acta physica slovaca vol. 49 No. 4, 549 – 556 August 1999

SECURITY OF QUANTUM CRYPTOGRAPHY WITH REALISTIC SOURCES*

N. Lütkenhaus[1]
Helsinki Institute of Physics,
P.O.Box 9, 00014 Helsingin yliopisto, Finland

Received 5 May 1999, accepted 10 May 1999

The interest in practical implementations of quantum key distribution (QKD) is steadily growing. However, there is still a need to give a precise security statement which adapts to realistic implementation. In this paper I give the effective key rate we can obtain in a practical setting within the scenario of security against individual attacks by an eavesdropper. It illustrates previous results that high losses together with detector dark counts can make secure QKD impossible.

PACS: 03.67.Dd, 03.65.Bz, 42.79.Sz

1 Introduction

In 1984 Bennett and Brassard [1] proposed the first protocol which allows to distribute a cryptographic key such that the security of this distribution is guaranteed by quantum mechanics. Eight years later the first experiment [2] was performed to show the practicability of that scheme. (For an overview about QKD see for example [3].) Since then several groups demonstrated experimental techniques suitable for quantum key distribution. (See for example [4].)

From the theory point of view, however, the situation has evolved at a slower pace. Up to the present day we do not have a consistent and convincing way to establish an unconditionally secure key with existing experiments. To make this statement more precise, let me recapitulate what we know about security. We know that there exists no measurement in quantum mechanics which extracts information about the four signal states of the BB84 scheme without disturbing the signals. Therefore the original idea runs along the line that the occurrence of errors in the transmission is the signature of eavesdropping. This signature is open to observation by the two communicating parties. Departing from the ideal scheme, we always expect to find errors due to noise along the transmission line. Subsequent work, therefore, concentrates on the relation between the amount of Shannon information accessible by the eavesdropper as a function of the observed error rate. This has been done for various classes of eavesdropping attacks, first

* Presented at the 6th Central-European Workshop on Quantum Optics, Château Chudobín, Czech Republic, April 30 - May 3, 1999.

[1] E-mail address: lutkenha@rock.helsinki.fi

for von Neumann measurements on individual signals (see e.g. [5]), then later for general measurements on individual signals [6]. The resulting estimates show that the amount of Shannon information available to Eve is non-negligible even for ideal BB84 signals. We therefore need to suppress Eve's information on the key using the technique of generalized privacy amplification [7]. This technique allows to cut Eve's information from the key at the cost of the length of the key. To apply this techniques, estimates of another quantity, the collision probability (see below), as a function of the observed error rate are needed. The allowed new (shortened) length of the key has been calculated in the case of individual attacks for different settings [8–10].

From an early stage on, it has been recognized to be an important question to show *unconditional security*, that is security not only against individual attacks, but against the most general attack within quantum mechanics (coherent attack). In that case it is no longer possible to separate the creation of the secure key into a) the generation of the sifted key with b) subsequent key reconciliation and c) privacy amplification. Instead one has to view this process as a whole. The first work showing that this is indeed possible is the work by Mayers. He shows that one can obtain a secure key, which is unconditionally secure even for realistic error rates. Other results were obtained regarding unconditional security [11] and security against so-called *collective attacks* [12].

These results, however, cannot be applied directly to present day proposals for quantum key distribution experiments. The main reason is that the signal states used in those experiments are not single photon states. More precisely, the four signal states do now show the correct overlap probabilities as demanded by the BB84 protocol. It is not a straightforward task to extend Mayer's proof to the weak coherent states used in experiments. Instead, I will show that such a proof can be given once we make the restriction that the eavesdropper can perform attacks on individual signals only. This restriction opens the opportunity to include another features which, at present, cannot be included into Mayer's proof: error correction codes which are efficient in our situation work with bi-directional classical communication [13], while Mayers assumes uni-directional communication only.

In previous work I demonstrated a complete protocol to establish a secure key with the BB84 protocol under the restriction to individual attacks and ideal single photon signal states. Here I extend these results to any signals states which are mixtures of Fock states in the four polarization modes of the BB84 protocol. The sources for the signals covered therefore include a) dim coherent states with no fixed phase relation between subsequent pulses and b) signals generated by parametric down conversion.

The following results will highlight the difficulties arising from the use of multi-photon signals on lossy channels. In that situation we will find a limit on the amount of loss which can be tolerated without making the transmission insecure. This has been observed before by [2, 14, 15]. A more explicit demonstration can be found in [16, 17]. In contrast to these works, which show a necessary condition for secure QKD, I will present here a positive proof of security, restricted by the assumption of individual attacks on the signals.

2 Review of security against individual attacks

As pointed out in earlier work [10], we can not guarantee absolute security of the final key. Instead we can guarantee that the knowledge of an eavesdropper on the key is bounded with a certain probability. The measure of the eavesdropper's knowledge is the change of entropy due to the eavesdroppers measurement. If we denote by M the sequence of measurement results and of additional information obtained during the creation of a key with a given length, and by X the set of all possible keys, then this change of entropy is given by

$$\Delta_S = -\sum_{x\in X} p(x)\log p(x) + \sum_{x\in X} p(x|M)\log p(x|M)\ . \tag{1}$$

The security statement on the final key after error correction then takes the form that sender and receiver manage to obtain a key, which they share with a probability $1-\gamma$, and for which the entropy change is below a tolerable value Δ_{tol} with a probability $1-\alpha$. As shown in [10], the values of α and γ go to zero exponentially with the length of the key. At the same time, Δ_{tol} can be made exponentially small as well as long as the total gain of secure bits is positive. The last condition takes the form

$$N_{\text{gain}} = n_{\text{sif}}\left[1-\tau_1(\overline{\epsilon})\right] - n_{\text{sif}} f\ \left[1 - I_{AB}(\overline{\epsilon})\right]\ . \tag{2}$$

The first term describes the length of the final key after privacy amplification. The quantity τ_1 has been calculated in [10]. We assume as relevant case here that the error reconciliation protocol corrects errors using a bi-directional protocol, e. g. that by Brassard and Salvail [13]. Then we have

$$\tau_1(\overline{\epsilon}) \leq \begin{cases} \log\left(1+4\overline{\epsilon}-4\overline{\epsilon}^2\right) & \text{for } \overline{\epsilon}\leq 1/2 \\ 1 & \text{for } 1/2 \leq \overline{\epsilon} \end{cases}\ . \tag{3}$$

where $\overline{\epsilon}$ is in the limit of long keys and neglection of ambiguous detector signals equal to the observed error rate of the experiment. The second term in (2) comes from the fact that we have to employ secret bits to perform error correction without leaking additional information to an eavesdropper. The minimum number of bits to be exchanged this way is given by $1 - I_{AB}\left(\overline{\epsilon}\right)$. The Shannon information I_{AB}, shared between Alice and Bob on the noisy binary channel with error rate $\overline{\epsilon}$, is given in general by

$$I_{AB}(\overline{\epsilon}) = 1 + \overline{\epsilon}\log_2\overline{\epsilon} + (1-\overline{\epsilon})\log_2(1-\overline{\epsilon})\ . \tag{4}$$

This limit is, however, hard to achieve. Therefore I include a correction factor $f\geq 1$. We know that the error correction protocol by Brassard and Salvail works with $f\leq 1.35$ for an error rate up to 15%.

3 Multi-photon signals

Presently there are no single photon sources available. Therefore other sources are used to approximate the BB84 signals. This is done by inserting weak coherent pulses into the BB84 polarization modes. The weak coherent pulses contain on average less than one photon, but with finite probability they contain two or more photons. It has been pointed out before that this leads to potential security hole for quantum key distribution [14–16]. Another practical signal source uses parametric downconversion to create a signal state in the BB84 signal modes conditioned on a successful detection of one photon of the created photon pairs. As shown in [16], and illustrated by the examples of Section 4, this can improve the performance of the set-up although the basic security problem remains.

In [16] we have argued that any signal created by the two methods mentioned above can be thought of as a *mixture* of Fock states due to the lack of a phase reference. This leads to a description of the signals as the phase average over the signals states, which are Fock diagonal states. (Note that a phase reference exists in the "Plug and Play" scheme [18]. However, a phase randomization of each dim pulse will bring this scheme back into the context of Fock diagonal signal states.) In both cases we can think, therefore, for each signal as carrying zero, one, or more photons.

A signal carrying two or more photons can reveal its information to an eavesdropper without causing errors in Bob's detector. This is true since one can split off one photon from a signal without disturbing the polarization of either component.

The quantity τ_1 is given by the expected a posteriori collision probability p_c as $\tau_1 = 1 + \frac{1}{n}\log_2(p_c)$. The collision probability is given in terms of the a-posteriori probability distribution $p(X|M)$ for the key prior to privacy amplification. It is the same probability distribution which has been used in to define the change of Shannon entropy (1). In these terms, the collision probability is defined as $p_c = \langle \sum_{x\in X} p(x|M)^2 \rangle_M$. If all signals arriving at Bob's site stem from single photon signals sent by Alice, then the total collision probability for a key of length n is given by [10]

$$p_c = \left(p_c^{(1)}(\overline{\epsilon}^{(1)})\right)^n \tag{5}$$

with the collision probability on a single photon signal estimated by

$$p_c^{(1)}(\overline{\epsilon}^{(1)}) \leq \begin{cases} \frac{1}{2} + 2\overline{\epsilon}^{(1)} - 2\left(\overline{\epsilon}^{(1)}\right)^2 & \text{for } \overline{\epsilon}^{(1)} \leq 1/2 \\ 1 & \text{for } 1/2 \leq \overline{\epsilon}^{(1)} \end{cases} . \tag{6}$$

Here $\overline{\epsilon}^{(1)}$ is the error rate *on the single photon signals*. If we can give a bound that at most m out of the n_{sif} signals stem from multi-photon signals, then we obtain a bound on the collision probability as

$$p_c \leq \left(p_c^{(m)}\right)^m \left(p_c^{(1)}\right)^{n-m} = \left(p_c^{(1)}\right)^{n-m} . \tag{7}$$

For each multi-photon signal the collision probability is given by $p_c^{(m)} = 1$ since here Eve knows the signal. It follows that we have to shorten the key during privacy amplification by the fraction

$$\tau_1^{(m)}(\overline{\epsilon}^{(1)}) = 1 + \frac{n-m}{n}\log_2 p_c^{(1)}(\overline{\epsilon}^{(1)}) . \tag{8}$$

We can obtain such a bound using a theorem by Hoeffding [19] which can be used to relate the expected number of multi-photon signals $\overline{m}$ to the actually created number of such signals m for a key of length n with some probability. The statement is that the inequality

$$|\overline{m} - m| \leq \delta n \tag{9}$$

for some chosen value of δ holds with a probability $P > 1 - \exp\left(-2n\delta^2\right)$. This means, that we can choose $m = \overline{m}$ since we deal in this article only with the limit of large keys. For experimental realizations, however, one has to keep an eye on the choice of δ which might be rather small. Then n has to be quite large to obtain a reasonable value for P. More discussion concerning the statistical issue can be found in [10].

Given the characterizations of the signal source to send signals with zero, one, or more than one photon with probability S_0, S_1, S_m respectively, and for Bob to receive a signal with probability p_{exp}, we can analyze the security of this scheme. For that we have to assign the probabilities that the received signals stem from zero, one, or multi-photon signals respectively corresponding to the fractions R_0, R_1, R_m. There are three different regimes characterized by $p_{exp} > S_1 + S_m$, which would correspond to a detection scheme with many dark counts, $p_{exp} < S_m$, which cannot lead to a secure communication, and $S_1 + S_m > p_{exp} > S_m$, which describes the normal range of operation. We need to discuss only this last scenario. In this case Eve will split all multi-photon signals and eavesdrop on some of the single-photon signals while blocking the remaining single-photon signals. This corresponds to the assignment

$$R_0 = 0 \,, \tag{10}$$

$$R_1 = \frac{p_{exp} - S_m}{p_{exp}} \,, \tag{11}$$

$$R_2 = \frac{S_m}{p_{exp}} \,. \tag{12}$$

We have to assume that all errors are caused by eavesdropping on single-photon signals. Therefore the error rate on these signal $\bar{\epsilon}^{(1)}$ is given via the total expected error rate $\bar{\epsilon}$ as

$$\bar{\epsilon}^{(1)} = \frac{\bar{\epsilon}}{R_1} = \bar{\epsilon} \frac{p_{exp}}{p_{exp} - S_m} \,. \tag{13}$$

With these results we are in a position to calculate the creation of secure bits per time slot of the set-up. It is given from eqn. (2) as

$$G = \frac{1}{2} p_{exp} \left\{ 1 - \tau_1^{(m)} \left(\bar{\epsilon} \frac{p_{exp}}{p_{exp} - S_m} \right) - f \; \left[1 - I_{AB} \left(\bar{\epsilon} \right) \right] \right\} \,. \tag{14}$$

We insert the expressions for $\tau_1^{(m)}$ in the form

$$\tau_1^{(m)} = 1 + \frac{p_{exp} - S_m}{p_{exp}} \log_2 \left(1/2 + 2\bar{\epsilon} \frac{p_{exp}}{p_{exp} - S_m} - 2 \left(\bar{\epsilon} \frac{p_{exp}}{p_{exp} - S_m} \right)^2 \right) \,, \tag{15}$$

which follows from eqn. (8), and for I_{AB} (4), and we obtain the formula

$$\begin{aligned} G &= \frac{1}{2} p_{exp} \left\{ - \frac{p_{exp} - S_m}{p_{exp}} \log_2 \left[1/2 + 2\bar{\epsilon} \frac{p_{exp}}{p_{exp} - S_m} - 2 \left(\bar{\epsilon} \frac{p_{exp}}{p_{exp} - S_m} \right)^2 \right] \right. \\ & \left. \quad + f \; \left[\bar{\epsilon} \log_2 \bar{\epsilon} + (1 - \bar{\epsilon}) \log_2 (1 - \bar{\epsilon}) \right] \right\} \,. \end{aligned} \tag{16}$$

In this form, the gain function is a function of the measured rate of arriving signals p_{exp}, the observed error rate $\bar{\epsilon}$, and of the source characteristics S_m. Note that the remaining source characteristics S_1 will be implicitly contained in p_{exp}. Given the source characteristics, a model for the channel and for the detection, one can model p_{exp} to optimize the gain rate over a parameter space.

4 Examples

To illustrate the implications of the obtained expression for the gain rate (16) I calculate the optimal gain rate as a function of the distance for set-ups taken from the literature. In these demonstrations we have to model the signal source, the detectors in their efficiency and dark count rate, and the channel. The error rate is modeled taking into account an error rate e proportional to the number of signals, which corresponds, for example, to errors due to misalignments or polarization diffusion. Additionally, detector dark counts of the total detection unit at a rate d_B per time slot are taken into account. The loss is modeled by the transmission efficiency of the channel,

$$\eta_T = 10^{-\frac{\alpha l + c}{10}}$$

with the loss coefficient α, the length of the channel l, and a constant loss (in dB) of Bob's detection set-up. On top of that, the finite detection efficiency of Bob's detector η_B is taken into account. In the examples, I will use values taken from two experiments performed at British Telecom. The first data come from an experiment performed by Marand and Townsend [20] in the second telecommunication window at 1.3 μm. The reported values are a detection efficiency $\eta_B = 0.11$, a darkcount rate $d_B = 10^{-5}$ while the fiber shows a loss of $\alpha = 0.38$ dB/km and the detection unit shows a loss of $c = 5$ dB. The alignment error is given by $e = 0.8$ % of the signals. The second experiment performed by Townsend [21] at 0.8 μm is characterized by $\eta_B = 0.5$, $d_B = 5 \times 10^{-8}$, $\alpha = 2.5$ dB/km, and a loss in Bob's detection unit of $c = 8$ dB. With these two set of data I simulate the expected gain of secret bits in the limit of large keys. I do so for four simulations:

WCP 1.3 Use of weak coherent states at 1.3 μm,

WCP 0.8 Use of weak coherent states at 0.8 μm,

PDC 1.3/1.3 Parametric downconversion over the 1.3 μm network with the trigger photon at Alice's site detected by the 1.3 μm detector, and

PDC 0.8/1.3 Parametric downconversion over the 1.3 μm network with the trigger photon at Alice's site detected by the 0.8 μm detector.

For all simulations I assumed the efficient bi-directional error correction protocol by Brassard and Salvail [13]. The rates are shown in Fig. 1.We clearly see that all those schemes have a cut-off in distance. The reason for that is that one has to decrease the average photon number in the signals with increasing loss of the channel in order to keep the multi-photon probability low. (We certainly need to have $p_{exp} - S_m \geq 0$.) On the other hand, a decrease of the photon number will lead to a decrease of the number of expected signals so that the dark counts of Bob's detector begin to dominate the error rate. There is always an optimal photon number for the signals, but we encounter an upper limit on the loss which still leads to a positive gain rate. Extensive discussions and bounds on this tolerable loss are given in [16].

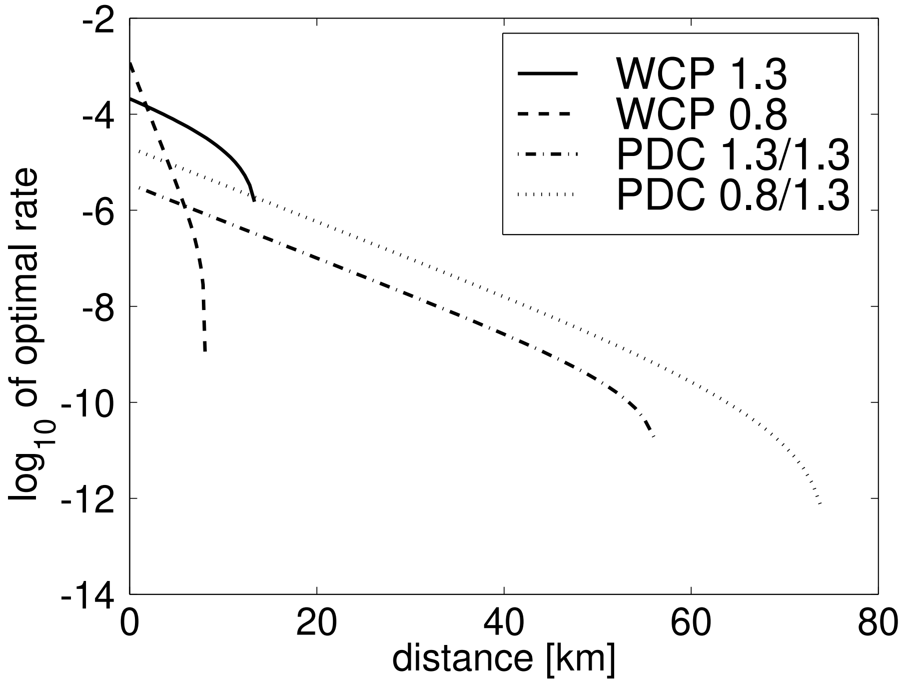

Fig. 1. Simulation of gain rate of secure bits per time slot as function of the covered distance.

5 Discussion

It still remains to be shown how to generate and distribute a secure key in practice so that this transmission is unconditionally secure. However, as an intermediate step, it is possible to do so with technology available today, if we accept the restriction to eavesdropping action on individual signals only. With view to current difficulties to manipulate coherently a few qubits, this restrictions seems acceptable. For the future, we can hope to unite the approach of Mayers with the current approach to find a proof of unconditional security for a *practical* realization. We find that QKD which is secure against individual attacks, can be achieved using current technology. However, the distance covered by these experiments is limited by the detector characteristics and is lower than usually assumed. For example, I found in my calculations that the photon number optimizing the total gain rate of secure bits is of the magnitude of the order of the total loss (fiber loss, loss in Bob's detector, and detection efficiency in Bob's detector). This value is in most cases considerably lower than the value used in the actual experiments. This can be partly explained by a different notion of security used by the authors. It is therefore important to clearly state the assumptions underlying any security statement given for a QKD experiment. An important approach in that direction is that used in [17, 22] where the additional assumptions is made that the detection efficiency of Bob's detector and the loss of Bob's detection unit cannot be circumvented by Eve. This assumption has to be justified by the actual set-up of Bob's detection unit, which is not the case for current experiments. In that case, the reported rate of gained secure bits and the distance covered exceed the values given in the estimate (16).

Acknowledgment I would like to thank Steve Barnett, Mohammed Bourenanne, Mila Dušek, Ondřej Haderka, Martin Hendrych, Hitoshi Inamori, Anders Karlsson, Tal Mor, Eugene Polzik, Louis Salvail, Christian Schori, Jens-Lykke Sorensen, and Paul Townsend for all the discussions during the long-standing research into the security of practical quantum cryptography.

References

[1] C. H. Bennett, G. Brassard: *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (New York,1984) pp. 175–179

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

[3] D. Bruß, N. Lütkenhaus: *quant-ph/9901061*

[4] Special issue on quantum information, *J. Mod. Opt.* **41** (1994)

[5] B. Huttner, A. K. Ekert: *J. Mod. Opt.* **41** (1994) 2455

[6] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, A. Peres: *Phys. Rev. A* **56** (1997) 1163

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

[8] N. Lütkenhaus: *Phys. Rev. A* **54** (1996) 97

[9] B. Slutsky, R. Rao, P. C. Sun, Y. Fainman: *Phys. Rev. A* **57** (1998) 2383

[10] N. Lütkenhaus: *Phys. Rev. A* **59** (1999) 3301

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

[12] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, T. Mor: *quant-ph/9801022*

[13] G. Brassard, L. Salvail: in *Advances in Cryptology - EUROCRYPT '93*, *Lecture Notes in Computer Science* **765** (Springer, 1994) p.410

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

[15] H. P. Yuen: *Quantum Semiclassic. Opt.* **8** (1996) 939

[16] G. Brassard, N. Lütkenhaus, T. Mor, B. Sanders: unpublished

[17] M. Dušek, O. Haderka, M. Hendrych: unpublished

[18] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, N. Gisin: *Applied Phys. Lett.* **70** (1997) 793

[19] W. Hoeffding: *J. Am. Stat. Assoc.* **58** (1963) 13

[20] C. Marand, P. T. Townsend: *Opt. Lett.* **20** (1995) 1695

[21] P. D. Townsend: *IEEE Photonics Technology Letters* **10** (1998) 1048

[22] M. Dušek, O. Haderka, M. Hendrych, Robert Myška: *Phys.Rev. A* (1999) to appear