of the bases, Eve no longer obtains full information about those bits. See Ref. [31] and V. Scarani, A. Acín, N. Gisin, and G. Ribordy, e-print quant-ph/0211131.
[21] M. Dušek, M. Jahma, and N. Lütkenhaus, Phys. Rev. A **62**, 022306 (2000).
[22] G. Gilbert and M. Hamrick, e-print quant-ph/0009027.
[23] N. Lütkenhaus, Phys. Rev. A **59**, 3301 (1999).
[24] B. Yurke, Phys. Rev. A **32**, 311 (1985).
[25] Alternatively, one can also characterize Bob's detection setup using only one POVM which already includes the action of the polarization shifter.
[26] For instance, any attempt by Eve to shift the wavelength of the signals into a region of a higher detection efficiency of Bob's detectors can be blocked by the use of a narrow frequency filter.
[27] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).
[28] X.-B. Wang, e-print quant-ph/0110089.
[29] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).
[30] D. Bruss, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).
[31] A. Acín, N. Gisin, and V. Scarani, Phys. Rev. A **69**, 012309 (2004).
[32] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[33] C.-S. Niu and R. B. Griffiths, Phys. Rev. A **58**, 4377 (1998).
[34] When Alice uses the basis $|0\rangle,|1\rangle$ the situation is equivalent.
[35] L. B. Levitin, in *Quantum Communications and Measurements*, edited by V. P. Belavkin, O. Hirota, and R. L. Hudson, (Plenum Press, New York, 1995), p. 439.
[36] C. A. Fuchs, in *Proceedings of the Fourth International Conference on Quantum Communication, Measurement, and Computing*, 1998, edited by P. Kumar, G. M. D'Ariano, and O. Hirota (Kluwer Academic, New York, 2000), p. 11.
[37] If Alice uses the other basis, the situation is again equivalent. But note that for this cloning machine one has to change the notation, and use the states $|\bar{0}\rangle$, $|\bar{1}\rangle$ instead of $|0\rangle$, $|1\rangle$, where $|\bar{0}\rangle = 1/\sqrt{2}(|0\rangle + i|1\rangle)$ and $|\bar{1}\rangle = 1/\sqrt{2}(|0\rangle - i|1\rangle)$.
[38] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[39] G. Gilbert and M. Hamrick, Algorithmica **34**, 314 (2002).
[40] G. Gilbert and M. Hamrick, e-print quant-ph/0106033.