Unambiguous discrimination of linearly independent states as an eavesdropping strategy

Miloslav DUŠEK [1], Mika JAHMA[2], and Norbert LÜTKENHAUS [2]

[1]*Dept. of Optics, Palacký University, 17. listopadu 50, 772 00 Olomouc, Czech Rep.*

[2]*Helsinki Institute of Physics, P.O. Box 9, 00014 Helsingin yliopisto, Finland*

Abstract. Realistic implementations of quantum key distribution (QKD) mostly use signal states which are non-orthogonal but *linearly independent.* This fact enables an eavesdropper to perform unambiguous state discrimination and to get some information on the key without disturbing the transmission. In this paper, the limits for secure QKD, imposed by such an attack, are determined. It is also shown that security against beam-splitting attack does not necessarily imply security against the unambiguous-state-discrimination attack.

1. Introduction

The only *provably* secure way to communicate with guaranteed privacy is the so called one-time pad or Vernam cipher [1]. It requires both communicating parties share a secret key of the same length as the message. Quantum key distribution (QKD) is a technique to provide two parties with such a secure, secret and shared key. The first complete protocol for QKD was given by Bennett and Brassard [2] (BB84) following first ideas by Wiesner [3]. The essence of the protocol is that if non-orthogonal quantum states are used for communication and a channel transmit them perfectly then eavesdropping is detectable.

We consider the BB84 protocol in a typical quantum optical implementation. Ideally, Alice sends a sequence of single photons which are at random polarized in one of the following four states: right or left circular polarized, or vertically or horizontally polarized. 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, 6, 7]. In this article we follow another goal: we would like to illuminate to which extend even a very simple attack can render QKD impossible once realistic imperfections like lossy lines and non-ideal signal states are taken into account. The difficulties implied by the use of weak coherent states in combination with lossy lines has been pointed out earlier [8, 9, 10] and this subject has been illuminated in depth in [11], where bounds on coverable distances are given. Positive security proofs for sufficiently short distances considering realistic signals are given for individual attacks in [12]. The eavesdropping attacks which crack the secrecy of the key for setups exceeding this secure distances are still quite complicated (an eavesdropper needs to perform a QND measurement and store photons).

In this paper we deal with much simpler eavesdropping strategy that uses the opportunities arising from lossy lines and non-ideal signals. The attack has been first proposed by Bennett [13] and Yuen [9]. It is based on the fact that Eve can, with a 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 transmit 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 that Eve has to invest into a perfect quantum channel.

Our investigation of this scenario refines Bennett's and Yuen's analysis. It takes into account that the photon statistics of the signals arriving at Bob's detectors can be monitored to a certain extent. The results illuminate the restrictions placed on implementations of QKD on lines with strong losses. We show that, contrary to common belief, the use of unambiguous state discrimination can be a more efficient eavesdropping strategy than the beam-splitting attack [13], even for dim coherent states.

2. Unambiguous discrimination of signal states

Let us consider N different quantum states. Unambiguous state discrimination is possible whenever these N states are linearly independent. The problem can be described by a measurement which can give the results 'state 0', 'state 1', ...'state $N-1$', and the result 'don't know'. The constraint is that the measurement results should never wrongly identify a state, and the goal is to keep the fraction of 'don't know' results as low as possible. This problem has been investigated by Ivanovic [14] for the case of two equally probable non-orthogonal states. Peres [15] solved this problem in a formulation with probability operator measures (POM). Later Jaeger and Shimony [16] extended the solution to arbitrary a priori probabilities. Peres's solution has been generalized to an arbitrary number of equally probable states which are generated from each other by a symmetry operator by Chefles and Barnett [17]. They used the fact that the symmetry allows to write the input states in the form

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

where $|\phi_j\rangle$ represent a set of orthonormal states. Then they have shown that the maximum probability of the successful unambiguous state discrimination is given by the formula:

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

Practical implementations of QKD mostly employ attenuated laser pulses. Thus the reasonable description of realistic signal states seems to be that of a coherent state with a small amplitude α. The four BB84 signal states, carrying two linear and two circular polarizations, may be expressed in terms of two modes (corresponding to two linear orthogonal polarizations) as follows

$$\begin{aligned} |\Psi_0\rangle &= \left|\alpha/\sqrt{2}\right\rangle \left|\alpha/\sqrt{2}\right\rangle, \qquad & |\Psi_1\rangle &= \left|\alpha/\sqrt{2}\right\rangle \left|\mathrm{i}\alpha/\sqrt{2}\right\rangle, \\ |\Psi_2\rangle &= \left|\alpha/\sqrt{2}\right\rangle \left|-\alpha/\sqrt{2}\right\rangle, \qquad & |\Psi_3\rangle &= \left|\alpha/\sqrt{2}\right\rangle \left|-\mathrm{i}\alpha/\sqrt{2}\right\rangle. \end{aligned} \tag{3}$$

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. That means that for a given polarization she does not see the coherent state $|\alpha\rangle$ but the phase averaged density matrix $\frac{1}{2\pi}\int_\phi |e^{\mathrm{i}\phi}\alpha\rangle\langle e^{\mathrm{i}\phi}\alpha|\, \mathrm{d}\phi$. This results in signal states which are mixtures of Fock states with a Poissonian photon number distribution described by the density matrix

$$\rho = e^{-\mu} \sum_n \frac{\mu^n}{n!} |n\rangle\langle n|. \tag{4}$$

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 and a following measurement which unambiguously discriminates between the four resulting conditional states for each total photon number. The justification for this is that the measurement of the total photon number "comes free", since the execution of this measurement does not change the signal states. Therefore 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

$$P_D = \sum_{n=0}^{\infty} e^{-\mu} \frac{\mu^n}{n!} P_D^{(n)}. \tag{5}$$

The conditional states resulting from the QND measurement and corresponding to n photons in total satisfy again the symmetry condition which allows to apply the results by Chefles and Barnett. The maximum probability of unambiguous state discrimination for fixed value of n is given by (for more details see [18])

$$P_D^{(n)} = \begin{cases} 0 & n \le 2 \\ 1 - 2^{1-n/2} & n \text{ even} \\ 1 - 2^{(1-n)/2} & n \text{ odd.} \end{cases} \tag{6}$$

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

$$P_D = \sum_{n=0}^{\infty} e^{-\mu} \frac{\mu^n}{n!} P_D^{(n)} = 1 - e^{-\mu}\left(\sqrt{2}\sinh\frac{\mu}{\sqrt{2}} + 2\cosh\frac{\mu}{\sqrt{2}} - 1\right). \tag{7}$$

This result is compared to the result for coherent states in Fig. 1. 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. Actually, Bennett et al. [13] and Yuen [9] gave a simple beam-splitter setup which obtains a discrimination probability of $P_D = \frac{1}{32}\mu^3 + O(\mu^4)$.

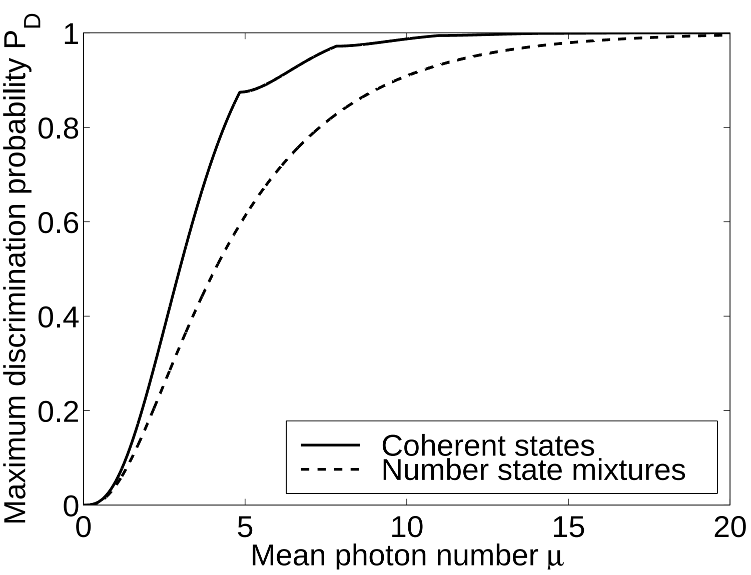

Figure 1. Comparison of the optimum probability of unambiguous states discrimination for coherent states and for the corresponding mixture of Fock states. Both have the same Poissonian photon number distribution with mean photon number μ.

3. Unambiguous state discrimination as eavesdropping strategy

Let us now consider the realistic situation when Alice uses the phase-averaged coherent states as signal states. These mixed states undergo Poissonian photon-number statistics with mean photon number μ. We fix our eavesdropping scenario, to which we refer 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 will study this strategy under realistic constraint. Of course, any real quantum channel connecting both parties suffer by losses. Let its transmittance be characterized by the transmission efficiency η_L. Further, we will 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. The detectors are modeled as "yes/no" detectors, which either fire, or they do not fire; they cannot distinguish the number of impinging photons.

Once Eve identified 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 includes 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 non-vacuum 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 expects to find at most one detector clicks; the probability of a click is

$$\bar{P}_1 = 1 - \exp(-\eta_L \eta_B \mu), \tag{8}$$

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

$$\bar{P}_2 = \left[1 - \exp\left(-\frac{\eta_L \eta_B \mu}{2}\right)\right]^2 . \tag{9}$$

How the situation changes 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.

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

$$P_1^{(N)} = P_D \left[1 - (1-\eta_B)^N\right] . \tag{10}$$

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 polarization bases, we can think of the photons as being equally and independently distributed to both Bob's detectors. The probability of double click in Bob's "yes-no" detectors when Eve is active then reads (see [18])

$$P_2^{(N)} = P_D \left[1 - 2\left(1 - \frac{\eta_B}{2}\right)^N + (1-\eta_B)^N\right] . \tag{11}$$

There is no reason to restrict Eve only to the use of number states. When she succeeds in 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 detection. 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 that his and Alice's bases coincide) and double clicks (if the bases differ). One can plot very illustrative diagram displaying relations between corresponding single-click and double-click probabilities (see Fig. 2). 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

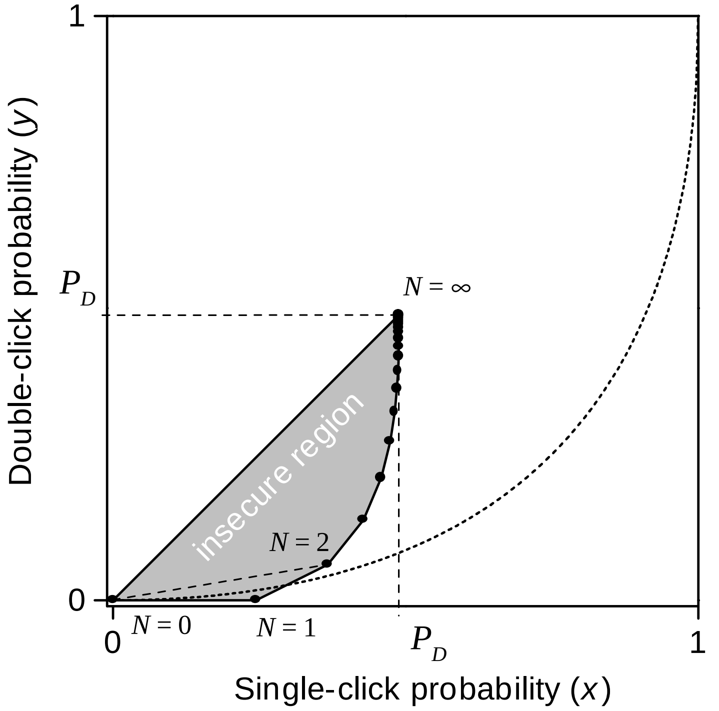

Figure 2. Diagram displaying relations between "single-click" and "double-click" probabilities. The highlighted area contains all possible combinations of Bob's detection probabilities stemming from Eve's activity for a given detection efficiency (here, particularly, $\eta_B = 0.5$) and a given mean 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 value of $\mu = 4$ is chosen to make the diagram well readable. The structure is the same for lower, realistic values. 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 $\bar{P}_1$ and $\bar{P}_2$. 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).

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. 2). This area 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 $\bar{P}_1$ represents x-coordinate, expected double-click probability $\bar{P}_2$ represents y-coordinate. Thus the explicit equation of the working point curve reads

$$y = \left[1 - (1 - x)^{1/2}\right]^2 . \qquad (12)$$

Now we have to find the values of parameters η_L, η_B, and μ for which the working point lies in the region of insecurity.

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 $N = 2$	$x_2 = P_D(2\eta_B - \eta_B^2)$	$y_2 = P_D\eta_B^2/2$

Table 1. 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.

3.1. Necessary condition for insecurity

If the expected probability of single clicks satisfies inequality $\bar{P}_1 > P_1^{(N)}$ for all N then the working point will certainly not fall to the region of insecurity. This leads to the necessary condition for insecurity given by $\bar{P}_1 < P_D$. To evaluate the implication for the experimental parameters, we substitute Eq. (8). We get

$$\eta_L\eta_B < \frac{-\ln[1 - P_D(\mu)]}{\mu}. \tag{13}$$

It means 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 which depends on the the expected photon number μ. The surprising aspect is, that the threshold does not go to 1 as μ goes to infinity. Instead we find

$$(\eta_L\eta_B)^{(\infty)} = \lim_{\mu\to\infty} \frac{-\ln[1 - P_D(\mu)]}{\mu} = (1 - 2^{-1/2}) \approx 0.293. \tag{14}$$

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 $\eta_L\eta_B \geq 1 - 2^{-1/2}$.

3.2. Sufficient condition of insecurity

Now 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 the working point falls below the straight line going through the origin and the vertex $N = 2$. This condition corresponds to

$$x_w \geq y_w \frac{x_2}{y_2}. \tag{15}$$

The coordinates of points used in this condition are defined in Tab. 1. 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 connecting the vertices $N = 1$ and $N = 2$ it lies (see Fig. 2). If it is on the left, QKD is insecure. This corresponds to the inequality

$$x_w \leq y_w \frac{x_2 - x_1}{y_2} + x_1. \tag{16}$$

First, let us turn to the inequality (15). Substituting expressions for all coordinates according to Tab. 1 one obtains an inequality which is quadratic in the variable $R =$

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

$$\mu < \mu_2 = \frac{-2}{\eta_L\eta_B} \ln\left(\frac{4-3\eta_B}{4-\eta_B}\right). \tag{17}$$

We find that $\mu_2 \in [1/\eta_L, 2\ln 3/\eta_L]$ for any η_B and always $\mu_2 \geq 1$. As one 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 non-negligible loss.

Now let us turn our attention to the condition (16) which, whenever condition (17) is fulfilled, determines whether the working point is in the region of insecurity. It can be expressed in the following form

$$F(\mu,\eta_L,\eta_B) := x_w\eta_B - 2y_w(1-\eta_B) - P_D\eta_B^2 \leq 0, \tag{18}$$

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.

Condition (18) can be easily evaluated numerically. E.g., for values of line transmittance $\eta_L = 0.1$ and detection efficiency $\eta_B = 0.5$ (so that $\mu_2 \approx 13.46$) function F is positive if $\mu \in (0,\mu_0)$ and negative (i.e. QKD is totally insecure) if $\mu \in (\mu_0,\mu_2)$ where the zero point lies at $\mu \approx 2.07$ photons.

3.3. Partly accessible loss in a system with large loss

Eve does not necessarily need to access the whole lossy quantum channel to be successful. (By *accessing* we mean, that she 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 derived above still apply if we collect into 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 non-accessible losses ($\eta_B \ll 1$). In that case we can approximate function F of equation (18) by

$$F \approx \eta_B^2 \left(\eta_L\mu - \frac{1}{2}\eta_L^2\mu^2 - P_D\right). \tag{19}$$

The insecurity criterion $F \leq 0$ in the region $\mu < \mu_2$ then leads to the condition

$$\eta_L \leq \eta_L^{\rm crit} = \frac{1}{\mu}\left(1 - \sqrt{1-2P_D}\right) \approx \frac{P_D}{\mu} \approx \frac{1}{12}\mu^2, \tag{20}$$

which is independent of η_B. Dependence of $\eta_L^{\rm crit}$ on μ is shown as a solid line in Fig. 3. The additionally condition (17) can be approximated by $\mu < 1/\eta_L$ in leading order of η_B (a dashed line in Fig. 3).

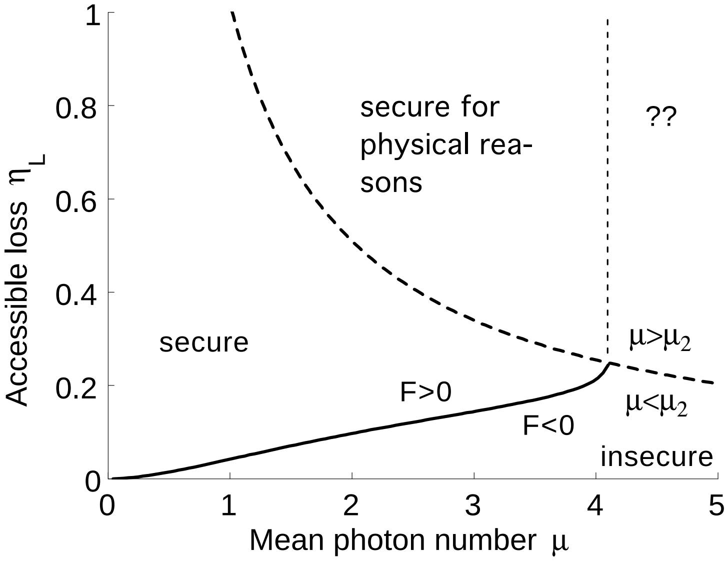

Figure 3. The secure parameter regime for the losses accessible to Eve for large Bob's losses ($\eta_B \ll 1$) is the region above the solid line ($F > 0$). In the region with $F \leq 0$ and $\mu < \mu_2$ the system is insecure. In the remaining region we have $F \leq 0$, but since $\mu > \mu_2$, we cannot make any definitive statements about security.

We can conclude that the system is secure against USD attacks in the regime of small detection efficiencies η_B if $F > 0$ and $\mu < \mu_2$. Furthermore, the system is insecure if $F \leq 0$ and $\mu < \mu_2$. For the parameter 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. In the remaining region we have $F \leq 0$, but since $\mu > \mu_2$, we cannot make any definitive statements about security. Note that these considerations are valid for $\eta_B \ll 1$ and only in this limit η_B does no longer play any role. For higher values of η_B this changes.

4. Comparison of USD attack and beam-splitting attack

Traditionally, security against the beam-splitting attack [13] has been used as a *practical* level of security. In the beam-splitting attack the lossy line is replaced by an ideal lossless one 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. If both the eavesdropper *and* the receiver obtain a photon (it 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 worth mentioning that security against beam-splitting attack allows that one can obtain a secure key even for large average photon numbers [12, 18]. 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.

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 depend on μ *and* on the transmission coefficient η, and this probability goes *down* with increasing loss for fixed μ. 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 probabilities $p(n, 2-n)$ 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

$$\begin{aligned} p(0,2) &= (1-\eta)^2, \\ p(1,1) &= 2\eta(1-\eta), \\ p(2,0) &= \eta^2. \end{aligned} \tag{21}$$

This means, that for high losses ($\eta \ll 1$) most likely both photons are sent to Eve. 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. There is no need of a quantum channel with reduced loss and no need of quantum memory, as required by the beam-splitting attack.

5. Conclusions

We have shown that unambiguous discrimination of linearly independent signal states can be used as an effective attack against realistic quantum crypto-systems. This attack enables eavesdropper to gain information on the key without causing any errors. It does not require the ability to store quantum states or to perform complicated quantum dynamics and it does not require to substitute the lossy quantum channel by a perfect one. We have derived a set of conditions which allow to judge whether a given system is insecure. In the limit of small detection efficiencies η_B we have obtained an analytic result that determines 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 with respect to the USD attack. We have also showed that security against beam-splitting attacks does not necessarily imply security against the USD attack.

Acknowledgments

This work was supported by the Academy of Finland (project 43336), the Czech Ministry of Education (research project "Wave and particle optics" and project VS 96028), and the Czech National Security Authority (19982003012).

References

[1] G. S. Vernam, Journal of the American Institute of Electrical Engineers **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 quant-ph/9606003.

[6] D. Mayers, Unconditional security in Quantum Cryptography, available as quant-ph/9802025v4.

[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 Semiclass. Opt. **8**, 939 (1996).

[10] M. Dušek, O. Haderka, and M. Hendrych, Opt. Comm. **169**, 103 (1999).

[11] G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Security Aspects of Practical Quantum Cryptography, available as quant-ph/9911054.

[12] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000), also available as quant-ph/9910093.

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

[14] I. D. Ivanovic, Phys. Lett. A **123**, 257 (1987).

[15] A. Peres, Phys. Lett. A **128**, 19 (1988).

[16] G. Jaeger and A. Shimony, Phys. Lett. A **197**, 83 (1995).

[17] A. Chefles and S. M. Barnett, Phys. Lett. A **250**, 223 (1998).

[18] M. Dušek, M. Jahma, N. Lütkenhaus, Unambiguous-state-discrimination attack in cryptography with weak coherent states, to appear in Physical Review A (August 2000), also available as quant-ph/9910106.