Strathprints Institutional Repository

Conditional beam splitting attack on quantum key distribution

John Calsamiglia[1], Stephen M. Barnett [2], and Norbert Lütkenhaus[3]
[1] *Helsinki Institute of Physics, PL 64, FIN-00014 Helsingin yliopisto, Finland*
[2] *Department of Physics and Applied Physics, University of Strathclyde,John Anderson Building, 107 Rottenrow,Glasgow G4 0NG, Scotland.*
[3] *MagiQ Technologies Inc., 275 Seventh Avenue, 26th floor, NY 10001-67 08, USA.*
(Received June 28, 2006)

We present a novel attack on quantum key distribution based on the idea of *adaptive absorption* [1]. The conditional beam splitting attack is shown to be much more efficient than the conventional beam spitting attack, achieving a performance similar to the, powerful but currently unfeasible, photon number splitting attack. The implementation of the conditional beam splitting attack, based solely on linear optical elements, is well within reach of current technology.

I. INTRODUCTION

The use of quantum effects extends our communication capabilities beyond the solutions offered by classical communication theory. A prominent example is *quantum key distribution* (QKD) which allows to expand a small initial secret key shared between two parties into a larger secret key. This task, which cannot be accomplished within classical communication theory, enables the two parties to exchange secret messages via the encryption technique of the *one-time pad* [2]. The idea has been introduced by Wiesner [3] and the first complete protocol for QKD has been given by Bennett and Brassard [4].

In a quantum optical implementation, the sender (Alice) encodes a random bit value "0" and "1" in the orthogonal polarization states of a single photon. She chooses at random either a linear or a circular polarization basis. The receiver (Bob) uses a polarization bases chosen at random from these two bases. In the following classical communication, Alice and Bob identify those signals for which they used the same basis, and the corresponding bit values form the *sifted key*. Either due to noise or due to eavesdropping, Alice's and Bob's version of the sifted key differ. As long as the error rate is below some threshold, they can correct these errors and perform privacy amplification [5] to obtain a secure key. The theoretical security analysis of this scheme has been a subject of intense research and only recently a full proof of security for the whole protocol has been given [6–9].

A first implementation of this protocol [10] demonstrated the feasibility of this scheme. Since then, many groups improved the implementations. State of the art schemes can maintain the coherence of the system over distances as far as 50 km. However, the signals used in these implementations are not single photon signals. Instead, weak coherent pulses (WCP) are used with typical average photon numbers of 0.1 or higher. The signals are described by coherent states in the chosen polarization mode. This modification of the signals together with the large loss of the fiber optical implementations over long distances opens a security loophole [11]. The restrictions on practical implementations imposed by the use of WCP signals has been demonstrated [12], giving a limit on the distance over which QKD can be performed as a function of Bob's detection efficiency and dark count rate. Nevertheless, it has been shown that, despite these restrictions, it is still possible to obtain a secure key [13,14]

The key process which makes Eve very powerful if Alice and Bob use WCP signals is the *photon number splitting attack* (PNS) [12,13]. In this attack Eve performs a quantum non-demolition measurement (QND) of the *total* number of photons of the signal. Whenever she finds that a signal contains two or more photons, she deterministically takes one photon out of the signal. The remaining photons of the signal are then forwarded over a lossless channel to Bob. For a WCP with mean photon number μ, sent by Alice, Eve obtains a single photon in the same polarization state as those in the signal reaching Bob with probability

$$p_{\rm PNS}^{\rm succ} = 1 - {\rm e}^{-\mu} - \mu {\rm e}^{-\mu}. \qquad (1)$$

Eve now can delay the measurement on that photon until she learns the polarization basis of each signal, thereby learning the bit value for each signal. In order to ensure that Bob does not get too many signals compared to the installed lossy quantum channel, Eve can actually block some signals completely, starting with the initial one-photon signals which cannot be split. We find that this strategy gives the complete key to Eve once the losses of the installed quantum channel are so high that she can block all single photon signals.

This splitting process used in the PNS attack is allowed by quantum mechanics, but the implementation is out of reach of current technology. Therefore earlier analyses of this situation made use of the *beam splitting attack* (BS) which has the appeal of simplicity and feasibility. The basic concept uses the idea that a lossy quantum channel acts like a combination of a lossless channel and a beam splitter which accounts for the losses. Eve monitors the second output arm of the beam splitter and will gain the complete knowledge of a bit of the sifted key (via a delayed measurement) if a multi-photon signal is split such that Bob and Eve both get at least one photon of the signal. The central quantities are the probability that

Bob receives a non-vacuum signal

$$P^{\rm B}_{\rm BS}[\neg 0] = 1 - \exp\left(-\mu\eta\right) \qquad (2)$$

where η is the single photon transmission efficiency of the quantum channel. The probability that Bob and Eve both receive a signal is

$$p^{\rm succ}_{\rm BS} = \left[1 - \exp\left(-\mu\eta\right)\right]\left[1 - \exp\left(-\mu(1-\eta)\right)\right]. \qquad (3)$$

Despite its simplicity and perfect simulation of the lossy channel, the beam splitter attack is very ineffective when replacing channels with large losses, i.e. large transmission distances. In that case, for example, two photon signals are more likely to see both photons being directed to Eve (and therefore becoming useless) rather than being split.

In [1] the authors present the idea of *adaptive absorption*. This consists of sending a photonic signal through a linear absorber in which absorption events can be continuously monitored in such a way that as soon as a single photon is absorbed, a feed-forward mechanism decouples the signal from the absorbing medium. With this simple procedure it is possible to extract precisely one photon from a field-mode prepared in any state (other than the vacuum, of course). In this paper we show how the idea of adaptive absorption leads to the *conditional beam splitting attack* (CBS) on weak coherent pulse QKD. By using only linear optical elements, the CBS reduces the number of events where more than one photon is split off. This allows an eavesdropping efficiency that overwhelms the conventional beam splitting attack and can be as large as the ones given by the PNS.

The paper will be organized as follows. In Sec. II we describe the CBS attack and introduce the quantum jump method, which in turn will be used to calculate the state of the signal during the various stages of the attack. The results will allow us to compare the performances of the CBS and the conventional BS attack. For sake of simplicity this will be done in the scenario in which the eavesdropper is able delay her measurement until the encoding basis is announced by Alice [15]. In Sec. III we consider the more realistic situation in which Eve does not have the technological skills to store photons, and introduce a variation of the CBS where Eve tries to split two single photons from the signal before forwarding it to Bob. In Sec. IV we study the photon statistics in Bob's detectors and see that in principle Alice and Bob could use this information to disclose Eve's attack. The possibility of improving the CBS attack by using mixed strategies will be investigated in Sec. V. In Sec. VI we rederive some basic results for finite beam splitters and compare them with the ones obtained using the quantum jump method. Sec. VII concludes the paper with a brief summary.

II. CONDITIONAL BEAM SPLITTING ATTACK

As mentioned in the introduction the hope is to take advantage of the fact that the signal bits are implemented through polarized coherent states with very low mean photon number (instead of single photons). To do that Eve will weakly couple her modes to the signal modes and try to extract one excitation from the signal sent by Alice. As soon as she gets one photon into her modes, Eve will allow any remaining signal photons to reach Bob through an ideal channel. Otherwise she will keep on trying for a longer time. If she does not succeed after a maximum coupling time τ, Eve will directly send the signal to Bob through the ideal channel.

After Alice announces publicly the encoding basis used to send each of the bits, Eve can measure her photon to learn the bit value of transmitted signal [15]. Only in the cases where the multiphoton signal is split in such a way that both Eve and Bob receive a non-vacuum signal, will the bit value learned by Eve form part of the sifted key shared between Alice an Bob. We will therefore refer to the probability of this event as the probability of success of the CBS ($p^{\rm succ}_{\rm CBS}$). Since this attack does not produce any qubit errors, we will take the probability of success as a figure of merit for the attack. On the other hand, in order to remain unnoticed, Eve's attack has to be such that the number of non-vacuum signals that arrive to Bob agrees with what he expects from the lossy channel. Hence, the probability $P^{\rm B}_{\rm CBS}[\neg 0]$ that Bob receives a non-vacuum signal fixes a bound on the eavesdropping attack. The probabilities $p^{\rm succ}_{\rm CBS}$ and $P^{\rm B}_{\rm CBS}[\neg 0]$ will be the central quantities when evaluating the attack.

In Fig.1 a possible implementation of the CBS is shown. The initial state sent by Alice occupies only two photonic modes (a and b) corresponding for example to the two polarization degrees of freedom of a traveling mode. Conditional beam splitting consists of sending the input state to a polarization independent weak beam splitter. A measurement to determine if there are any photons is then done in the weakly coupled output arm (modes a_e and b_e). If no photon is detected the signal is sent through an identical beam splitter again. Otherwise the signal is transmitted through a perfect channel without any further processing.

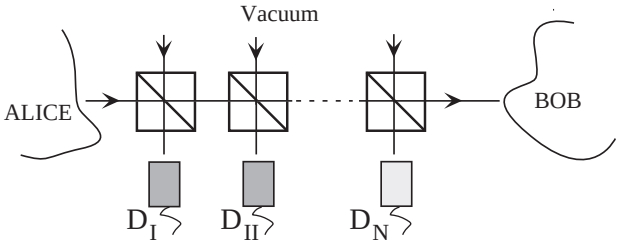

FIG. 1. Possible experimental realization of the conditional beam splitting attack.

To investigate this procedure we will take the limit of infinitesimally weak beam splitting which will allow us to take results from quantum jump methods [16–18] as we did for the study of adaptive absorption [1]. In Sec. VI we

will give some numerical results for finitely weak beam splitters. Quantum jump methods are wave function (as opposed to density matrix) approaches to study the evolution of small systems coupled to a large reservoir. In addition to being a very powerful method it has a nice physical interpretation: The stochastic evolution of the wave function corresponds to the stochastic read outs of the continuously monitored reservoir.

We preface our analysis with a brief review of the quantum jump approach to open systems. Suppose that initially the system is in the state $|\phi(0)\rangle$. If no jump occurs the evolution of the system is described by the effective Hamiltonian, $H_{\text{eff}} = H_S - \frac{i}{2}\sum_m J_m^\dagger J_m$,

$$\left|\phi^0(t)\right\rangle = \mathrm{e}^{-iH_{\text{eff}}t}\left|\phi(0)\right\rangle. \tag{4}$$

Here H_S is the Hamiltonian of the isolated system and the J_m's are the jump operators which account for the coupling to the reservoir. Since the effective Hamiltonian is not hermitian, this state $\left|\phi^0(t)\right\rangle$ is not normalized. The square of its norm gives the probability of having no jump after a time t,

$$p_0(t) = \langle\phi(0)|\,\mathrm{e}^{iH_{\text{eff}}^\dagger t}e^{-iH_{\text{eff}}t}\left|\phi(0)\right\rangle \tag{5}$$

If a jump to a mode m occurs in a time between t and $t+\delta t$ then the system will be in the state

$$|\phi^m(t+\delta t)\rangle = \sqrt{dt}J_m\left|\phi(t)\right\rangle \tag{6}$$

immediately after this period. And again the probability of this event is given by the square of the norm of the conditional state,

$$\delta p_m(t) = \langle\phi(t)|\,J_m^\dagger J_m\left|\phi(t)\right\rangle dt \tag{7}$$

Using these probabilities one can follow the history of the system's wave function when the reservoir is continuously monitored to detect what kind of jump occurred or if any jump occurred at all. It can be shown that by averaging over different histories the state of the system at a given time t, one recovers the master equation

$$\frac{d\rho}{dt} = -i[H_S,\rho] - \frac{1}{2}\sum_m (J_m^\dagger J_m\rho + \rho J_m^\dagger J_m) + \sum_m J_m\rho J_m^\dagger \tag{8}$$

for the system density operator ρ. The first term in this equation describes the standard unitary evolution of the system. The last two terms describe the relaxation process due to the coupling of the system to the reservoir. In order for this description to be true, the coupling and the reservoir have to be such that the jump probability $\delta p_m(t)$ is very small and does not depend on the previous history of the system.

In this paper we use the quantum jump method to study the evolution of the system formed by the *signal modes* (a and b), and Eve's modes (a_e and b_e). The action of the infinitesimally weak beam splitting together with a measuring device that checks if the number of photons in Eve's modes has increased will play the role of reservoir being continuously monitored. An increase in the photon number in Eve's modes is then represented by the jump operator

$$J = \epsilon(a_e^\dagger a + b_e^\dagger b), \tag{9}$$

where $\epsilon \ll 1$ is the reflection coefficient of the weak beam-splitting. After this jump the photons in Eve's modes and the signal photons will be in a shared wave function. If no jump occurs Eve's modes will remain in the vacuum state.

The initial state is given by

$$|\phi(0)\rangle = |\alpha;\beta\rangle\,|0;0\rangle, \tag{10}$$

where the first two modes are the signal modes initially in a coherent state and with a definite polarization, and the last modes are Eve's modes. The mean photon number of the signal sent by Alice is $\mu = |\alpha|^2 + |\beta|^2$. If Eve does not intervene then the signal that Bob will receive after going through the lossy channel is

$$\left|\phi_\eta^B\right\rangle = |\sqrt{\eta}\alpha;\sqrt{\eta}\beta\rangle\,|0;0\rangle, \tag{11}$$

where η is the transmissivity of the channel. This means that the probability that Bob gets a non-vacuum signal is

$$P_\eta^{\mathrm{B}}[\neg 0] = 1 - P_\eta^B[0] = 1 - \exp(-\mu\eta), \tag{12}$$

where $P_\eta^{\mathrm{B}}[0]$ is the probability of Bob getting the vacuum signal.

We now proceed to calculate what happens when Eve tries to eavesdrop on the signal using the conditional beam splitting attack (CBS). At time $t_o = 0$ Eve starts a conditional beam splitting attack on the signal sent by Alice. The conditional state of the system after a time t when no photon has been detected in Eve's modes is

$$\begin{aligned}\left|\phi^0(t)\right\rangle &= \mathrm{e}^{-t\frac{1}{2}J^\dagger J}\left|\phi(0)\right\rangle \\ &= \mathrm{e}^{-\frac{t\epsilon^2}{2}(n_a+n_b)}\left|\alpha;\beta\right\rangle\left|0;0\right\rangle \\ &= \mathrm{e}^{\frac{1}{2}(\gamma_t^2-1)\mu}\left|\gamma_t\alpha;\gamma_t\beta\right\rangle\left|0;0\right\rangle,\end{aligned} \tag{13}$$

where we have defined $\gamma_t = \exp(-\frac{t\epsilon^2}{2})$ and used the normal ordered form of the exponential of the number operator [19]. The squared norm of this state is the probability of detecting no photon in Eve's mode after a time t,

$$p_0(t) = \left\langle\phi^0(t)\right|\left.\phi^0(t)\right\rangle = \mathrm{e}^{(\gamma_t^2-1)\mu}. \tag{14}$$

If the first jump occurs in the time interval $[t, t+dt]$ then the conditional state of the system is

$$\begin{aligned}&\left|\phi^1(t+dt)\right\rangle = J\mathrm{e}^{-t\frac{1}{2}J^\dagger J}\left|\phi(0)\right\rangle \\ &= \mathrm{e}^{\frac{1}{2}(\gamma_t^2-1)\mu}J\left|\gamma_{t_1}\alpha;\gamma_t\beta\right\rangle\left|0;0\right\rangle \\ &= \mathrm{e}^{\frac{1}{2}(\gamma_t^2-1)\mu}\epsilon\gamma_{t_1}\left|\gamma_t\alpha;\gamma_{t_1}\beta\right\rangle(\alpha\left|1;0\right\rangle + \beta\left|0;1\right\rangle).\end{aligned} \tag{15}$$

The probability density of detecting a photon in Eve's modes at the time interval $[t, t+\delta t]$ is therefore given by

$$p_1(t) = \left\langle \phi^1(t) \left| \phi^1(t) \right\rangle = \epsilon^2 \gamma_{t_1}^2 \mu \mathrm{e}^{(\gamma_{t_1}^2 - 1)\mu}. \right. \tag{16}$$

As already mentioned, the first thing that Alice and Bob will check to detect the presence of Eve, is that Bob receives a fraction of non-vacuum signals consistent with the lossy channel, given in (12). That is,

$$P_{\mathrm{CBS}}^{\mathrm{B}}[\neg 0] = P_{\eta}^{\mathrm{B}}[\neg 0] \;\text{ or }\; P_{\mathrm{CBS}}^{\mathrm{B}}[0] = P_{\eta}^{\mathrm{B}}[0]. \tag{17}$$

The total probability that after the CBS attack Bob gets a vacuum signal is

$$\begin{aligned} P_{\mathrm{CBS}}^{\mathrm{B}}[0] &= p_0(\tau) |\langle 0;0 \,|\gamma_\tau \alpha; \gamma_\tau \beta\rangle\,|^2 + \\ &\quad + \int_0^\tau p_1(t) |\langle 0;0 \,|\gamma_t \alpha; \gamma_t \beta\rangle\,|^2 dt \\ &= \mathrm{e}^{-\mu}(1 + \mu(1-\gamma_\tau^2)), \end{aligned} \tag{18}$$

where we have made use of Eqs. (14) and (16). With the results of Eqs. (12) and (18) we find the required value of the coupling time τ so that condition expressed in Eq. (17) is fulfilled,

$$\gamma_\tau^2 = \mathrm{e}^{-\epsilon^2 \tau} = \frac{1}{\mu}(1 + \mu - \mathrm{e}^{\mu(1-\eta)}). \tag{19}$$

Notice that $\gamma_\tau^2 < \eta$.

In order to quantify the performance of the CBS we will now calculate the probability of a successful splitting $p_{\mathrm{CBS}}^{\mathrm{succ}}$. This is the probability that Eve manages to extract one photon from the signal and still leaves at least one photon for Bob. Splittings that leave the transmitted signal in the vacuum state are not useful to Eve since these bits will not contribute to the sifted key. The success probability for the CBS attack is given by

$$\begin{aligned} p_{\mathrm{CBS}}^{\mathrm{succ}} &= 1 - (P_{\mathrm{CBS}}^{\mathrm{B}}[0] + P_{\mathrm{CBS}}^{E}[0] - P^{\mathrm{EB}}[0,0]) \qquad (20) \\ &= 1 - \mathrm{e}^{-\mu}(1 + \mu(1-\gamma_\tau^2)) - \mathrm{e}^{(\gamma_\tau^2 - 1)\mu} + \mathrm{e}^{-\mu} \\ &= 1 - \mu \mathrm{e}^{-\mu}(1-\gamma_\tau^2) - \mathrm{e}^{-(1-\gamma_\tau^2)\mu}, \qquad (21) \end{aligned}$$

where $P_{\mathrm{CBS}}^{E}[0] = p_0(\tau)$ is the probability of having no photon in Eve's modes (i.e. no jump) after the attack and $P^{\mathrm{EB}}[0,0] = \mathrm{e}^{-\mu}$ is the probability that there are photons neither in Eve nor in Bob's modes.

By inverting Eq. (19) we find the transmissivity η 'mimicked' (in the sense of Eq. (17)) by the CBS attack,

$$\eta_{\mathrm{CBS}} = 1 - \frac{1}{\mu}\ln(1 + \mu(1-\gamma_\tau^2)). \tag{22}$$

Since η_{CBS} is an increasing function of γ_τ^2 and we know that this achieves its minimum for $\tau \to \infty$ ($\gamma_\tau^2 \to 0$), we find that, given a mean photon number μ, the attack just described cannot mimic arbitrarily large channel losses. The minimum transmissivity is then given by

$$\eta_{\mathrm{CBS}}^{\min} = 1 - \frac{1}{\mu}\ln(1+\mu) \approx \frac{1}{2}\mu - \frac{1}{3}\mu^2 + O(\mu^3). \tag{23}$$

This makes sense since for $\tau \to \infty$ all non-vacuum signals will leak one photon to Eve while the remaining photons always reach Bob. It is clear, therefore, that the removal of only one photon cannot account for arbitrarily high channel losses. In order to meet Bob's expectations even when $\eta \leq \eta_{\mathrm{CBS}}^{\min}$, Eve can apply the protocol corresponding to $\eta_{\mathrm{CBS}}^{\min}$ and then block the outgoing signals with a probability

$$p_{\mathrm{CBS}}^{\mathrm{block}} = \frac{1 - \mathrm{e}^{\mu\eta}}{1 - \mathrm{e}^{\mu\eta_{\mathrm{CBS}}^{\min}}}. \tag{24}$$

Note that if the channel loss is equal to or larger than $1 - \eta_{\mathrm{CBS}}^{\min}$, then the probability of success is equal to the probability of having more than one photon in a signal pulse

$$p_{\mathrm{CBS}}^{\mathrm{succ}}(\eta_{\mathrm{CBS}}^{\min}) = 1 - \mathrm{e}^{\mu} - \mu \mathrm{e}^{\mu}. \tag{25}$$

This means that for these high channel losses (i.e. $\eta \leq \eta_{\mathrm{CBS}}^{\min}$) Eve can extract one excitation from the signal without modifying Bob's expected number of non-vacuum signals. All Bob's non-vacuum contributions effectively come from the multiphoton part of the signal pulses, and Eve will possess one photon from each of those signals. Therefore she will obtain the *full* sifted key shared by Alice and Bob after the public announcement of the bases. This could never have happen if Eve had chosen the BS attack. This is a very important feature since Eve's knowledge of the full key does not leave any room for Alice and Bob to perform privacy amplification to obtain a secure key.

Taking into account the blocking, in the regime of high losses, the success probability calculated in (21) takes the following form

$$p_{\mathrm{CBS}}^{\mathrm{succ}} = \begin{cases} 1 - \mu \mathrm{e}^{-\mu}(1-\gamma_\tau^2) - \mathrm{e}^{-(1-\gamma_\tau^2)\mu} & : \eta > \eta_{\mathrm{CBS}}^{\min} \\ p_{\mathrm{CBS}}^{\mathrm{block}} \lim\limits_{\gamma_\tau \to 0} p_{\mathrm{CBS}}^{\mathrm{succ}} = 1 - \mathrm{e}^{-\mu\eta} & : \eta \leq \eta_{\mathrm{CBS}}^{\min} \end{cases}. \tag{26}$$

In order to evaluate the performance of an attack it is more convenient to normalize the probability of success with the probability that Bob gets a non-vacuum signal (potential sifted key bit) to obtain the *key fraction* known by Eve,

$$f_{\mathrm{CBS}} = \frac{p_{\mathrm{CBS}}^{\mathrm{succ}}}{1 - P_{\mathrm{CBS}}^{\mathrm{B}}[0]}. \tag{27}$$

As discussed previously, for $\eta \leq \eta_{\mathrm{CBS}}^{\min}$ Eve can acquire the whole key, so in this regime $f_{\mathrm{CBS}} = 1$. For other channel loss values the key fraction never reaches unity. Similarly one can define the same quantity for the BS attack obtaining

$$f_{\mathrm{BS}} = \frac{p_{\mathrm{BS}}^{\mathrm{succ}}}{1 - P_{\mathrm{BS}}^{\mathrm{B}}[0]} = 1 - \mathrm{e}^{-(1-\eta)\mu}, \tag{28}$$

where we have made use of Eq. (2) and (3). It is easy to prove that the fraction of key known by Eve is always bigger for the CBS than for the BS attack. In Fig. 2 we can see these fractions as a function of the channel transmissivity for a typical value of the mean photon number used in current experiments (see also Fig. 8).

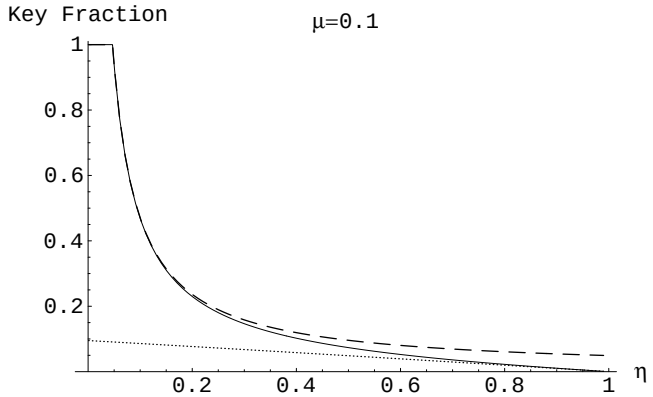

FIG. 2. Fraction of the key known by Eve in CBS (solid curve), BS (dotted) and PNS (dashed) attacks for $\mu = 0.1$

In order to compare quantitatively the CBS with the BS we define the performance quotient $q_{\text{CBS}} = \frac{f_{\text{CBS}}}{f_{\text{BS}}}$ which is plotted in Fig. 3 as a function of the mean photon number of the signal pulses and the channel transmissivity.

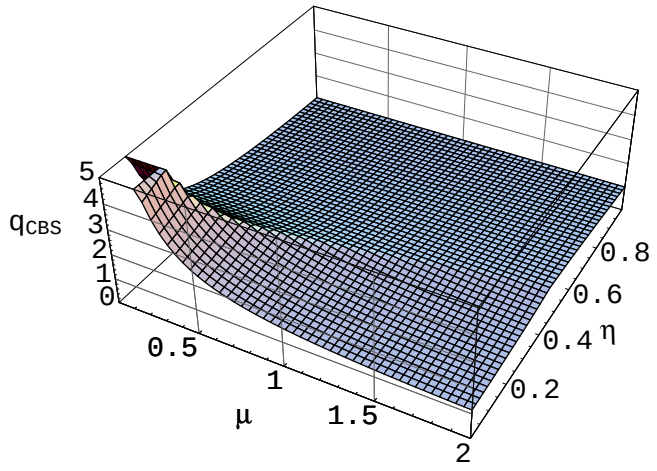

FIG. 3. Performance quotient q_{CBS} for the CBS. Since it is not bounded from above we have only plotted values smaller than five.

We see that for small μ the CBS can be substantially better than the BS. For example, for the experimentally reasonable values $\mu = 0.1$ and $\eta = 0.1$ the CBS provides Eve with a fraction of the key $q_{\text{CBS}} = 5.4$ times bigger than the BS attack. For a fixed mean photon number μ, the optimum advantage $q_{\text{CBS}}^{\max} = 1 + \mu^{-1}$ is achieved when the channel losses are $\eta = \eta_{\text{CBS}}^{\min}$.

III. CBS WITHOUT STORAGE

There is an important fact that makes the CBS, as described above, rather more technically demanding than the BS. In order to follow the CBS protocol described in the previous section Eve has to be able to perform two experimentally non-trivial tasks [20]. *a)* Firstly she has to detect the presence of photons in her modes a_e and b_e without altering their polarization. This is necessary because Eve has to be able to carry out the conditional dynamics, i.e. stop the splitting as soon as she gets the desired photon. This operation is not as technologically demanding as the PNS since it only needs to discriminate the non-vacuum states from the vacuum. However, it is out of reach of the immediately available technology. *b)* The second task Eve must be able to realize is to store the extracted photon until the encoding basis is publicly announced by Alice.

In the conventional beam splitting attack Eve is not required to carry out task *a)*. On the other hand, we notice that Alice can always delay the public announcement, making it harder for Eve to store coherently the signal and thereby, effectively constraining Eve to attacks that do not rely on the storage of the extracted signal. This of course applies to all the error-free attacks that we have seen in this paper, that is the PNS, BS and CBS. Inasmuch as Eve is forced to carry out the signal measurement before knowing the encoding basis, in the CBS attack she does not have to rely anymore on her ability to detect photons without disturbing their polarization (task *a)*). Eve can realize the conditional dynamics by directly measuring the extracted photons with photodetectors. Acknowledging the impracticability of indefinite qubit storing, thus, puts on equal footing the BS and CBS as far as technological difficulty is concerned, and still leaves the PNS as unfeasible.

As in the previous section, we can now calculate the performance of the CBS in this new no-storage or direct measurement scenario. In this situation the CBS is bound to fail in half of the cases. Eve only succeeds when she measures the extracted photon in the right basis. The probability of success and key fraction in the *directly measured conditional beam splitting* (DCBS) will accordantly be reduced by a factor $\frac{1}{2}$, i.e. $p_{\text{DCBS}}^{\text{succ}} = \frac{1}{2} p_{\text{CBS}}^{\text{succ}}$ and $f_{\text{DCBS}} = \frac{1}{2} f_{\text{CBS}}$. Clearly, since the number of extracted photons is the same as in the scenario with the possibility of storage, the number of non-vacuum signal that arrive at Bob's site remains the same.

The success probability for the directly measured beam splitting attack (DBS) can be calculated taking into account that Eve's attack is unsuccessful only in the case where all split photons from a signal are measured [21] in the wrong basis,

$$\begin{aligned} p_{\text{DBS}}^{\text{succ}} &= (1 - e^{-\eta\mu}) \left(1 - \sum_{n=0}^{\infty} \frac{1}{2^n} \frac{\mu^n (1-\eta)^n}{n!} e^{-\mu(1-\eta)} \right) \\ &= (1 - e^{-\eta\mu})(1 - e^{-\frac{\mu}{2}(1-\eta)}). \end{aligned} \tag{29}$$

The fraction of the key known by Eve in this attack is therefore,

$$f_{\text{DBS}} = 1 - e^{-\frac{\mu}{2}(1-\eta)}. \tag{30}$$

Since for small μ the most important contribution in the BS comes from the two photon signals, as in CBS, the success probability of both attacks is reduced approximately by the same factor $\frac{1}{2}$. But this factor is always a bit larger for DBS since in the cases where more than one photon per signal are split, Eve has a bigger chance to measure in the right basis. The performance quotient is now defined relatively to the DBS, $q_{\text{DCBS}} = \frac{f_{\text{DCBS}}}{f_{\text{DBS}}}$ and it is plotted in Fig. 4 for relevant values of μ and η. We see that for large mean photon numbers ($\mu > \ln 4 \approx 1.4$) the DBS can actually perform slightly better than the DCBS for some range of channel losses (see also Figs. 8 and 7).

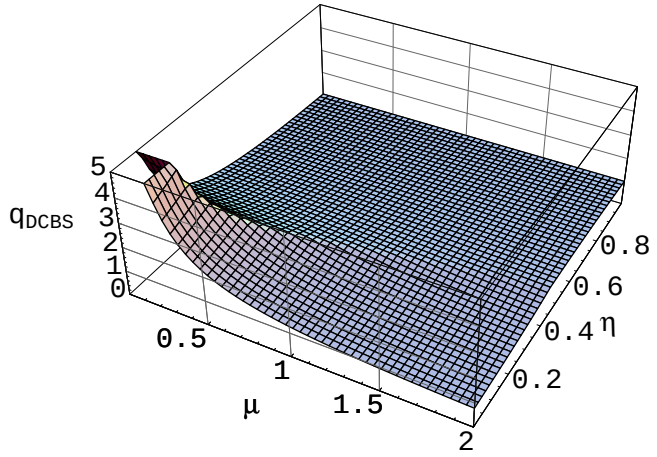

FIG. 4. Performance quotient q_{DCBS} for the DCBS . Since it is not bounded from above we have only plotted values smaller than five.

Despite this last remark it looks like the CBS maintains its efficiency over the BS under the no-storage constraint (compare Fig. 4 with Fig. 3), but in fact under this scenario the DCBS has lost the threatening feature of being able to extract the full key ($f_{\text{CBS}} = 1$) for high channel losses (see Fig. 8).

In the remaining of this section we will propose a variation of the CBS which allows Eve to extract the full key even in the no-storage scenario, and to perform better than DBS for any mean photon number. The idea of the adapted conditional beam splitting attack (ACBS) is to extract two photons, one by one, from the signal and measure each of them in a different polarization basis. In order to do that, Eve just has to follow the same protocol as in the single photon CBS but instead of stopping the beam splitting as soon as she detects one photon, she has to continue the splitting until a second photon is extracted. As previously, in order to match the expected number of photons in Bob's side, the splitting procedure can run for a maximum coupling time $\tilde{\tau}$ after which the signal must be transmitted to Bob through a lossless channel. Obviously, this attack will only be advantegeous in the no-storage scenario since otherwise, when the key can be extracted from the first photon, it is of no use to extract a second photon.

The total probability that Bob gets a vacuum signal after the ACBS is

$$\begin{aligned} P^{\text{B}}_{\text{ACBS}}[0] &= p_0(\tilde{\tau})p_c^0(\mu) + \int_0^{\tilde{\tau}} p_1(t_1) \\ &\left[\int_{t_1}^{\tilde{\tau}} p_{11}(t_2|t_1)p_c^0(\gamma_{t_2}^2\mu)dt_2 + p_{10}(\tilde{\tau}|t_1)p_c^0(\gamma_{\tilde{\tau}}^2\mu)\right] dt_1 \\ &= \mathrm{e}^{-\mu}(1+\mu(1-\gamma_{\tilde{\tau}}^2) + \frac{\mu^2}{2}(1-\gamma_{\tilde{\tau}}^2)^2), \end{aligned} \tag{31}$$

where $p_c^n(\mu)$ is the probability of having n photons in a coherent state with mean photon number μ, $p_{11}(t_2|t_1) = \epsilon^2\gamma_{t_2}^2\mu \mathrm{e}^{\mu(\gamma_{t_2}^2-\gamma_{t_1}^2)}$ is the probability of having a jump at t_2 conditional to a previous jump at t_1, and $p_{10}(\tilde{\tau}|t_1) = \mathrm{e}^{\mu(\gamma_{\tilde{\tau}}^2-\gamma_{t_1}^2)}$ is the probability of having no jump in the time interval $[t_1, \tilde{\tau}]$ conditional to a jump at t_1. These probabilities can be calculated following the general results in the beginning of Sec. II. The previous result is equal to the corresponding probability in CBS (Eq.18) plus a second order in μ term which represents the removal of two photons.

The coupling time $\tilde{\tau}$ can be now fixed so that Bob's probability of detecting at least one photon agrees with the result he would expect from the lossy channel,

$$P^{\text{B}}_{\text{ACBS}}[\neg 0] = P^{\text{B}}_{\eta}[\neg 0] \longrightarrow P^{\text{B}}_{\text{ACBS}}[0] = P^{\text{B}}_{\eta}[0] \tag{32}$$

$$\longrightarrow \gamma_{\tilde{\tau}}^2 = \mathrm{e}^{-\epsilon^2\tilde{\tau}} = 1 + \frac{1}{\mu}(1 - \sqrt{2\mathrm{e}^{\mu(1-\eta)} - 1}). \tag{33}$$

As expected we see that the maximum coupling time will be smaller for the ACBS than the CBS $\gamma_{\tau}^2 < \gamma_{\tilde{\tau}}^2 < \eta$.

To calculate the probability of success we have to count the events in which Eve extracts a signal while leaving some non-vacuum contribution to Bob. We also have to take into account that Eve only gets the bit value with certainty when she manages to extract two single photons, otherwise she will only get it in half of the cases. The success probability for the ACBS attack is then given by

$$\begin{aligned} p^{\text{succ}}_{\text{ACBS}} &= \int_0^{\tilde{\tau}} p_1(t_1) \left[\int_{t_1}^{\tilde{\tau}} p_{11}(t_2|t_1)p_c^{\neg 0}(\gamma_{t_2}^2\mu)dt_2 + \right. \\ &\left. + \frac{1}{2}p_{10}(\tilde{\tau}|t_1)p_c^{\neg 0}(\gamma_{\tilde{\tau}}^2\mu)\right] dt_1 = 1 - \mathrm{e}^{-\mu}\left[\mathrm{e}^{\gamma_{\tilde{\tau}}^2\mu} + \right. \\ &\left. + \frac{\mu}{2}(1-\gamma_{\tilde{\tau}}^2)(1+\mathrm{e}^{\gamma_{\tilde{\tau}}^2\mu}) + \frac{\mu^2}{2}(1-\gamma_{\tilde{\tau}}^2)^2\right], \end{aligned} \tag{34}$$

where $p_c^{\neg 0}(\mu)$ is the probability of having at least one photon in a coherent state with mean photon number μ.

By inverting Eq. (33) we find that the transmissivity 'mimicked' (in the sense of Eq. (32)) by the ACBS attack is

$$\eta_{\text{ACBS}} = 1 - \ln(1 + \mu(1 - \gamma_{\tilde{\tau}}^2) + \frac{\mu^2}{2}(1 - \gamma_{\tilde{\tau}}^2)^2). \qquad (35)$$

Since this is an increasing function of $\gamma_{\tilde{\tau}}^2$ we find the minimum transmissivity that can be mimicked by the ACBS without extra blocking (for $\tilde{\tau} \to \infty$) is

$$\eta_{\text{ACBS}}^{\min} = 1 - \frac{1}{\mu}\ln(1 + \mu + \frac{\mu^2}{2}) \approx \frac{1}{2}\mu^2 + O(\mu^3). \qquad (36)$$

In this limit of very high losses Eve can extract two excitations from all signals and still meet Bob's expectations. Therefore, by measuring each photon in a different basis, she will be able to acquire the full key even in the no-storage scenario ($f_{\text{ACBS}} = \frac{p_{\text{ACBS}}^{\text{succ}}}{P_{\text{ACBS}}^{\text{B}}[\neg 0]} = 1$). If the losses are still higher ($\eta \leq \eta_{\text{ACBS}}^{\min}$) Eve has to block some signals with probability

$$p_{\text{ACBS}}^{\text{block}} = \frac{1 - \mathrm{e}^{-\mu\eta}}{1 - \mathrm{e}^{-\mu\eta_{\text{ACBS}}^{\min}}}. \qquad (37)$$

The performance quotient is now $q_{\text{ACBS}} = \frac{f_{\text{ACBS}}}{f_{\text{DBS}}}$. In Fig. 5 we can see the values of this ratio as a function of the tranmissivity of the channel and the mean photon number. Notice that in this case the performance quotient is larger than unity for all values of the mean photon number, which means that the ACBS is more efficient than DBS. On the other hand, for low mean photon numbers ($\mu < 1$), higher losses are required to achieve the same performance as the DCBS (see also Figs. 7 and 8).

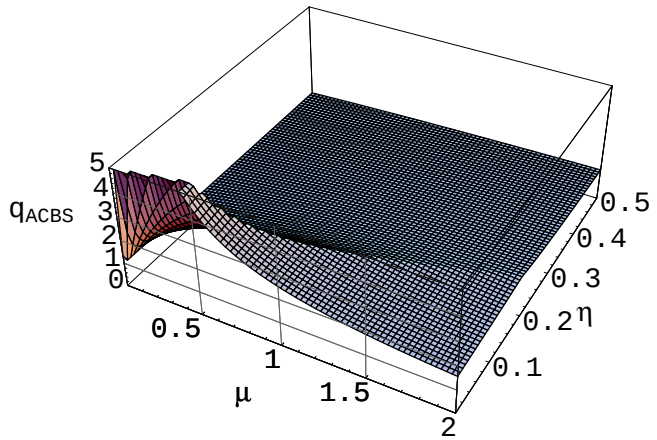

FIG. 5. Performance quotient q_{ACBS} for the ACBS.

We see that the ACBS can still be substantially better that the DBS. For the values $\mu = 0.1$ and $\eta = 0.1$ the ACBS attack provides Eve with a fraction of the key $q_{\text{ACBS}} = 1.3$ times bigger than the DBS attack. In Fig. 6 we can see the behavior of the performance quotient as a function of the mean photon number for a fixed value of the losses. We observe that, contrary to the other attacks, for a fixed transmissivity of the channel η, the efficiency of ACBS over DBS can increase with μ. For example, if the mean photon number of the previous example is increased to $\mu = 1.1$ keeping the transmissivity in $\eta = 0.1$ the efficiency factor grows to $q_{\text{ACBS}} = 2.48$.

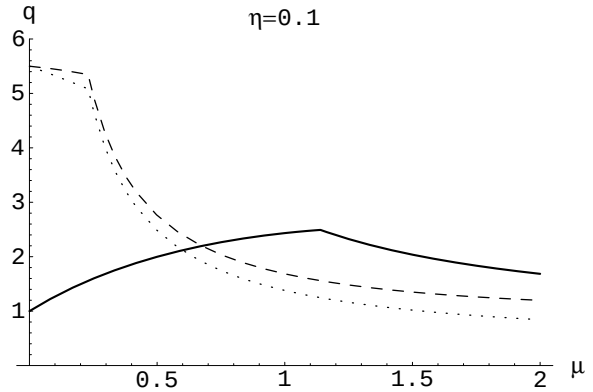

FIG. 6. Performance quotient at a fixed transmissivity $\eta = 0.1$ for the ACBS (solid), DCBS (dotted) and CBS (dashed).

In Fig. 7 we represent which of the studied attacks is most effective in the no-storage scenario for different values of the parameters μ and η. As a summary, in Fig. 8 we show the key fraction as a function of the losses for four different values of the mean photon and for the different attacks studied in this paper. For comparison, the results for the PNS in the storage and no-storage scenarios are also plotted. Once again, we notice that the CBS and ACBS provide real alternatives to the, at present, unfeasible PNS and the ineffective BS.

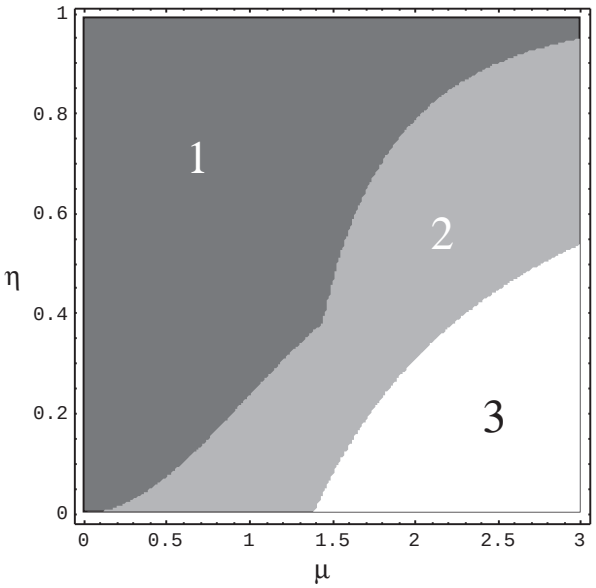

FIG. 7. Diagram of dominance of the different attacks under no-storing conditions: 1.$f_{\text{DCBS}} \geq f_{\text{ACBS}} \geq f_{\text{DBS}}$, 2.$f_{\text{ACBS}} \geq f_{\text{DCBS}} \geq f_{\text{DBS}}$ and 3.$f_{\text{ACBS}} \geq f_{\text{DBS}} \geq f_{\text{DCBS}}$

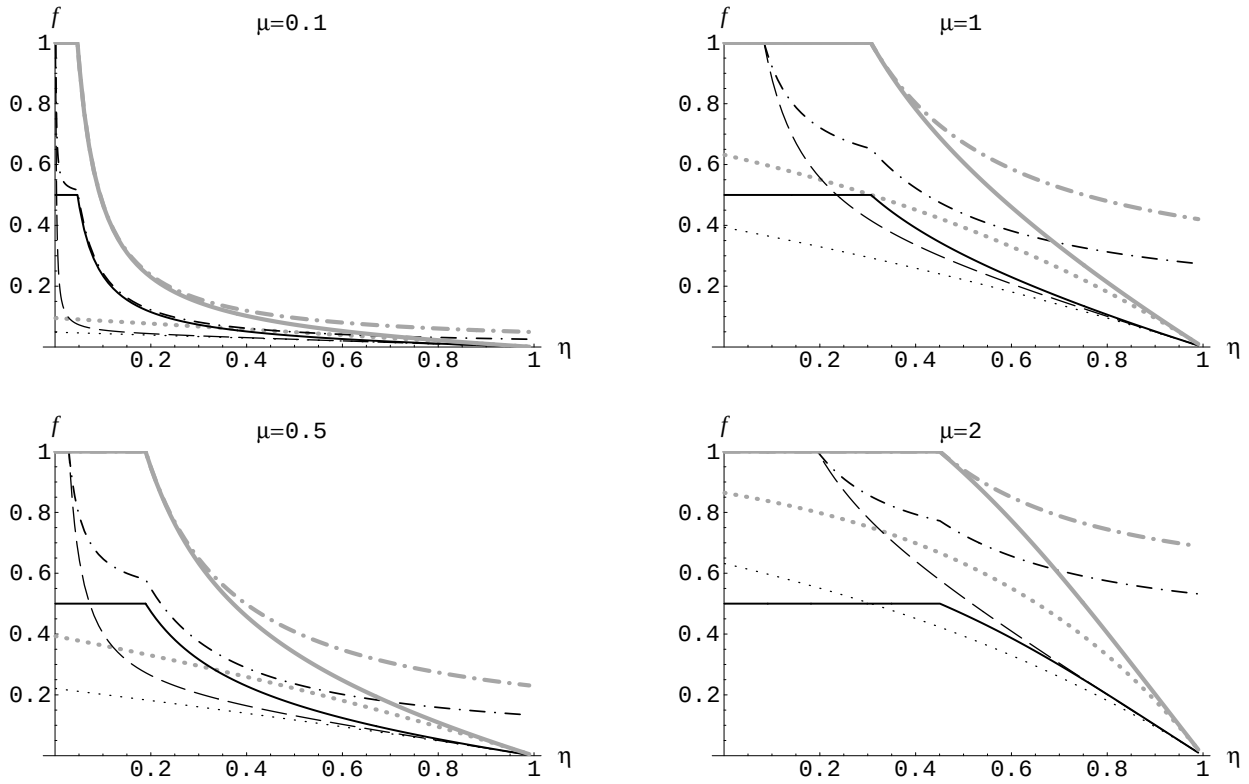

FIG. 8. Key fraction for different scenarios (Black: no-storage allowed, Gray: storage allowed) and attacks (Solid: CBS, Dashed: ACBS, Dotted: BS, Dot-dash: PNS).

IV. PHOTON STATISTICS

The task of an eavesdropper is to acquire knowledge about the secret key that Alice and Bob want to share. But the important point is that she does this without leaving any trace in the signal that could indicate her presence to Alice and Bob. Eve's eavesdropping capabilities are therefore strongly dependent on the capabilities of Alice and Bob to prepare and analyze their signals. In this work we have assumed that Alice is not able to prepare single photon signals, using instead very weak coherent states. Moreover, we have assumed that Bob's capabilities are limited as well by a detection setup that gives the same outcome for single photons than for multiphoton signals. In this situation Eve has only to forward signals to Bob in such a way that expected number of non-vacuum signals is the same as for the lossy channel, as expressed in Eq.(17).

In this section we will study what happens in the situations where Bob's capabilities are not so poor. In particular we consider the realistic situation in which Bob's analyzer is a polarizing beam splitter (in two possible orientations according to the basis measured) with a photon detector in each of its arms. We will assume that these detectors do not have photon number resolution, so that they only have two possible outcomes corresponding to non-vacuum ('click') and vacuum (no 'click') impinging signals.

When Bob and Alice bases coincide, only one of Bob's detectors can click and Eve remains safe. But in the case that Bob measures in a different basis than the encoding basis, the multiphoton part of the signal can lead to simultaneous clicks in both detectors. Here is where Eve can reveal her presence depending on what attack she chooses. Bob is expecting to receive a weak coherent state of a given amplitude (determined by the amplitude of the selected coherent state and by the channel losses) and therefore an expected number of these double clicks. The probability of these double clicks without Eve's intervention (or under the BS attack) is given by

$$p_{\rm BS}^{dc} = \frac{1}{2}(1-{\rm e}^{-\frac{\mu\eta}{2}})^2, \tag{38}$$

where the factor $\frac{1}{2}$ accounts for the probability that Alice and Bob use different basis.

When Eve tries to eavesdrop using the CBS attack without extra blocking (i.e $\eta > \eta_{\rm CBS}^{\rm min}$) the probability of double counts is,

$$\begin{aligned} p_{\rm CBS}^{dc} &= \frac{1}{2}p_0(\tau)(1-{\rm e}^{-\frac{\gamma_\tau\mu}{2}})^2 + \frac{1}{2}\int_0^\tau p_1(t)(1-{\rm e}^{-\frac{\gamma_t\mu}{2}})^2 dt \\ &= \frac{1}{2} - \frac{{\rm e}^{-\mu}}{2}(4{\rm e}^{\frac{\mu}{2}} - 1 - \mu(1-\gamma_\tau^2) - 2{\rm e}^{-\frac{\gamma_\tau^2\mu}{2}}). \end{aligned} \tag{39}$$

By using (19) to express γ_τ in terms of the the channel losses, and taking into account the blocking probability

$p^{\text{block}}_{\text{DCBS}}$ (24) for $\eta < \eta^{\min}_{\text{CBS}}$ we plot in Fig. 9 the ratio of both probabilities $q^{dc}_{\text{CBS}} = \frac{p^{dc}_{\text{CBS}}}{p^{dc}_{\text{BS}}}$ as a function of the mean photon number and channel transmissivity.

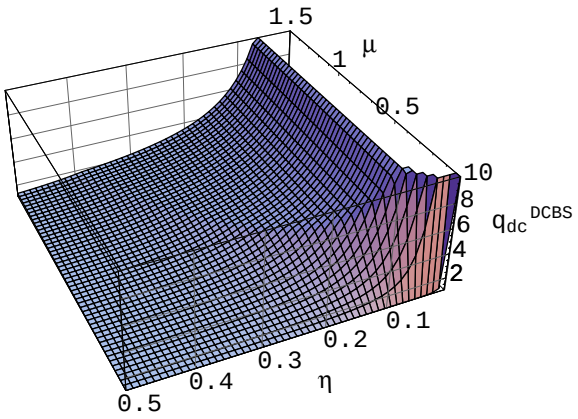

FIG. 9. Ratio of the CBS and BS double-click probabilities.

We see that the CBS increases the probability of double-clicks relative to the lossy channel. The reason for this increase is that the CBS only takes one photon out while several signal photons might be lost in the lossy channel. For increasing transmissivities the differences tend to vanish. So, for example $\mu = \{0.1, 0.01\}$ and $\eta = 0.3$ lead to $q_{dc} = \{1.1, 1.02\}$. But for higher losses the ratio can be quite high, e.g for $\mu = \{0.1, 0.01\}$ and $\eta = 0.1$ $q_{dc} = \{3.45, 1.2\}$. Inclusion of the effect of dark counts in Bob's detectors in p^{dc}_{CBS} shows only a slight reduction of the discrepancies for reasonable dark count probabilities ($p_{\text{D}} \sim 10^{-5}$). Even though this is a definite handicap of the CBS it might be of relative importance in practice. The probability of double counts is very small ($p^{dc} \sim \frac{1}{8}(\eta\mu)^2$) while the statistical fluctuations are large, therefore the number of transmitted signals needed to appreciate Eve's intervention might be exorbitant. As shown in Fig. 11, for some parameter regimes one can find a good compromise between the probability of success and the double-count rate.

Moreover, as we shall see next, the disparity in the number of double-clicks can be further decreased if Eve uses the two-photon splitting adopted for the non-storage conditions (ACBS). The double-click probability in this case is

$$p^{dc}_{\text{ACBS}} = 1 - \mathrm{e}^{-\mu}\left(8\mathrm{e}^{\frac{\mu}{2}} - 1 - \mu(1-\gamma_\tau^2) - \frac{1}{2}\mu^2(1-\gamma_\tau^2)^2 + \right.$$
$$\left. -2\mathrm{e}^{-\frac{\gamma_\tau^2\mu}{2}}(3+\mu(1-\gamma_\tau^2))\right). \quad (40)$$

In Fig. 10 we can see the ratio between this probability and the corresponding probability for the lossy channel $q^{dc}_{\text{ACBS}} = \frac{p^{dc}_{\text{ACBS}}}{p^{dc}_{\text{BS}}}$, taking into account the blocking for $\eta < \eta^{\min}_{\text{ACBS}}$. In Fig. 11 the same quantity is compared to the performance quotient.

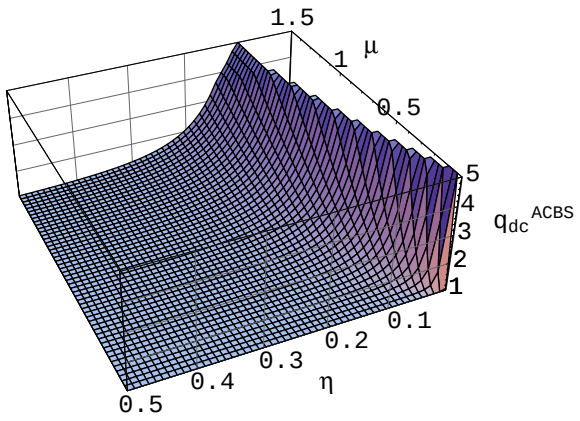

FIG. 10. Ratio of the ACBS and BS double-click probabilities.

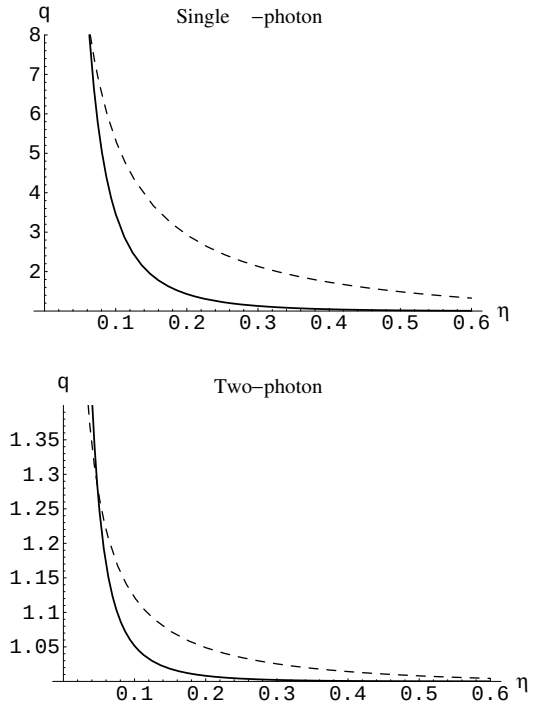

FIG. 11. Double-click ratio (solid) and performance quotient (Dashed) at a fix $\mu = 0.1$ for CBS and DCBS (top) and ACBS(bottom)

We see that for the ACBS attack the double click probability takes nearly the same values as for the lossy channel ($\mu = 0.1$ and $\eta = 0.1$ give $q_{dc} = 1.05$) while still providing larger key fractions than the BS attack.

V. MIXED STRATEGIES

In the previous sections Eve's attacks were characterized by only one parameter γ_τ. Once the type of attack

was chosen (CBS, ACBS) she could only vary the coupling time τ to tune her attack. In this section we will study the situation in which Eve can use mixed strategies, i.e. for each signal she can choose a different coupling time. In this way, Eve has the freedom to choose a probability distribution $\{p_i\}$ according to which she will apply a coupling time τ_i (i.e. γ_{τ_i}). A mixed strategy could in principle lead to a lowering of the double-click probability without sacrificing to much probability of success. Unfortunately we will see that this is not the case for the CBS and ACBS.

We start by considering the CBS attack. In this case the number of non-vacuum signals received by Bob (18) is linearly dependent on $\gamma^2_{\tau_i}$, therefore the mixed strategy has to be such that the average value of $\gamma^2_{\tau_i}$ is equal to the pure strategy value fixed in Eq. (19), i.e.

$$\begin{aligned}\bar{P}^{\rm B}_{\rm CBS}[0] &= \sum_i p_i P^{\rm B}_{\rm CBS}[0]_i \\ &= \sum_i p_i \mathrm{e}^{-\mu}(1+\mu(1-\gamma^2_{\tau_i})) = P^{\rm B}_{\rm CBS}[0] \qquad (41)\\ \longrightarrow \sum_i p_i \gamma^2_{\tau_i} &= \gamma^2_\tau. \qquad (42)\end{aligned}$$

Now we want to know what is the behavior of the probability of success and of the double-clicks when using mixed strategies. From Jensen's inequality [22] we know that

$$f''(x) \gtrless 0 \Longleftrightarrow \sum_i p_i f(x_i) \gtrless f(\sum_i p_i x_i). \qquad (43)$$

Since Eq. (42) assures that Bob gets the expected number of clicks we find, by using Eq. (21), that the mixed strategy always leads to a smaller probability of success than a pure one

$$\begin{aligned}\bar{p}^{\rm succ}_{\rm CBS} = \sum_i p_i p^{\rm succ}_{\rm CBS}(\gamma^2_{\tau_i}) \text{ and } \frac{d^2 p^{\rm succ}_{\rm CBS}}{d(\gamma^2_\tau)^2} < 0 \\ \Longleftrightarrow \bar{p}^{\rm succ}_{\rm CBS} < p^{\rm succ}_{\rm CBS}(\gamma^2_\tau). \qquad (44)\end{aligned}$$

Similarly one can easily see that the probability of double-clicks in the CBS $p^{dc}_{\rm CBS}$ (39) increases when mixing strategies. Since we already saw that the double-click probability is higher than for the lossy channel we arrive to the conclusion that using mixed strategies does not offer any advantages to the CBS attack.

The same happens in the two-photon conditional beam splitting (ACBS). To prove this, one has to write the probability of success and of double-clicks as a function of Bob's probability of receiving a non-vacuum signal, and check for its concavity/covexity.

VI. CBS WITH FINITE BEAM SPLITTERS

In this section we will see how to implement the CBS attack with finite reflectivity beam splitters. The beam splitters have now a finite reflectivity $|r|^2$ (and transmissivity $|t|^2 = 1-|r|^2$). Without any loss of generality we will assume that r and t for the signal are real. We also assume that they are independent of polarization.

The initial state can be written as $|\phi_0\rangle = |\alpha;\beta\rangle\,|0;0\rangle$ where the first ket is Alice's coherent state and the second is Eve's mode. After the first beam splitter the state of the system is

$$|\phi_1\rangle = |t\alpha;t\beta\rangle\,|r\alpha;r\beta\rangle\,. \qquad (45)$$

Notice that Eve's and the signal modes are still in a separable state. This means that Bob's state will be the same independently of what Eve does to her modes. For coherent input states, Bob's state will depend only on the number of beam splitters put in by Eve during the attack. Eqs.(13) and (15) reflect this situation in the infinitesimal beam splitting case. This simplified the calculations leading to the results in this paper, but the quantum jump method described in Sec. II can be used to describe the conditional beam splitting for any kind of input as long as Eve's modes are in the vacuum state initially [1].

After the first beam splitter Eve will try to detect the presence of photons in her modes. With probability $p^0_1 = p^0_c(r^2(|\alpha|^2+|\beta|^2)) = \mathrm{e}^{-\mu r^2}$ she will detect no photon. If this happens she will split the signal with a second beam splitter. She will repeat this process until she detects some photons in her modes. After the m^{th} beamsplitting the state of the system is

$$|\phi_m\rangle = |t^m\alpha;t^m\beta\rangle\,\left|rt^{m-1}\alpha;rt^{m-1}\beta\right\rangle\,. \qquad (46)$$

To keep the notation simple, we are omitting here the tested vaccum modes of earlier beam splitters. The total probability of reaching this state is,

$$\begin{aligned}p_m = \prod_{i=1}^{m-1} p^0_c(\mu r^2 t^{2(m-1)}) = \prod_{i=1}^{m-1} \mathrm{e}^{-\mu r^2 t^{2(i-1)}} = \\ = \mathrm{e}^{-\mu r^2 \sum_{i=1}^{m-1} t^{2(i-1)}} = \mathrm{e}^{-\mu(1-t^{2(m-1)})}. \qquad (47)\end{aligned}$$

Therefore the total probability that Eve detects some signal after the m^{th} beam splitter is

$$\begin{aligned}p^{\neg 0}_m &= p_m p^{\neg 0}_c(\mu r^2 t^{2(m-1)}) \\ &= \mathrm{e}^{-\mu(1-t^{2(m-1)})}(1-\mathrm{e}^{-\mu r^2 t^{2(m-1)}}). \qquad (48)\end{aligned}$$

If this event occurs, the splitting stops and the signal is sent to Bob through the lossless channel. Otherwise Eve keeps on adding beam splitters until she reaches a maximum number N of attempts. After the conditional beam splitting attack with finite beam splitters (CBSF), Bob will therefore receive a coherent state $\left|\phi^{bob}_m\right\rangle = |t^m\alpha\rangle$ with probability $p^{\neg 0}_m$ for $m = 1\ldots N-1$ or p_N for $m = N$. From here one can calculate the probability of vacuum signals arriving at Bob's site in the CBSF

$$P^{\rm B}_{\rm CBSF}[0] = p_N p^0_c(\mu t^{2N}) + \sum_{m=1}^{N-1} p^{\neg 0}_m p^0_c(\mu t^{2m})$$
$$= {\rm e}^{-\mu}\left(1 - N + \sum_{n=0}^{N-1} {\rm e}^{\mu r^2 t^{2n}}\right). \qquad (49)$$

The probability of success of the CBSF attack is,

$$p^{\rm succ}_{\rm CBSF} = \sum_{m=1}^{N} p^{\neg 0}_m p^{\neg 0}_c(\mu t^{2m}) = \sum_{m=1}^{N} p_m(1 - {\rm e}^{-\mu t^{2m}})$$
$$= 1 + {\rm e}^{-\mu}\left(N - {\rm e}^{\mu t^{2N}} - \sum_{n=0}^{N-1} {\rm e}^{\mu r^2 t^{2n}}\right) \qquad (50)$$

Notice that Eqs. (48) and (47) and the derived quantities are in agreement up to first order in r^2 with the corresponding probabilities for the infinitesimal CBS derived with the quantum jump method, i.e. Eqs. (14) and (16) (with $r^2 = \frac{\tau}{N}\epsilon^2$).

In order to match Bob's probability of detecting a non-vacuum signal with the result he would expect from the lossy channel, Eve has now two free parameters: the maximum number N of beam splitters used and their transmission amplitude t. From the infinitesimal CBS results we know that for small reflection coefficients (i.e. $t \sim 1$), $t^{2N} \approx \gamma^2_\tau$ taking γ^2_τ from Eq. (19). Of course, for a finite N this approximation will not hold when we are in or near the region $\eta < \eta^{\rm min}_{\rm CBS}$ which corresponds to $\tau \to \infty$. The reason for this is that now we are dealing with finite beam splitters and accordingly, for any given N, we can 'mimic' a lossy channel with arbitrarily high losses. For the same reason now we are not forced to block any signals as done for the CBS in the high losses regime.

To get the quantitative results presented in the rest of this section we have to find numerically the condition on Eve's free parameters (t and N) such that Bob's expectations on the number of non-vacuum signals are fulfilled. For a given N we use Newton's method to find the value of t for which $P^{\rm B}_{\rm CBSF}[0]$ (49) equals to $P^{\rm B}_{\eta}[0]$ (12), taking a starting value of $t_o = \eta^{\frac{1}{2N}}$.

In Fig. 12 and 13 we have plotted the performance quotient $q_{\rm CBSF} = \frac{f_{\rm CBSF}}{f_{\rm BS}}$ as a function of μ and η for an attack using a maximum of two and ten beams splitters respectively.

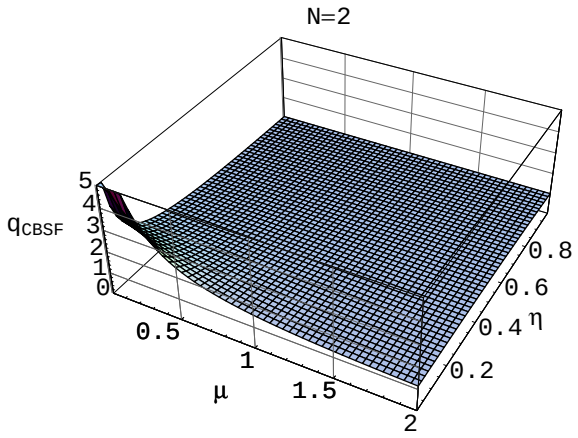

FIG. 12. Ratio between the CBSF with two beam splitters and the BS success probabilities.

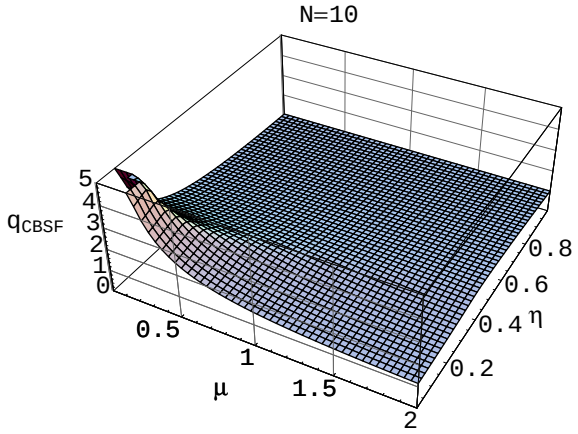

FIG. 13. Ratio between the CBSF with ten beam splitters and the BS success probabilities.

We notice that doing CBSF with only two beam splitters, Eve already obtains a much bigger fraction of the key than with the standard beamsplitting attack, e.g for $\mu = 0.1$ and $\eta = 0.1$ the key she obtains is $q^{N=2}_{\rm CBSF} = 2.5$ times longer. With ten beam splitters she almost reaches the infinitesimal result (compare with Fig. 3). For $\mu = 0.1$ and $\eta = 0.1$ the key she obtains is $q^{N=10}_{\rm CBSF} = 4.7$ times longer.

In Fig. 14 we can compare the key fraction obtained with the BS, CBS and CBSF with different numbers of beam splitters.

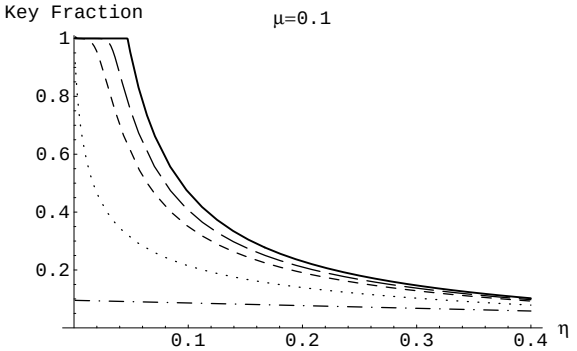

FIG. 14. Key fraction for CBS (solid), CBSF with N=2 (Dotted), N=5 (Short-dashed), N=10 (Long-dashed) and BS (Dash-dotted).

The number of double-clicks in Bob's detectors when he measures in the wrong basis can be calculated from

$$p^{dc}_{\mathrm{CBSF}} = p_N p_c^{\neg 0}(\frac{1}{2}\mu t^{2N})^2 + \sum_{m=1}^{N-1} p_m^{\neg 0} p_c^{\neg 0}(\frac{1}{2}\mu t^{2m})^2. \quad (51)$$

The ratio between the double-click probabilities of the BS and CBSF for various values of N, is plotted Fig. 11 together with the corresponding performance quotients. This figure shows that, depending on the parameter regime, an attack with a small number of finite beam splitters might be more suitable than the infinitesimal CBS in that the number of double clicks is much closer to its lossy channel values.

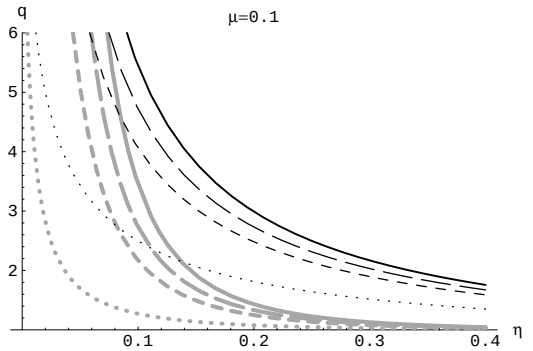

FIG. 15. Quality factors (black) and double-click ratio (Gray) for CBS (solid), CBSF with N=2 (Dotted), N=5 (Short-dashed), N=10 (Long-dashed).

VII. CONCLUSION

In this paper we have introduced a novel attack on weak coherent pulse quantum key distribution in lossy channels. The conditional beam splitting takes advantage of the multiphoton component of the transmitted signals to extract information on the encoded bit. This task is accomplished optimally using the photon number splitting attack. However, the implementation of the PNS attack entails a quantum non demolition measurement which is something unattainable, at least at the single photon level, with the current technology. Until now the technologically possible alternative to the PNS has been the simple beam splitting attack [23]. For high losses (i.e. long transmission distances) the BS attack turns out to be very ineffective. Here we have presented the conditional beam splitting attack which also requires only linear optical elements and is therefore feasible with present technology, but is much more efficient than the conventional beam splitting attack. The CBS attack, thus, shortens substantially the gap in performance between the ideal and practical eavesdropping attacks. This is of great importance if one considers that the eavesdroppers success in a quantum key distribution attack is dictated by the technology at the moment of the signal transmission. In contrast with the case of classical cryptographic protocols, no future technologies can help unveil present key exchanges.

Starting from the simplest scenario in which Eve is capable of storing her signals until the encoding basis is announced, we have moved to more realistic situation in which Eve has no storing capabilities. For this situation an adapted CBS attack, based on the extraction of two single photons, has been proven to be advantageous for some relevant parameter regimes.

Numerical results for the implementation of CBS with finite reflectivity beam splitters show that using only two beam splitters one can easily duplicate the efficiency of the conventional beam splitting, and that the infinitessimal CBS results are reached with the use of a few beam splitters.

The photon statistics at Bob's detectors has been studied and shown to be a matter of concern in this type of attack. However, we argue that, if handled with care, this drawback does not disqualify the CBS attacks. We believe that further elaborations of this basic idea can lead to attacks which are specialized for certain parameter regimes and other protocols.

ACKNOWLEDGEMENTS

S. M. B. thanks the Royal Society of Edinburgh and the Scottish Executive Education and Lifelong Learning Department for financial support. J.C. acknowledges the Academy of Finland (project 4336) and the European Union IST EQUIP Programme for financial support.

[1] J. Calsamiglia, S.M. Barnett, N. Lütkenhaus and K-A. Suominen, Phys. Rev. A (in press), and quant-ph/0106086.
[2] G. S. Vernam, Journal of the American Institute of Electrical Engineers **45**, 109 (1926).
[3] S. Wiesner, Sigact News **15**, 78 (1983).

[4] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[5] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[6] D. Mayers, Unconditional security in quantum cryptography, Journal of ACM, 2001 (to appear); also available as quant-ph/9802025.
[7] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[8] E. Biham *et al.*, in *Proceedings of the Thirty Second Annual ACM Symposium on Theory of Computing, New York, USA* (ACM, New York, 2000), pp. 715–724. and quant-ph/9912053
[9] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[10] C. H. Bennett *et al.*, J. Cryptology **5**, 3 (1992).
[11] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[12] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[13] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
[14] H. Inamori, N. Lütkenhaus, and D. Mayers, quant-ph/0107017.
[15] Naturally, this requires Eve to be able to perform a QND measurement in order to determine the presence of a single photon without absorbing it. This is not realistic with current technology. Allowing Eve to do this, however, serves to demonstrate the full potential of the CBS attack.
[16] K. Mølmer, Y. Castin and J. Dalibard, J. Opt. Soc. Am. B. **10**, 524 (1993)
[17] M. B. Plenio and P.L. Knight, Rev. Mod. Phys. **70** 101 (1998).
[18] H. Carmichael *An open systems approach to quantum optics* (Springer-Verlag, Berlin, 1993).
[19] S. M. Barnett and P. M. Radmore, *Methods in theoretical quantum optics* (Oxford University Press, Oxford, England, 1997) p. 236.
[20] For simplicity we will not consider in this paper the effects of any imperfections in the channel used by Eve to send the photons to Bob. In any case it is reasonable to assume that Eve can provide a channel with lower losses than the one used by Alice and Bob. The effect of considering Eve's losses is equivalent to the effect of Bob's detector efficiency.
[21] Eve can use a cascade of beams splitters in order to distribute the photons she receives so that the probability of having two photon detections is infinitesimally small.
[22] See e.g. W. P. Ziemer, *Weakly differentiable functions: Sobolev spaces and functions of bounded variation* (Springer, New York, 1989).
[23] Other technlogically possible alternatives become available if quantum bit errors are present. See e.g. S. Félix, N. Gisin, A. Stefanov and H. Zbinden, quant-ph/0106086.