1 October 1999

ELSEVIER

Optics Communications 169 (1999) 103–108

OPTICS COMMUNICATIONS

www.elsevier.com/locate/optcom

Generalized beam-splitting attack in quantum cryptography with dim coherent states

Miloslav Dušek [a,*], Ondřej Haderka [a,b], Martin Hendrych [a,b]

[a] *Department of Optics, Palacký University, 17. listopadu 50, 772 00 Olomouc, Czech Republic*
[b] *Joint Laboratory of Optics of Palacký University and the Physical Institute of the Czech Academy of Sciences, 17. listopadu 50, 772 00 Olomouc, Czech Republic*

Received 3 February 1999; received in revised form 26 June 1999; accepted 23 July 1999

Abstract

As it is very difficult to prepare a good approximation of one-photon states, practical quantum cryptography uses highly attenuated laser pulses which can well be represented by coherent states with average photon number below one photon. In such a case more than one photon may appear in some pulses. Thus an eavesdropper has a chance to split the signal and gain some information on the key without disturbing the transmission in a substantial way. In this paper we derive the number of bits an eavesdropper can gain by this sort of attack and the question of limits on the average number of photons in a pulse is discussed. It is assumed an eavesdropper may have detectors with 100% efficiency, she can store the ‘extracted’ qubits, she can non-destructively measure the number of photons, and also she is able to perform ‘cascade’ beam splitting resulting in extraction of just one photon. Besides, it is assumed that she can replace a lossy communication line by a lossless one. © 1999 Published by Elsevier Science B.V. All rights reserved.

PACS: 03.67.D
Keywords: Quantum cryptography; Beam-splitting attack

1. Introduction

In principle, quantum cryptography offers unconditional security. Therefore its potential practical applications are taken very seriously today and many groups work on its technical realization. However, reality is harder than the Platonic world. There are several problems in practice. First, each real apparatus and transmission line exhibit losses, imperfections, and misalignments. This results in non-zero error rates during transmissions even in the absence of an eavesdropper. The unconditional security is imperilled. Fortunately, it seems that if the technological error rate is low enough, quantum key distribution (QKD) could still be unconditionally secure [1–7]. The principle of security of quantum cryptography lies in the overlap of the signal states used. A proof of security will not need to make any reference on the physical implementation of these states as

[*] Corresponding author. Tel. +420-68-563-4271; fax: +420-68-522-5246; e-mail: dusek@optnw.upol.cz

PII: S0030-4018(99)00419-8

long as they have the correct overlap probabilities and if the recipient is able to detect exactly the same set of states as are sent. But the latter condition represents a serious difficulty in practice, because real detectors are usually not able to distinguish the number of impinging particles. This fact may jeopardize the security even if information is encoded into other degrees of freedom (e.g., polarization of light or phase differences in an interferometer). Clearly, an eavesdropper can split the signal without the recipient detecting it (he is not able to distinguish, e.g., the states $|m\rangle$ and $|n\rangle$ for $m \neq n$ and $m,n > 0$; losses and a non-unity detection efficiency make the situation even more complicated). A way out from this impasse is to use for each bit exactly one particle (e.g., a photon) as an individual particle cannot be split.

The most suitable carrier of information seems to be light, however, the detectors of light suffer with the above-mentioned disability and, besides, it is not easy at all to prepare anything close to a single photon. Instead of one-photon states of light, highly attenuated laser pulses are usually used. If the spectral width of the pulse is much lower than its mean frequency, a real weak laser pulse may well be described by a monochromatic coherent state. In practice, the mean photon number is usually set to 0.1 . In such a case there are, on the average, 90.5% of laser pulses containing ‘no photon’, 9% with ‘one photon’, and 0.5% with ‘more than one photon’. The ratio of ‘one-photon pulses’ to ‘multi-photon ones’ increases with decreasing the mean photon number per pulse. However, herewith the transmission rate decreases rapidly. Still, there are some pulses remaining that contain more than one photon. The eavesdropper can try to split them in order to learn partial information without being disclosed.

A simple beam-splitting attack was first analyzed in Ref. [8]. Generalized versions of attacks of this kind were presented in Refs. [9,10]. These works deal with attacks involving beam splitting and quantum non-demolition measurement, and discuss the advantages of the use of quantum bits produced via parametric down conversion.

In the present paper we discuss a generalized beam-splitting attack including a full discussion of the statistics involved. The legitimate communicating parties are, by tradition, named Alice and Bob, and an eavesdropper is called Eve. We assume the BB84 transmission protocol [11]: Alice sends random bits encoded into two orthogonal states in one of two conjugated bases, which are also randomly chosen. Bob randomly and independently of Alice changes the same two bases in which he detects quantum states of the photons conveying qubits.

It is shown that beam splitting represents a rather effective attack. A *necessary* condition for security is derived, i.e., the limits to the values of mean photon numbers and losses are set. The discussed attack is related to specific technical conditions, particularly Alice transmits coherent states, whereas Bob’s detectors distinguish just the presence or absence of the field.

In the Sections below we employ the following notations:

μ – the mean photon number in a laser pulse at the output of Alice’s part of the apparatus;
η_L – intensity transmittance of the transmission line;
η_B – intensity ‘transmittance’ of Bob’s part of the apparatus (including detection efficiency);
N – the total number of laser pulses sent.

2. The number of key bits Eve can obtain by ‘beam-splitting’

Clearly, the average number of bits an eavesdropper can gain in this way is equal to at most one half of the number of all pulses ‘containing’ more than one photon (i.e., two or more photons). The reason for the *one half* is that Alice and Bob coincide just in one half of bases, on the average. Thus (when Alice sends coherent states)

$$N_E^{(\max)} = \frac{N}{2}\left[1 - e^{-\mu}(1+\mu)\right]. \tag{1}$$

Even for such a rough estimation there is, in principle, a set of mean photon numbers μ and losses characterized by transmittances η_L and η_B, for which secure communication is possible. However, a realistic consideration of Eve’s abilities enables us to make a more precise estimation.

Owing to the losses of the transmission line and of Bob’s terminal, not all $N_E^{(\max)}$ bits become part of the key. Since Eve is capable of learning deterministic information about these bits, an optimum strategy for her is to maximize Bob's chances of detecting these bits. Within the framework of the beam-splitting attack, she achieves this goal by splitting off as little as possible, i.e., just one photon.

Let us assume the following attack when Eve replaces the current lossy transmission line by a lossless one and then measures (non-destructively) numbers of photons in laser pulses during quantum key distribution. We will not be concerned with cases when she finds 0 or 1 photon, as in these cases she can gain no information through the discussed attack (of course, she can then apply other strategies). If she detects the number of photons $n \geq 2$, she will 'repeatedly split' the beam and measure photon numbers in order to finally separate exactly one photon for her own purposes and to sent the rest of $n-1$ photons to Bob (the higher the number of resent photons, the higher the probability of Bob's detection)[1]. In practice, the portion of photons transferred to Bob will perhaps be smaller, nevertheless the described case can be regarded as a possible limit and the 'worst' value[2]. Eve keeps the earmarked photons and after the public comparison of Alice's and Bob's bases she makes measurements on them. Knowing bases used for transmission, Eve can then obtain deterministic information on all bits of the key originating from 'multi-photon' pulses, i.e., she can get all the bits when Bob has detected a split 'multi-photon' pulse and when he agreed with Alice in the basis.

Let us now assume that states $|n\rangle$ arrive at Bob's part of the apparatus each with probability $\pi(n)$. Then photocount statistics at the outputs are described by the Bernoulli distribution:

$$p(m) = \sum_{n=m}^{\infty} \binom{n}{m} \eta_{\mathrm{B}}^{m} (1-\eta_{\mathrm{B}})^{n-m} \pi(n). \tag{2}$$

If Bob's detectors are only able to distinguish the presence or absence of the field, the detection probability is given by the sum

$$P = \sum_{m=1}^{\infty} p(m). \tag{3}$$

Since we are only interested in pulses with original number of photons $\ell \geq 2$ and since in such cases Eve always sends to Bob states $|\ell - 1\rangle$, the particular form of $\pi(n)$ defined above is

$$\pi(n) = \begin{cases} 0 & \text{for } n = 0,1, \\ p_{\mathrm{Poisson}}(n+1) = \dfrac{\mu^{n+1}}{(n+1)!} \mathrm{e}^{-\mu} & \text{for } n \geq 2, \end{cases} \tag{4}$$

where the fact that coherent states exhibit a Poissonian photon-number distribution was used.

Finally we obtain the following formula for the detection probability at Bob's detectors

$$\begin{aligned} P(\eta_{\mathrm{B}},\mu) &= \mathrm{e}^{-\mu} \sum_{m=1}^{\infty} \sum_{n=m}^{\infty} \binom{n}{m} \eta_{\mathrm{B}}^{m} \\ &\quad \times (1-\eta_{\mathrm{B}})^{n-m} \frac{\mu^{n+1}}{(n+1)!} \\ &= \mathrm{e}^{-\mu} \sum_{n=1}^{\infty} \frac{\mu^{n+1}}{(n+1)!} \sum_{m=1}^{n} \binom{n}{m} \\ &\quad \times \eta_{\mathrm{B}}^{m} (1-\eta_{\mathrm{B}})^{n-m} \\ &= 1 - \frac{\mathrm{e}^{-\eta_{\mathrm{B}}\mu}}{1-\eta_{\mathrm{B}}} - \mathrm{e}^{-\mu} \left(1 - \frac{1}{1-\eta_{\mathrm{B}}} \right), \end{aligned} \tag{5}$$

where simple reordering of summations is applied and the following expressions are employed:

$$\begin{aligned} &\sum_{m=1}^{n} \binom{n}{m} \eta_{\mathrm{B}}^{m} (1-\eta_{\mathrm{B}})^{n-m} \\ &\quad = \sum_{m=0}^{n} \binom{n}{m} \eta_{\mathrm{B}}^{m} (1-\eta_{\mathrm{B}})^{n-m} - (1-\eta_{\mathrm{B}})^{n} \\ &\quad = 1 - (1-\eta_{\mathrm{B}})^{n}, \end{aligned} \tag{6}$$

$$\sum_{n=1}^{\infty} \frac{x^{n+1}}{(n+1)!} = \sum_{k=0}^{\infty} \frac{x^{k}}{(k)!} - 1 - x = \mathrm{e}^{x} - 1 - x. \tag{7}$$

[1] As a 'practical' approximation of this process Eve can, e.g., diverge a small fraction of the beam and measure the photon number. If she finds zero, she repeats the procedure with the 'rest' of the beam. After some time she gets, with a high probability, just one photon.

[2] Detector efficiencies and losses of Bob's terminal are assumed out of Eve's control. However, as detection efficiency depends on the wavelength, Eve could try to shift the wavelength of the resent signal in order to increase the number of Bob's detections. Even if Alice and Bob do not operate at the 'most effective' wavelength, this intervention can be countered by inserting narrow-band filters in front of Bob's detectors.

Thus the average number of key bits Eve can obtain, by the attack discussed, is

$$N_{\mathrm{E}} = \frac{N}{2} P = \frac{N}{2}\left[1 - \frac{\mathrm{e}^{-\eta_{\mathrm{B}}\mu}}{1-\eta_{\mathrm{B}}} - \mathrm{e}^{-\mu}\left(1 - \frac{1}{1-\eta_{\mathrm{B}}}\right)\right]. \tag{8}$$

For small μ we obtain (expansion to the second order): $N_{\mathrm{E}} \approx \frac{N}{4}\mu^2\eta_{\mathrm{B}}$.

3. Excluding ‘one-photon’ pulses by Eve

Eve can perpetrate the iniquity that she stops all pulses in which she has found only one photon. If she also replaces the lossy line by a lossless one, Bob need not ever notice a decrease of data rate. Since actual numbers of detected qubits fluctuate, a slight decrease of data rate is hardly detectable. If losses on the line exceed a certain limit, Bob could even receive more qubits than expected.

In other words, communication can be secure only if the number of key bits Bob has received is greater than the number of key bits Eve could overhear. Otherwise Eve can know all bits of the key and neither Alice nor Bob can detect it.

For given losses and a given mean photon number, Bob expects (if no Eve is present) about

$$N_{\mathrm{B}} = \frac{N}{2}\left[1 - \exp(-\eta_{\mathrm{L}}\eta_{\mathrm{B}}\mu)\right] \tag{9}$$

bits of sifted key (after comparing bases). This estimation holds for the situation when Alice sends coherent states and Bob can detect and distinguish only two cases: no photon and one or more photons (he cannot measure the number of photons). So, from the inequality $N_{\mathrm{B}} > N_{\mathrm{E}}$ it follows that

$$1 \geq \eta_{\mathrm{L}} > \frac{1}{\eta_{\mathrm{B}}\mu}\ln\left[\frac{1-\eta_{\mathrm{B}}}{\exp(-\eta_{\mathrm{B}}\mu) - \eta_{\mathrm{B}}\exp(-\mu)}\right]. \tag{10}$$

With increasing η_{B} (decreasing losses in Bob’s terminal), the lower bound of η_{L} decreases, but cannot fall below the limit value $1 - \ln(1+\mu)/\mu$. For too low transmittances of the line, QKD is totally insecure. However, the limitation may not be fatal. There is still some room for certain practical applications, e.g., ‘local’ cryptosystems within buildings or cities. A system built in our laboratory [14,15] with a line 0.5 km long has $\eta_{\mathrm{L}} = 0.63$ and $\eta_{\mathrm{B}} = 0.19$. Thus inequality (Eq. (10)) is fulfilled for all $\mu < 2.68$ (of course, the actual value of μ must be considerably lower – see next Section).

4. Optimization

Taking the beam-splitting attack into consideration naturally leads to the question what mean photon number is optimal to render the particular implementation of QKD as efficient as possible, while maintaining its security. Beam-splitting attacks represent a very effective strategy which enables Eve to gain deterministic bits of the key without making disturbances detectable by Alice and Bob. A good eavesdropping strategy would then be to combine the generalized beam-splitting attack with some kind of optimal attack (possibly coherent) applied to the remaining one-photon pulses [1–3,5–7]. However, it has not been settled yet, which of attacks on one-photon pulses is the optimal one, nor was reliably determined the ultimate amount of information Eve could acquire through measurements on one-photon pulses, while producing a given error rate.

The optimal value of the mean photon number not only depends on the information that Eve might get through beam splitting and measurements on one-photon pulses, it is also affected by the particular error correction and privacy amplification procedures that are to be employed.

If Eve has only partial information on the key and if Alice and Bob can estimate the upper limit of her information [1,2], it can still be possible to ensure secure communication by force of a mathematical procedure called *privacy amplification* [8,12,13]. However, the newly obtained key may be considerably shorter.

Privacy amplification is applied after *error correction* to the corrected key. The corrected key has the same length or is shorter [3] than the sifted key. Reliable privacy amplification must take account of all possible Eve’s attacks. Besides, part of the result-

[3] If one wants to stop extra flow of information to Eve during error correction, some bits must be discarded.

ing key is also consumed for *authentication* of auxiliary, but necessary, public discussion. So, to guarantee secure QKD, the total number of corrected-key bits N_C should be equal to or greater than the sum of the number of bits discarded during privacy amplification N_{PA},the number of bits consumed for authentication N_{Au}, and – of course – the number of 'effective' bits N_K intended for later cryptographic use:

$$N_C \geq N_{PA} + N_{Au} + N_K . \tag{11}$$

Assuming no eavesdropper, the average number of corrected-key bits N_C can be estimated as

$$N_C = \frac{N}{2} f(\varepsilon)\left[1 - \exp(-\eta_L \eta_B \mu)\right], \tag{12}$$

where $0 \leq f(\varepsilon) \leq 1$ is a function of error rate ε. This function is given by the particular error-correcting procedure.

If the generalized beam-splitting attack is separated from all other attacks on one-photon pulses, one can write

$$N_{PA} = N_E + N_{Other} + N_{Secur} . \tag{13}$$

The quantity N_E is defined by Eq. (8), N_{Other} depends on the length of the sifted key and on the error rate, and N_{Secur} is the privacy amplification compression decreasing Eve's information to an arbitrarily low level defined by a security parameter δ.

The total number of secret bits needed for authentication depends on the length a of the authentication tag and on the length of the authenticated message; since the positions of bits in the train of pulses must be sent, this is proportional to $\log_2 N$ [14,15]. However, a shared secret sequence of this size has to be exchanged between Alice and Bob just once. Later on it suffices to renew (to 'refuel' from the transmitted key) only a much shorter password used for one-time pad encryption of the authentication tag [16], so $N_{Au} = a$.

Clearly, for given transmittances η_L and η_B, a maximal tolerable error rate ε, function $f(\varepsilon)$, parameters a and δ, and the length N_K of the required final key, one can optimize Eq. (11) with respect to μ in order to minimize the total number of laser pulses N.

There are cases in which inequality (Eq. (11)) cannot be fulfilled for any finite N. For some parameters of the apparatus, the number of transmitted bits N_C is always lower than the number of bits required by 'auxiliary' procedures – 'always' means for any μ and N. If the length N_C of corrected key is not large enough to cover demands on the right-hand side of Eq. (11), secure communication cannot be established. E.g., if the losses of the transmission line are too high, Eq. (11) cannot be satisfied for any μ irrespective of the value of N, because N_E would always be too large. In other words, if Eve replaces a lossy line by a lossless one, then she can know even more deterministic bits than Bob expects to obtain.

A particular example of an optimization process performed with our laboratory prototype of quantum-cryptographic apparatus can be found in Ref. [14].

5. Conclusions

It has been shown that the use of weak coherent states for quantum key distribution with a lossy channel enables a very efficient attack based on beam splitting. If the transmittance of the line is lower than a certain limit (depending on the losses of the recipient's apparatus and on the mean photon number per laser pulse), QKD becomes insecure. In spite of this, a large set of reasonable values of line transmittance η_L, Bob's apparatus efficiency η_B, and a mean photon number μ exist that secure communication is possible even if such an attack is taken into account.

Acknowledgements

The authors thank Charles H. Bennett for important advice concerning authentication and are grateful to Hoi-Kwong Lo and Norbert Lütkenhaus for valuable discussions. This research was supported by Czech Ministry of Education (VS 96028) and Czech National Security Authority (19982003012).

References

[1] C. Fuchs, N. Gisin, R.B. Griffits, C.-S. Niu, A. Peres, Phys. Rev. A 56 (1997) 1164.

[2] N. Lütkenhaus, Phys. Rev. A 54 (1996) 97.

[3] E. Biham, T. Mor, Phys. Rev. Lett. 78 (1997) 2256.

[4] E. Biham, T. Mor, Phys. Rev. Lett. 79 (1997) 4034.

[5] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, T. Mor, Security of Quantum Key Distribution Against All Collective Attacks, e-print: quant-ph/9801022.

[6] D. Mayers, Unconditional security in Quantum Cryptography, e-print: quant-ph/9802025 v4.

[7] H.-K. Lo, H.F. Chau, Quantum Computers Render Quantum Key Distribution Unconditionally Secure Over Arbitrarily Long Distances, e-print: quant-ph/9803006.

[8] C.H. Bennett, F. Bessette, G. Brassard, L. Salvail, J. Smolin, J. Cryptol. 5 (1992) 3.

[9] N. Lütkenhaus, Dim coherent states as signal states in the BB84 protocol: Is it secure?, Proc. QCM'98, Evanston, USA, August 1998.

[10] G. Brassard, T. Mor, B.C. Sanders, Quantum cryptography by parametric down conversion, Proc. QCM'98, Evanston, USA, August 1998.

[11] C.H. Bennett, G. Brassard, in: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175.

[12] G. Brassard, L. Salvail, in: Advances in Cryptology: Proc. of Crypto'93, Vol. 765 of Lecture Notes in Comp. Sci., Springer-Verlag, 1994, p. 410.

[13] C.H. Bennett, G. Brassard, C. Crépeau, U.M. Maurer, IEEE Trans. Inf. Theory 41 (1995) 1915.

[14] M. Dušek, O. Haderka, M. Hendrych, R. Myška, Phys. Rev. A 60 (1999) 149.

[15] M. Dušek, O. Haderka, M. Hendrych, Acta Physica Slovaca 48 (1998) 169.

[16] M.N. Wegman, J.L. Carter, J. Comput. Syst. Sci. 22 (1981) 265.