Unambiguous state discrimination in quantum cryptography with weak coherent states

Miloslav Dušek,[1] Mika Jahma,[2] and Norbert Lütkenhaus[2]
[1]*Department of Optics, Palacký University, 17. listopadu 50, 772 00 Olomouc, Czech Republic*
[2]*Helsinki Institute of Physics, P.O. Box 9, 00014 Helsingin Yliopisto, Finland*
(Received 20 March 2000; published 13 July 2000)

The use of linearly independent signal states in realistic implementations of quantum key distribution (QKD) enables an eavesdropper to perform unambiguous state discrimination. We explore quantitatively the limits for secure QKD imposed by this fact taking into account that the receiver can monitor, to some extent the photon-number statistics of the signals even with todays standard detection schemes. We compare our attack to the beam-splitting attack and show that security against the beam-splitting attack does not necessarily imply security against the attack considered here.

PACS number(s): 03.67.Dd, 03.65.Bz, 42.79.Sz

I. INTRODUCTION

Quantum key distribution (QKD) is a technique to provide two parties with a secure, secret, and shared key. Such a key is the necessary ingredient in the only *provably* secure way to communicate with guaranteed privacy, the one-time pad or Vernam cipher [1]. The first complete protocol was given by Bennett and Brassard [2] (BB84) following ideas by Wiesner [3]. It uses the fact that any channel that transmits two nonorthogonal states perfectly automatically makes eavesdropping on this channel detectable.

We consider the BB84 protocol in a typical quantum optical implementation. Ideally, Alice sends a sequence of single photons that are at random polarized in one of the following four states: right or left circular polarization, or vertically or horizontally polarization. Bob chooses at random between two polarization analyzers, one distinguishing the circular polarized states, and the other distinguishing the linear polarized states. Following a public discussion about the basis of the sent signals and the measurement apparatus applied to them, sender and receiver can obtain a shared key made up from those signals where the measurement device gives deterministic results. This is the *sifted key* [4]. Proofs of security of this scheme against the most general attack, even in the presence of noise, have been obtained [5–7]. In this paper we follow another goal: we would like to illuminate to what extent very simple attacks can render QKD impossible once realistic imperfections like lossy lines and nonideal signal states are taken into account. The difficulties implied, for example, by the use of weak coherent states in combination with lossy lines has been pointed out earlier [8–10] and this subject has been illuminated in depth in Ref. [11], where bounds on coverable distances are given. Positive security proofs for sufficiently short distances, taking into account the realistic signals are given for individual attacks [12] and coherent attacks [13]. The eavesdropping attacks that crack the secrecy of the key for setups exceeding these secure distances are still quite complicated. The eavesdropper needs to perform a quantum nondemolition (QND) measurement on the total photon number of the signal, then he has to split a photon off the occurring multiphoton signals [11], store that photon, and then, finally, measure it after the public discussion.

In this paper we are looking into much simpler eavesdropping strategies that make use of the opportunities arising from lossy lines and nonideal signals. Such an attack has been proposed by Bennett [14] and Yuen [9]. It uses the fact that Eve can, with finite probability, discriminate the four signal states unambiguously. Whenever such a discrimination is performed successfully, the eavesdropper knows immediately which of the four signal states was sent and can send this information, via a classical channel, to Bob's detector, in front of which she places a state preparation machine to prepare the identified state. This way this state does not experience the losses of the actual quantum channel, without which Eve has to invest into a perfect quantum channel.

The investigation of this scenario refines Bennett's and Yuen's analysis since it takes into account that, to a certain extent, the photon statistics of the signals arriving at Bob's detectors can be monitored. The results illuminate the restrictions placed on implementations of QKD on lines with strong losses. Thereby we can show that the currently widely used conditional security standard of security against beam-splitting attacks [14] is incomplete. Especially, contrary to common belief, the use of unambiguous state discrimination can be a more efficient eavesdropping strategy than the beam-splitting attack, even for dim coherent states.

This paper is organized as follows. In Sec. II we recapitulate the principles of unambiguous state discrimination. These are applied in Sec. III to the signal states in the BB84 protocol with dim coherent signal states. In Sec. IV we introduce an eavesdropping attack based on unambiguous state discrimination (USD attack) and analyze it in detail, taking the photon number distribution of the signals arriving at Bob's detectors into account. In Sec. V we discuss the relation between the beam-splitting attack and the USD attack. Section VI concludes the article with a short summary.

II. UNAMBIGUOUS DISCRIMINATION OF SIGNAL STATES

Unambiguous state discrimination is possible whenever the N states in question are linearly independent. The problem can be described by a measurement that can give the results ''state 0,'' ''state 1,'' . . . ,''state $N-1$,'' and the result ''do not know.'' The constraint is that the measurement

results should never wrongly identify a state, and the goal is to keep the fraction of ''do not know'' results as low as possible. This problem has been investigated by Ivanovic [15] for the case of two equally probable nonorthogonal states. Peres [16] solved this problem in a formulation with probability operator measures. Later Jaeger and Shimony [17] extended the solution to arbitrary *a priori* probabilities. Peres's solution has been generalized to an arbitrary number of equally probable states that are generated from each other by a symmetry operator by Chefles and Barnett [18]. Their result can be summarized as follows: the symmetry allows one to write the input states in the form

$$|\Psi_k\rangle = \sum_{j=0}^{N-1} c_j \exp\left(2\pi i \frac{kj}{N}\right) |\phi_j\rangle, \tag{1}$$

where the states $|\phi_j\rangle$ represent some set of orthonormal states. Note that the states

$$|\tilde{\Psi}_l\rangle = \frac{1}{\sqrt{N}} \sum_{j=0}^{N-1} \exp\left(2\pi i \frac{lj}{N}\right) |\phi_j\rangle$$

form another orthonormal set. It turns out that the optimal strategy for unambiguous state discrimination consists of two steps. In the first step a filter operation is performed such that the output states are either the orthonormal states $|\tilde{\Psi}_l\rangle$ or some linear dependent states. This step can be described by a complete positive map with the two Kraus operators. They are defined with the help of the minimum coefficient $c_{\min} = \min_j |c_j|$ as

$$A_{\text{yes}} = \sum_{j=0}^{N-1} \frac{c_{\min}}{c_j} |\phi_j\rangle\langle\phi_j|, \tag{2}$$

$$A_{\text{no}} = \sum_{j=0}^{N-1} \sqrt{1-(c_{\min}^2/|c_j|^2)}\, |\phi_j\rangle\langle\phi_j|. \tag{3}$$

The conditional state in the event of successful filtering is now given as

$$|\Psi_k^{(\text{yes})}\rangle = \sqrt{N} c_{\min} |\tilde{\Psi}_k\rangle .$$

In a second step, we can perform a von Neumann projection measurement on this state to identify unambiguously the state k via the orthonormal state $|\tilde{\Psi}_k\rangle$. The probability of this successful identification is given by

$$P_D = N \min_j |c_j|^2. \tag{4}$$

For the case of two equal probable nonorthogonal polarization states of a single photon a quantum optical implementation following this two-step idea has been given by Huttner *et al.* [19] and by Brandt [20].

III. SIGNAL STATES

A first description of realistic signal states is that of a coherent state with a small amplitude α. This corresponds to the description of a dimmed laser pulse. The coherent state is given by

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{(\alpha a^\dagger)^n}{n!} |0\rangle, \tag{5}$$

where $a^\dagger$ is the creation operator for one of the four BB84 polarizations that can be expressed in terms of two creation operators $b_1^\dagger$ and $b_2^\dagger$ (corresponding, e.g., to two linear orthogonal polarizations) as

$$a_0^\dagger = \frac{1}{\sqrt{2}}(b_1^\dagger + b_2^\dagger), \tag{6}$$

$$a_1^\dagger = \frac{1}{\sqrt{2}}(b_1^\dagger + i b_2^\dagger), \tag{7}$$

$$a_2^\dagger = \frac{1}{\sqrt{2}}(b_1^\dagger - b_2^\dagger), \tag{8}$$

$$a_3^\dagger = \frac{1}{\sqrt{2}}(b_1^\dagger - i b_2^\dagger). \tag{9}$$

In terms of these two modes the signal states become therefore

$$|\Psi_0\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \left|\frac{\alpha}{\sqrt{2}}\right\rangle, \tag{10}$$

$$|\Psi_1\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \left|i\frac{\alpha}{\sqrt{2}}\right\rangle, \tag{11}$$

$$|\Psi_2\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \left|-\frac{\alpha}{\sqrt{2}}\right\rangle, \tag{12}$$

$$|\Psi_3\rangle = \left|\frac{\alpha}{\sqrt{2}}\right\rangle \left|-i\frac{\alpha}{\sqrt{2}}\right\rangle. \tag{13}$$

We can calculate the values of the c_j in terms of the overlaps of the four states according to the formula [18]

$$|c_j| = \frac{1}{N^2} \sum_{k,l} \exp\left[-\frac{2\pi i j(k-l)}{N}\right] \langle\Psi_k|\Psi_l\rangle$$

and find as a function of the expected photon number $\mu = |\alpha|^2$:

$$|c_0| = \frac{1}{\sqrt{2}} e^{-\mu/4} \sqrt{\cosh\frac{\mu}{2} + \cos\frac{\mu}{2}}, \tag{14}$$

$$|c_1| = \frac{1}{\sqrt{2}} e^{-\mu/4} \sqrt{\sinh\frac{\mu}{2} + \sin\frac{\mu}{2}}, \tag{15}$$

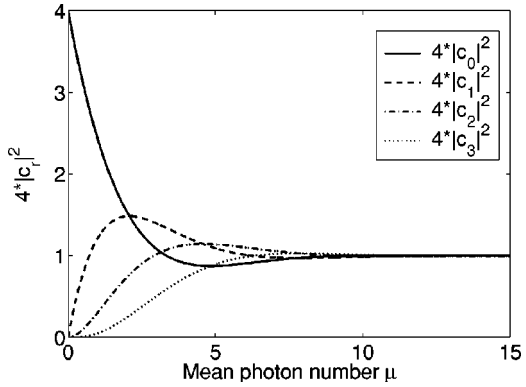

FIG. 1. The fourfold weight $4|c_j|^2$ of the four canonical states $|\phi_j\rangle$ as a function of the mean photon number μ. The lower bound of these four curves gives the optimum probability for unambiguous state discrimination.

$$|c_2| = \frac{1}{\sqrt{2}} e^{-\mu/4} \sqrt{\cosh\frac{\mu}{2} - \cos\frac{\mu}{2}}, \tag{16}$$

$$|c_3| = \frac{1}{\sqrt{2}} e^{-\mu/4} \sqrt{\sinh\frac{\mu}{2} - \sin\frac{\mu}{2}}. \tag{17}$$

The minimum of these four functions depends on the value of μ. The four functions $4|c_k|^2$ are plotted in Fig. 1 from where we can read off P_D as the minimum.

It turns out, however, that for realistic sources these states are not the correct description of the situation. The reason is that Eve does not have a phase reference, which means that for a given polarization she does not see the coherent state $|\alpha\rangle$ but the phase averaged density matrix

$$\frac{1}{2\pi}\int_{\phi} |e^{i\phi}\alpha\rangle\langle e^{i\phi}\alpha| d\phi.$$

This results in signal states that are mixtures of Fock states with a Poissonian photon-number distribution described by the density matrix

$$\rho = e^{-\mu}\sum_n \frac{\mu^n}{n!}|n\rangle\langle n|. \tag{18}$$

Here the state $|n\rangle$ denotes the Fock state with n photons in one of the four BB84 polarization states. The optimal strategy to discriminate between the four possible density matrices can be logically decomposed into a QND measurement on the total photon number in the modes b_1 and b_2 together and a following measurement that unambiguously discriminates between the four resulting conditional states for each total photon number. The justification for this is that the total photon number via the QND measurement ''comes free,'' since the execution of this measurement does not change the signal states. However, given the resulting information, we know the optimal strategy on the conditional states according to [18]. Therefore we find that the total probability of unambiguous state discrimination P_D is given in terms of the respective probabilities for each photon number subspace $P_D^{(n)}$ as

$$P_D = \sum_{n=0}^{\infty} e^{-\mu}\frac{\mu^n}{n!} P_D^{(n)}. \tag{19}$$

The conditional states resulting from the QND measurement and corresponding to n photons in total satisfy again the symmetry condition that allows to apply the results by Chefles and Barnett. We find for the four coefficients (as a function of the photon number $n>0$) the expressions

$$|c_0| = \sqrt{\frac{1}{4} + 2^{-(1+n/2)}\cos\left(\frac{\pi}{4}n\right)}, \tag{20}$$

$$|c_1| = \sqrt{\frac{1}{4} + 2^{-(1+n/2)}\sin\left(\frac{\pi}{4}n\right)}, \tag{21}$$

$$|c_2| = \sqrt{\frac{1}{4} - 2^{-(1+n/2)}\cos\left(\frac{\pi}{4}n\right)}, \tag{22}$$

$$|c_3| = \sqrt{\frac{1}{4} - 2^{-(1+n/2)}\sin\left(\frac{\pi}{4}n\right)}. \tag{23}$$

Therefore the maximum probability of unambiguous state discrimination for a fixed value of n is given by

$$P_D^{(n)} = \begin{cases} 0 & n \leqslant 2 \\ 1 - 2^{1-n/2} & n \text{ even} \\ 1 - 2^{(1-n)/2} & n \text{ odd.} \end{cases} \tag{24}$$

It is possible to sum up the contributions from different photon numbers from the Poissonian distribution and we obtain the expression

$$P_D = \sum_{n=0}^{\infty} e^{-\mu}\frac{\mu^n}{n!} P_D^{(n)}$$
$$= 1 - e^{-\mu}\left(\sqrt{2}\sinh\frac{\mu}{\sqrt{2}} + 2\cosh\frac{\mu}{\sqrt{2}} - 1\right). \tag{25}$$

This result is compared to the result for coherent states in Fig. 2. As expected, the probability for unambiguous state identification is lower for the mixture of Fock states than for the coherent states. An expansion in terms of the photon number μ gives $P_D = \frac{1}{12}\mu^3 + O(\mu^4)$ for both situations. For lower than third order the signal states are not linearly independent, so that no unambiguous state discrimination is possible. Note that an actual implementation does not necessarily need to follow the decomposition into a QND and another measurement. We just need to implement one generalized measurement. Actually, Bennett *et al.* [14] and Yuen [9] gave a simple beam-splitter setup that obtains a discrimination probability of $P_D = \frac{1}{32}\mu^3 + O(\mu^4)$.

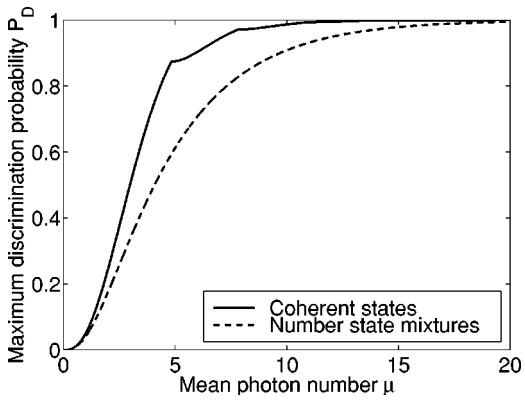

FIG. 2. Comparison of the optimum probability of unambiguous states discrimination for coherent states and for the corresponding mixture of Fock states. Both have the same Poissonian photon-number distribution with mean photon number μ.

IV. UNAMBIGUOUS STATE DISCRIMINATION AS EAVESDROPPING STRATEGY

We now consider the realistic situation that Alice uses the phase-averaged coherent states as signal states that are described by a Poissonian photon-number distribution with mean photon number μ. In this scenario we fix our eavesdropping strategy, to which we refer to as the *unambiguous state discrimination attack* (USD attack) as follows: The unambiguous state discrimination allows Eve to identify a fraction of the signals without error. For this fraction, she can prepare a corresponding state close to Bob's detectors such that no errors appear for these signals. Whenever the identification does not succeed, she sends the vacuum signal to Bob to avoid errors, which therefore will not be relevant in the considered scenario.

We need to study this strategy under realistic constraint. An important constraint is that the transmittance of the quantum channel connecting both parties is given by the transmission efficiency η_L. We consider a detection setup where Bob monitors each polarization mode in the chosen basis by one detector. These detectors have a finite detection efficiency η_B, in which we include any additional loss on Bob's side, e.g., from a polarizing beam splitter. The detectors are modeled as ''yes/no'' detectors, which either fire, or they do not fire; they cannot distinguish the number of impinging photons.

It is clear that once Eve identifies a signal she is interested to produce a signal in the corresponding polarization such that Bob will detect it despite his inefficient detectors. One strategy is to send a stronger signal than the original one in the correct polarization. This will work as long as Bob measures in the polarization basis, which includes the signal polarization (sifted key), but it will lead to an increased coincidence rate of clicks in both of Bob's detectors otherwise. Our analysis extends the previous analysis to include the additional constraint put on the eavesdropping strategy by the fact that Bob observes not only the rate of clicks of one or the other detector, but also the rate of events when both detectors fire, each monitoring one of the orthogonal polarization modes. The latter event will be observed ideally only when Alice and Bob use different bases, independently of the presence or absence of an eavesdropper. Eve's aim is to reproduce these two observables with the minimum number of nonvacuum signals to make efficient use of the successfully identified signals.

In the absence of Eve, whenever Alice and Bob use the same polarization basis, Bob's expects to find at most one detector clicks; the probability of a click is

$$\overline{P}_1 = 1 - \exp(-\eta_L \eta_B \mu), \tag{26}$$

as follows from the Poissonian photon-number statistics of coherent states.

Whenever Alice and Bob use different bases, a double click may occur; its probability is

$$\overline{P}_2 = \left[1 - \exp\left(-\frac{\eta_L \eta_B \mu}{2}\right)\right]^2. \tag{27}$$

What happens in the presence of Eve depends on the signals Eve sends for the successfully detected Alice's signals. It is clear that Eve can avoid the occurrence of double clicks when Alice and Bob measure in the same basis, since she unambiguously determined the signal. Therefore it is not useful to monitor the double-click rate when Alice and Bob use the same basis.

Note that we do not need to include detector dark count rates or take errors due to misalignment into account. The reason for that is that we will investigate the limit when the USD attack gives complete information to Eve while it reproduces the expected probabilities $\overline{P}_1$ and $\overline{P}_2$. The values of these probabilities in the absence of an eavesdropper and the reproduced values resulting from a successful USD attack will be affected in the same way by the error mechanisms of dark counts and misalignment, etc., so that the resulting real observed rates will still be indistinguishable.

A. Eve sends n-photon states

Let us suppose now, that whenever Eve succeeds in the unambiguous state discrimination she sends a number state (with correct polarization) containing N photons to Bob. If she fails she simply sends no photon.

If Alice and Bob use the same basis, at most one of two Bob's detectors will click. The probability of this event is given by

$$P_1^{(N)} = P_D\left[1 - \binom{m}{0} \eta_B^0 (1-\eta_B)^N\right] = P_D[1-(1-\eta_B)^N]. \tag{28}$$

This is the probability that one detector clicks if a state $|N\rangle$ comes, multiplied by the probability that Eve succeeds in USD (and sends $|N\rangle$).

If Alice and Bob use different bases, we can think of the photons as being equally and independently distributed to both Bob's detectors. The probability to find k photons at the first detector and l photons at the second one (with included detection efficiencies) is given by the formula

$$\Pi_{kl}=P_D\left(\frac{1}{2}\right)^N\sum_{m=k}^{N-l}\binom{N}{m}\left[\binom{m}{k}\eta_B^k(1-\eta_B)^{m-k}\right]\times\left[\binom{N-m}{l}\eta_B^l(1-\eta_B)^{N-m-l}\right],$$

where the summation limits stem from obvious constraints $m\geqslant k$, $N-m\geqslant l$. Thus the probability of double click in Bob's ''yes-no'' detectors when Eve is active and while Alice and Bob use different polarization bases reads

$$P_2^{(N)}=P_D\left[1-\sum_{l=0}^{N}\Pi_{0l}-\sum_{k=0}^{N}\Pi_{k0}+\Pi_{00}\right]$$

(note that Π_{00} would be subtracted two times). Because of the symmetry of the configuration, obviously,

$$\sum_{l=0}^{N}\Pi_{0l}=\sum_{k=0}^{N}\Pi_{k0}.$$

With the expressions

$$\Pi_{00}=P_D(1-\eta_B)^N,$$

$$\sum_{k=0}^{N}\Pi_{k0}=P_D\sum_{m=0}^{N}\binom{N}{m}2^{-N}\sum_{k=0}^{m}\binom{m}{k}\eta_B^k(1-\eta_B)^{N-k}=P_D\left(1-\frac{\eta_B}{2}\right)^N$$

we obtain finally for the double-click probability

$$P_2^{(N)}=P_D\left[1-2\left(1-\frac{\eta_B}{2}\right)^N+(1-\eta_B)^N\right]. \tag{29}$$

B. Eve sends a mixture of number states

Of course, there is no reason to restrict Eve only to the use of number states. After successful state discrimination she can send to Bob any pure state or mixture. However, from Bob's point of view these signals are effectively mixtures of photon-number states because of the nature of his detectors (they may be described by the pair of projectors: $P_{\mathrm{no}}=|0\rangle\langle 0|$ and

$$P_{\mathrm{yes}}=\sum_{n=1}^{\infty}|n\rangle\langle n|).$$

Therefore, it is sufficient to analyze only a mixture of photon-number states in the polarization of the identified signal, so that only the photon-number statistics remains to be chosen by Eve.

As already mentioned, Bob is interested only in the number of single clicks (in case his and Alice's bases coincide) and double clicks (if the bases differ). One can plot a very illustrative diagram displaying relations between corresponding single-click and double-click probabilities (see Fig. 3).

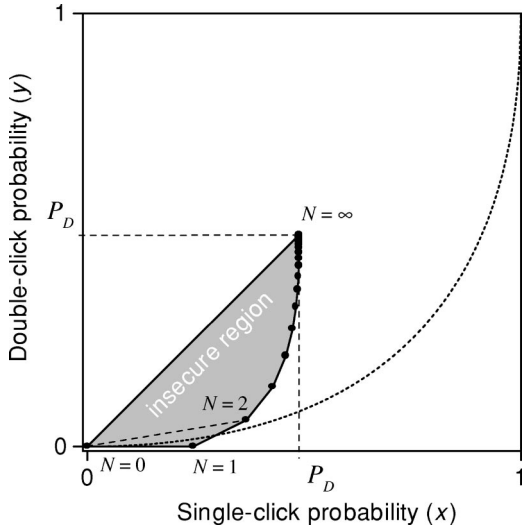

FIG. 3. Diagram displaying relations between ''single-click'' and ''double-click'' probabilities. The highlighted area contains all possible combinations of Bob's detection probabilities stemming from Eve's activity (described in the text) for a given detection efficiency (here, particularly, $\eta_B=0.5$) and a given mean photon number in states sent by Alice ($\mu=4$). It is a region of *insecure* key generation. The shape of the area depends on η_B, the scaling on μ [through discrimination probability $P_D(\mu)$]. The separate dotted curve represents a set of all possible ''working points'' without an eavesdropper, i.e., a set of all possible pairs of expected $\overline{P_1}$ and $\overline{P_2}$. Any particular position of a working point depends on the values of the line transmittance (η_L), the detection efficiency (η_B), and the mean photon number (μ). The value of $\mu=4$ is chosen to make the diagram well readable. The structure is the same for lower, realistic values.

The situation where Eve sends number states to Bob is represented by a dot for each value of the photon number N. The positions of these dots have been calculated for fixed values of η_L and μ. Coordinates of a point corresponding to any mixture of number states can always be expressed as a linear convex combination of coordinates corresponding to individual number states. Because of the convexity of the above-mentioned curve all such points must lie inside (or on the boundary) of the polygon with vertices at the points corresponding to number states (i.e., in the area highlighted in Fig. 3).

We can explicitly prove the convexity of the boundary formed by the points for fixed photon number. The points with x coordinate $P_1^{(N)}$ [Eq. (28)] and y coordinate $P_2^{(N)}$ [Eq. (29)] lie on a continuous curve that can be expressed with the help of Eq. (28) by a real continuation of the parameter N as

$$N=\frac{\ln(1-x/P_D)}{\ln(1-\eta_B)}.$$

Substituting into Eq. (29) we obtain the explicit equation of the curve

$$y=\left[2-2\left(1-\frac{x}{P_D}\right)^{\kappa}-\frac{x}{P_D}\right]P_D, \tag{30}$$

where

$$\kappa = \frac{\ln(1-\eta_B/2)}{\ln(1-\eta_B)}.$$

Calculating the second derivative of Eq. (30) with respect to x and using the fact that η_L, η_B, and x/P_D take values in the interval between 0 and 1, it follows that the curve given by Eq. (30) is convex. This proves that the highlighted area in Fig. 3 is indeed convex.

C. Insecure parameter regime

The convex area defined in the previous section can be called a region of insecurity. We define the working point of a setup as the point whose coordinates are given by expected values in the absence of an eavesdropper. If this working point falls into the region of insecurity, Eve can get complete information on the key without a risk of being disclosed.

The set of all possible working points is represented by the dotted curve in the diagram. Expected single-click probability $\overline{P}_1$ [Eq. (26)] represent the x coordinate, expected double-click probability $\overline{P}_2$ [Eq. (27)] represents the y coordinate. From Eq. (26) the exponential can be expressed and substituted into Eq. (27). Thus the explicit equation of the working point curve reads

$$y = [1-(1-x)^{1/2}]^2. \tag{31}$$

We have to answer the question: For which values of parameters η_L, η_B, and μ does the working point lie in the region of insecurity?

1. Necessary condition for insecurity

If the expected probability of single clicks satisfies $\overline{P}_1 > P_1^{(N)}$ for all N, then the working point will certainly not fall to the region of insecurity, which is clearly illustrated in Fig. 3. This leads to the necessary condition for insecurity given by $\overline{P}_1 < P_D$. To evaluate the implication for the experimental parameters, we substitute Eq. (26),

$$\eta_L \eta_B < \frac{-\ln[1-P_D(\mu)]}{\mu}. \tag{32}$$

An analysis of this expression shows that for a fixed expected photon number μ a system cannot be cracked by an USD attack if the total transmission efficiency $\eta_L \eta_B$ is higher than a certain threshold that depends on the the expected photon number μ. This dependence is evaluated numerically in Fig. 4. The surprising aspect is, that the threshold does not go to 1 as μ goes to infinity. Instead we find

$$(\eta_L \eta_B)^{(\infty)} = \lim_{\mu\to\infty} \frac{-\ln[1-P_D(\mu)]}{\mu} = (1-2^{-1/2}) \approx 0.293. \tag{33}$$

This shows, that that the implementation of quantum cryptography with weak coherent states cannot be cracked completely by the USD attack for *all* values of the expected photon number μ as long as the total transmission satisfies $\eta_L \eta_B \geqslant 1-2^{-1/2}$.

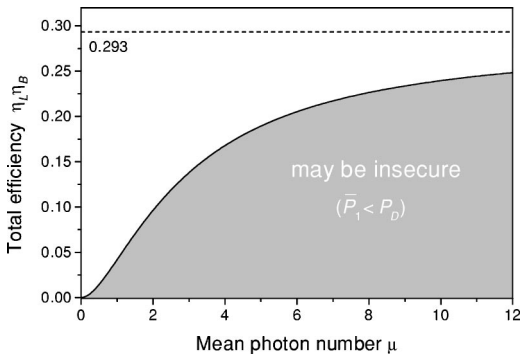

FIG. 4. If the value of expected single-click probability is greater then the discrimination probability ($\overline{P}_1 > P_D$) the described USD attack can be, in principle, detected. The plot shows an example of a curve separating the set of values of total efficiencies ($\eta_L \eta_B$) and mean photon numbers (in states sent by Alice) satisfying the above constraint [see inequality (32)].

2. Sufficient condition of insecurity

In this section we will derive precise conditions determining when a working point falls into the region of insecurity. In a first step we will show that for parameters of practical applications it is sufficient to consider the scenario that the working point falls below the straight line going through the origin and the vertex $N=2$. This condition corresponds to

$$x_w \geqslant y_w \frac{x_2}{y_2}. \tag{34}$$

The coordinates of points used in this condition are defined in Table I. In the second step we can then determine whether in this scenario the working point lies inside or outside the region of insecurity by checking on which side of the line going through the vertices $N=1$ and $N=2$ it lies (see Fig. 3). If it lies on the left, QKD is insecure. This corresponds to the inequality

$$x_w \leqslant y_w \frac{x_2 - x_1}{y_2} + x_1. \tag{35}$$

First, let us turn to the inequality (34). Substituting expressions for all coordinates according to Table I one obtains an inequality that is quadratic in the variable R

TABLE I. Coordinates of selected points in the parameter space of ''observables,'' which are the probabilities of single clicks (x) and double clicks (y) in Bob's detectors.

Working point	$x_w =$ $1-\exp(-\eta_L \eta_B \mu)$	$y_w =$ $\left[1-\exp\left(-\frac{\eta_L \eta_B \mu}{2}\right)\right]^2$
Vertex $N=1$	$x_1 = P_D \eta_B$	$y_1 = 0$
Vertex $N=2$	$x_2 = P_D(2\eta_B - \eta_B^2)$	$y_2 = P_D \eta_B^2/2$

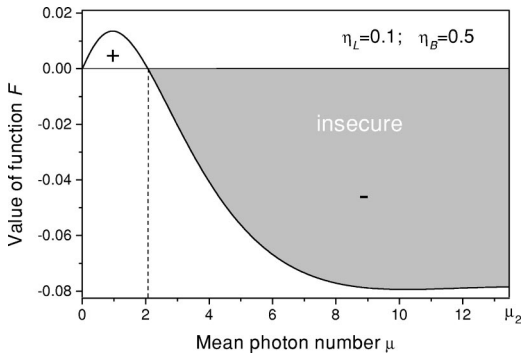

FIG. 5. The sign of the function $F(\mu,\eta_L,\eta_B)$ is a criterion for the security (positive) or insecurity (negative) of the quantum key distribution with respect to the USD attack. The line transmittance and Bob's detection efficiency are fixed: $\eta_L=0.1$, $\eta_B=0.5$. Mean photon number, μ goes from zero to μ_2 limit. If F is negative the transmission is totally insecure. The zero point lies at $\mu\approx 2.07$ photons.

$=\exp(-\eta_L\eta_B\mu/2)$ with the parameter η_B. We find that the working point lies below the line connecting vertices $N=0$ and $N=2$ if $R\in((4-3\eta_B)/(4-\eta_B),1)$. Thus the mean photon number in coherent states sent by Alice must be lower than a threshold μ_2 given by

$$\mu<\mu_2=\frac{-2}{\eta_L\eta_B}\ln\left(\frac{4-3\eta_B}{4-\eta_B}\right). \tag{36}$$

We find that $\mu_2\in[1/\eta_L,2\ln 3/\eta_L]$ for any η_B and, especially, always $\mu_2\geqslant 1$. As we can see, this condition is satisfied in all current experiments and does not pose a serious restriction to the validity of our analysis especially for nonnegligible loss.

Now let us turn our attention to the condition (35) which, whenever condition (36) is fulfilled, determines whether the working point is in the region of insecurity. It can be expressed in the following form:

$$F(\mu,\eta_L,\eta_B):=x_w\eta_B-2y_w(1-\eta_B)-P_D\eta_B^2\leqslant 0. \tag{37}$$

Due to the complicated dependence of P_D on μ we failed to find its analytical solution. The analytical statement we can do without any extra approximation is based on the observation that

$$\left.\frac{\partial F}{\partial\mu}\right|_{\mu=0}=\eta_L\eta_B^2>0 \quad \text{and} \quad F(0,\eta_L,\eta_B)=0.$$

This implies that there exists always a range of values for μ starting from $\mu=0$ for which we have $F>0$, i.e., the security of the key distribution cannot be cracked completely by the USD attack.

It is easy to evaluate condition (37) numerically. In Fig. 5 we give an example for the values of line transmittance $\eta_L=0.1$ and detection efficiency $\eta_B=0.5$ (so that $\mu_2\approx 13.46$). In this particular case, the transmission becomes insecure in about 2.07 photons. It is not completely satisfying to have to fall back to numerical methods to investigate

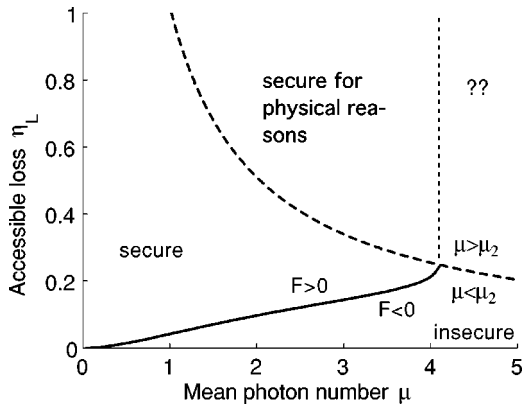

FIG. 6. The secure parameter regime for the losses accessible to Eve for large Bob's losses ($\eta_B\ll 1$) is the region above the solid line ($F>0$). In the region with $F\leqslant 0$ and $\mu<\mu_2$ the system is insecure. In the remaining region we have $F\leqslant 0$, but since $\mu>\mu_2$, we cannot make any definitive statements about security.

the security against the USD attack. Fortunately, it is possible to get some analytic results in a situation that is relevant to applications.

3. Partly accessible loss in a system with large loss

The results of the preceding sections illuminate to what extent Eve can achieve perfect eavesdropping by making an unambiguous state discrimination measurement followed by sending the identified signals directly to Bob's detectors, thereby bypassing the lossy quantum channel.

However, Eve does not necessarily need to access the whole lossy quantum channel to be successful. By accessing we mean that Eve can avoid these losses either by replacing a quantum channel by a perfect, loss-free one, or by replacing it by classical communication and state preparation. The formulas of the previous sections still apply if we collect in the quantity η_B all those losses on the way to Bob's detector that are not accessible to Eve, while η_L denotes now only that loss that is accessible to her. It is instructive to look at the limit of high nonaccessible losses ($\eta_B\ll 1$). In that case we can approximate the function F of Eq. (37) by

$$F\approx\eta_B^2(\eta_L\mu-\tfrac{1}{2}\eta_L^2\mu^2-P_D). \tag{38}$$

The insecurity criterion $F\leqslant 0$ in the region $\mu<\mu_2$ [from Eq. (36)] then leads to the condition

$$\eta_L\leqslant\frac{1}{\mu}(1-\sqrt{1-2P_D}), \tag{39}$$

which is independent of η_B. It can be approximated by

$$\eta_L\leqslant\eta_L^{\text{crit}}\approx\frac{P_D}{\mu}\approx\frac{1}{12}\mu^2. \tag{40}$$

Condition (39) is shown in Fig. 6 as a solid line. To make statements about security against the USD attack, we need to consider additionally condition (36), which can be approximated by $\mu<1/\eta_L$ in leading order of η_B and is shown as a dashed line. We now can conclude that the system is secure

against USD attacks in the regime of small detection efficiencies η_B if we are in the parameter region with $F>0$ and $\mu<\mu_2$. Furthermore, the system is insecure in the region $F\leqslant 0$ and $\mu<\mu_2$. For the region with $\mu>\mu_2$, we can only make indirect statements. One is, that if the system is secure for a pair of values (μ,η_L), then it must be secure for all values (μ,η_L') with $\eta_L'>\eta_L$, otherwise Eve could gain an advantage by not accessing all the loss available to her. Therefore the only region about which we cannot make a statement with the present calculation is the region with $\mu>4.1$ and $\eta_L>1/\mu$. Here more detailed calculation would be necessary.

Note that these considerations are valid for $\eta_B\ll 1$ and only in this limit does η_B no longer play any role. For higher values of η_B this changes.

D. Comment on the statistical nature of the problem

One should keep in mind that all of Bob's measurements have a statistical character. Bob does not measure probabilities but finite numbers of clicks, which naturally fluctuates. In practice Bob must set certain limits of a ''confidential interval'' of acceptable numbers of detector clicks. The effect of this is that in some cases Bob will reject the transmission even if no eavesdropper is present. A more serious implication is that there is always some nonzero probability that Eve will not be detected even if the working point lies outside the insecurity region.

Note that Eve does not need to eavesdrop all the time—she may let pass a fraction of the signal sequence without any intervention. Her (deterministic) information on the key decreases with this strategy. But both Bob's single and double-click probabilities also change. The point corresponding to such an eavesdropping strategy (in the diagram as in Fig. 3) shifts along the straight line connecting ''full time'' Eve's strategy point with Alice's and Bob's working point. The relative shift equals the fraction of transmission during which Eve is active.

For practical purposes it would be necessary to determine the probability that Eve's information on the key (due to the USD attack) will be smaller than a certain chosen limit, as a function of the limits of the confidential interval and of the length of the key. This represents a challenge for the further research in this field.

V. USD ATTACK VERSUS BEAM-SPLITTING ATTACK

Traditionally, security against the beam-splitting attack [14] has been used as a practical level of security. In the beam-splitting attack the lossy line is replaced by an ideal loss-free line complemented by a beam splitter such that the total loss of the original line is reproduced. The eavesdropper stores any photons coming out of the free arm of the beam splitter. Whenever the eavesdropper *and* the receiver obtain a photon, which is possible for multiphoton signals, Eve can measure her signal after she learns the polarization basis in the public announcement and she will learn thereby the bit value of these signals completely.

It is interesting to note that security against a beam-splitting attack suggests that one can obtain a secure key even for large average photon numbers. In the absence of errors, the gain rate of secure key bits per signal bit can be approximated in a way similar to that used in Ref. [12] for the optimal individual attack. This approximation is given by

$$G_{\mathrm{BS}}=\tfrac{1}{2}(p_{\mathrm{exp}}-p_{\mathrm{split}}), \tag{41}$$

where the factor 1/2 stems from discarding signals with unequal polarization basis. Then p_{exp} is the probability that Bob receives a signal, while p_{split} is the joint probability that Eve learned the bit value of a signal and that the signal is received by Bob. To point out the basic problem of the beam-splitting attack it is sufficient to consider the case of $\eta_B=1$ and of coherent states. Then we find for Poissonian photon statistics and a transmission rate η of the system

$$p_{\mathrm{exp}}=1-\exp(-\eta\mu), \tag{42}$$

$$p_{\mathrm{split}}=p_{\mathrm{exp}}\{1-\exp[-(1-\eta)\mu]\}, \tag{43}$$

$$G_{\mathrm{BS}}=\tfrac{1}{2}\exp[-(1-\eta)\mu][1-\exp(-\eta\mu)], \tag{44}$$

which is always positive. Actually, the optimum is obtained for $\mu\approx 1$. It is clear from our analysis, however, that for large values of μ and typical loss rates, the USD attack will render the quantum key distribution protocol completely insecure.

The awareness of this problem is low, and it is thought that it can be avoided by complementing the beam-splitting attack with the additional requirement of keeping the average photon number low, much lower than 1, to keep the setup in the quantum domain. This seems rather odd, since there is no obvious justification for this requirement. More importantly, even for photon numbers $\mu\ll 1$, we find that for sufficiently large loss the transmission becomes insecure according to the USD attack while the analysis according to the beam-splitting attack makes us believe that we are dealing with a secure key. It seems that the USD attack is underestimated since the probability of success in the unambiguous state discrimination goes with μ^3 since only for three or more photons the four signal states are actually linear independent. The beam-splitting attack, however, succeeds with a probability of order μ^2, since already two photons can be split by the beam splitter.

This seems to imply that beam splitting is the more powerful attack. However, this is not the case since the two attacks vary in their power differently as the loss of the system increases. In the USD attack the probability to identify a signal depends only on the average photon number μ, and once this probability is high enough to generate the expected number of signals for the receiver (which depends on the amount of loss) then the transmission becomes insecure. In the beam-splitting attack, on the other hand, the total probability of identified signals p_{split} depend on μ *and* on the transmission coefficient η, and this probability goes *down* with increasing loss for fixed μ. And indeed, we find that $p_{\mathrm{exp}}>p_{\mathrm{split}}$. In other words, the beam-splitting attack becomes less efficient with increasing loss. This is easy to see in a simple example of a two-photon signal. The probabili-

ties $p(n,2-n)$ that $n=0,1,2$ photons arrive at Bob's detectors and $n-2$ photons go to Eve in the beam-splitting attack, are given by

$$p(0,2)=(1-\eta)^2, \tag{45}$$

$$p(1,1)=2\eta(1-\eta), \tag{46}$$

$$p(2,0)=\eta^2. \tag{47}$$

This means, that for high losses ($\eta \ll 1$) most likely both photons are sent to Eve. The probability of this event is $p(0,2)\approx 1-2\eta$, while the splitting probability goes down as $p(1,1)\approx 2\eta$. The respective probabilities for n-photon signals are of the same order of magnitude in η. Therefore, clearly, there is a crossover as a function of η where for fixed average photon number η the USD attack is more efficient than the beam-splitting attack.

We would like to stress again that from a technological point of view the USD attack seems to be easier to implement than the beam-splitting attack. This is based on two points. First, experience indicates that complete measurements which destroy the quantum state completely, as is possible by the USD attack, are easier to realize (at least in some approximation) than the realization of a quantum channel with reduced loss, as required by the beam-splitting attack. Second, the beam-splitting attack implies the use of quantum memory, which could store the split-off signal photons until the polarization bases for each signal are announced.

Finally, we would like to point out again that a security proof for realistic signals with Poissonian photon-number distribution exists for individual attacks [12] and coherent attacks [13]. Naturally, these security proofs include the security against the beam-splitting attack and against the USD attack.

VI. CONCLUSIONS

We have quantitatively analyzed an attack against realistic quantum crypto systems that enables an eavesdropper to gain information on the key without causing any errors in case of a lossy channel or poor detection efficiencies. It uses unambiguous discrimination of linearly independent signal states. This attack does not require the ability to store quantum states or to perform complicated quantum dynamics. Moreover, the attack does not require to substitute the lossy quantum channel by a perfect one.

We have derived a set of conditions that allow one to judge whether a given system can be totally insecure under the USD attack. We have shown a secure parameter regime in terms of the total transmission efficiency and the mean photon number. In the important limit of small detection efficiencies η_B, we have obtained an analytic result so that we can give explicitly a set of parameters (line transmittances, detector efficiencies, and mean photon numbers in coherent states sent by Alice) for which the transmission is secure/insecure under the USD attack. In theory, the signal can always be chosen to be weak enough to allow secure communication. In practice, however, the detector noise places restrictions on that end [11]. Finally, we showed that security against beam-splitting attacks does not necessarily imply security against the USD attack. This implies that we need to search for a better conditional security criterion against attacks deemed practical with currently available technology.

ACKNOWLEDGMENTS

M.D. acknowledges discussions with Ondřej Haderka and Martin Hendrych and support from grants of the Czech Ministry of Education (research project ''Wave and particle optics'' and project VS 96028) and the Czech National Security Authority (19982003012). This work was supported under Project No. 43336 of the Academy of Finland.

[1] G. S. Vernam, J. Am. Inst. Electr. Eng. **45**, 109 (1926).
[2] 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.
[3] S. Wiesner, SIGACT News **15**, 78 (1983).
[4] B. Huttner and A. K. Ekert, J. Mod. Opt. **41**, 2455 (1994).
[5] D. Mayers, in *Advances in Cryptology—Proceedings of Crypto '96* (Springer, Berlin, 1996), pp. 343–357; also available as e-print quant-ph/9606003.
[6] D. Mayers, e-print quant-ph/9802025v4, 1998.
[7] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
[8] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[9] H. P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996).
[10] M. Dušek, O. Haderka, and M. Hendrych, Opt. Commun. **169**, 103 (1999).
[11] G. Brassard, N. Lütkenhaus, T. Mor, and B. Sanders, e-print quant-ph/9911054.
[12] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); also e-print quant-ph/9910093.
[13] H. Inamori, N. Lütkenhaus, and D. Mayers (unpublished).
[14] C. H. Bennett, F. Bessette, G. Brassard, and L. Savail, J. Cryptology **5**, 3 (1992).
[15] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).
[16] A. Peres, Phys. Lett. A **128**, 19 (1988).
[17] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).
[18] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).
[19] B. Huttner, A. Muller, J. D. Gautier, H. Zbinden, and N. Gisin, Phys. Rev. A **54**, 3783 (1996).
[20] H. E. Brandt, Am. J. Phys. **67**, 434 (1999).