

PACS numbers: 03.67.Dd; 03.67.Pp
DOI: 10.1070/QE2007v037n12ABEH013670

Quantum cryptography: individual eavesdropping with the knowledge of the error-correcting protocol

D.B. Horoshko

***Abstract*. The quantum key distribution protocol BB84 combined with the repetition protocol for error correction is analysed from the point of view of its security against individual eavesdropping relying on quantum memory. It is shown that the mere knowledge of the error-correcting protocol changes the optimal attack and provides the eavesdropper with additional information on the distributed key.**

Keywords: *quantum cryptography, quantum memory*.

In the last decade the criteria for unconditional security have been found for many quantum cryptography protocols, which provided their security from attacks of any type [1 – 3]. However, the criteria for security against the simplest and, therefore, most easily realised class of attacks – individual attacks, still attract considerable interest. This is explained by the fact that the security against such attacks is achieved at the much higher rate of key generation than the unconditional security.

The analysis of the security against individual attacks was based so far on the implicit assumption that the eavesdropper (Eve) performing a quantum measurement, which is a part of any eavesdropping process, does not obtain any advantage from the knowledge of the error-correcting protocol (ECP) applied by legitimate users (Alice and Bob) to generate identical keys [3, 4]. We show that generally this is not the case and *a priori* knowledge of ECP allows Eve to increase her information on the key even upon the individual attack.

We illustrate this by considering the simplest protocol of the quantum key distribution BB84 with the simplest ECP – the triple repetition protocol. Any quantum key distribution protocol consists of two stages: the data transmission and their classical processing. The data are transmitted by sending two-level systems (qubits) along a quantum channel. In commercial quantum cryptography devices, single photons are used as qubits and an optical fibre is used as the quantum channel. Recall the order of the quantum data transmission in the BB84 protocol [5]. One of the users (Alice) generates two random uniformly distributed bits, a and r. Depending on the result, she prepares a qubit in one of the four quantum states ($|0\rangle$, $|1\rangle$, $|\bar{0}\rangle$ and $|\bar{1}\rangle$). The two first and two last states are orthogonal in pairs, and the relation between the pairs of states is described by the expressions

$$|\bar{0}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tag{1}$$

$$|\bar{1}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle). \tag{2}$$

The states $|0\rangle$ and $|\bar{0}\rangle$ correspond to $a = 0$, and the states $|1\rangle$ and $|\bar{1}\rangle$ – to $a = 1$. For $r = 0$, Alice uses the basis $\{|0\rangle, |1\rangle\}$ and for $r = 1$ – the basis $\{|\bar{0}\rangle, |\bar{1}\rangle\}$. The created state is transmitted along the quantum channel to another user (Bob), who generates a random bit r' and, depending on its value, adjusts the device for measuring the qubit state in the basis $\{|0\rangle, |1\rangle\}$ for $r' = 0$ or the basis $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ for $r' = 1$. Bob obtains the value of the bit b equal to 0 if the measurement gives $|0\rangle$ or $|\bar{0}\rangle$, and the bit value equal to 1 if the measurement gives $|1\rangle$ или $|\bar{1}\rangle$. It is obvious that in the absence of transmission and measurement errors, bits a and b should coincide each time when bits r and r' coincide.

This procedure is repeated $2n + 2\delta$ times, where n and δ are natural numbers and $1 \ll \delta \ll n$. As a result, the so-called raw data sequences are produced: sequences of bits a for Alice and bits b for Bob. Then, the classical processing of the raw sequences begins, which is coordinated by transmission along a classical channel (for example, a local network), which is not secure from the passive eavesdropping.

The first stage of classical processing – the basis reconciliation, involves the disclosure of the sequence of bits r and r', which Alice and Bob send to each other along the classical transmission channel. After that both sides retain only the bits of the raw sequence corresponding to the coincidence of r and r'. The number of such bits will be $n + \delta$ (asymptotically in the limit of large n) and they will form the so-called sifted sequences.

At the second stage – the error estimate, Alice generates a random set of δ numbers from 1 to $n + \delta$ and transmits this set to Bob together with the values of bits of the sifted sequence, having the corresponding numbers. Bob finds the values of bits with the corresponding numbers in his sifted sequence and compares these values with the values of Alice's bits. Based on this comparison, Bob calculated the fraction Q of noncoinciding bits in a random sampling of length δ. This fraction is accepted by both sides as the

D.B. Horoshko B.I. Stepanov Institute of Physics, National Academy of Sciences of Belarus, prosp. Nezavisimosti 68, 220072 Minsk, Belarus; e-mail: dhoroshko@rambler.ru

Received 5 July 2007
Kvantovaya Elektronika **37** (12) 1105 – 1108 (2007)
Translated by M.N. Sapozhnikov

estimate of the bit error rate in the quantum transmission channel. The bits involved in the random sampling are removed from sifted sequences, which acquire as a result the length n of bits.

The third stage of classical data processing involves the error correction. For this purpose, the sides exchange some information along the classical transmission channel. The error correction process can be either one-sided, when only Alice sends information to Bob (or vice versa), or two-sided, when the interactive information exchange occurs. We will restrict our consideration here to one-sided ECPs, which are simplest for analysis.

According to the Shannon theorem of the standard theory of information [6], the number of bits, which Alice should send to correct Qn errors in the Bob's sifted key of length n, is asymptotically equal to $nh_2(Q)$, where

$$h_2(x) = -x\log_2 x - (1-x)\log_2(1-x) \tag{3}$$

is the binary Boltzmann H function. The number of transmitted bits in a particular ECP will be somewhat larger. After the ECP execution, the users obtain identical (with a high probability) corrected sequences of length n of bits. The ECP should be developed taking into account that all the data being transmitted reach the eavesdropper Eve, which can passively intercept the classical channel. Thus, some information I_{ec} on the corrected key reaching Eve is related to each ECP. This information is 'summed' by Eve with the information I_{qt} obtained during eavesdropping in the quantum channel at the quantum transmission stage. This summation is not a simple arithmetic operation because the information I_{qt} can be quantum rather than classical, which is possible for Eve having the quantum memory.

The last stage of the classical data processing is the privacy amplification procedure. This procedure involves the mapping by hashing of the corrected sequence of length n on the final sequence of length $m \leqslant n$, which can be already used as the cryptographic key [7]. The length m of this key is given by the special theory in which the upper limit of the classical information I_{qt+ec} on the corrected sequence of Alice and Bob, which is accessible to Eve, is used as the input parameter.

If Eve has no quantum memory capable of storing the quantum information during the time between the quantum transfer and classical data processing, the expression for the length of the secret key is especially simple. In this case, the information of Eve on the sifted sequence I_{qt} of Alice is simply a number (mutual information according to Shannon), which is estimated by simulating the eavesdropping process. For the error rate Q, the information of Bob on the sifted sequence of Alice is $I_B = n[1- h_2(Q)]$. It follows from the Csiszar–Korner theorem [8] that there exits the codes which asymptotically provide the obtainment of

$$m = I_B - I_{qt} \tag{4}$$

bits of the key, Eve's information about this key asymptotically tending to zero. These codes combine in fact the error-correcting codes and the privacy amplification procedure.

There also exists the possibility of another eavesdropping strategy lying beyond the scope of applicability of the Csiszar–Korner theorem, which is provided by the presence of a sufficiently durable quantum memory of Eve. In this paper, we consider how information on the ECP allows Eve to sum efficiently the quantum (I_{qt}) and classical (I_{ec}) information. Note that the usefulness of the quantum memory for eavesdropping is well-known and has been studied in detail from the information-theoretical point of view [9]. However, this approach does not consider, first, particular information eavesdropping protocols and, second, assumes that Eve has not only the quantum memory but also in fact a quantum computer providing collective measurements of many qubits. In this paper, we considered the case when Eve has the quantum memory but not a quantum computer, which is sufficient for the individual attack. The efficient use of information obtained at the error-correcting stage with such a limited arsenal of interception means has not been considered so far. Such an approach seems all the more reasonable because progress in the field of quantum memory is strongly ahead of that in the field of quantum computers. In addition, this approach is based on the constructive description of the eavesdropping process rather than merely proves its possibility.

To illustrate the eavesdropping principle, we consider one of the simplest ECPs – the triple repetition protocol, which operates in the following way. Alice divides randomly the zeroes of her sifted sequence into blocks containing three bits each. She performs the same procedure with ones. All the blocks are arranged randomly. Alice communicates to Bob the bit numbers in each triplet and writes their values as bits of her corrected sequence. Bob selects from his sifted sequence the bits with corresponding numbers, selects the value that is represented by the majority in the triplet and writes it into his corrected sequence. For a low error rate, the corrected sequences of Alice and Bob will be almost identical. The difference can appear only in cases when one or all three bits in one block contain errors, which gives the error probability

$$Q_B = 3(1-Q)Q^2 + Q^3 \tag{5}$$

in the corrected sequence. For the typical error rate in the sifted sequence equal to 10^{-2}, the error rate in the corrected sequence will be of the order of 10^{-4}. If such an error rate is unsatisfactory, another ECP can be used after the triple repetition protocol to achieve the required error rate.

Let us now describe the actions of Eve aimed at the information eavesdropping [4]. Eve attaches the probe four-level system A in the initial state $|\chi\rangle_A$ to each qubit X propagating in the quantum channel and performs the unitary transformation U with both systems:

$$|0\rangle_X|\chi\rangle_A \to \sqrt{1-Q}\,|0\rangle_X|A\rangle_A + \sqrt{Q}\,|1\rangle_X|B\rangle_A, \tag{6}$$

$$|1\rangle_X|\chi\rangle_A \to \sqrt{1-Q}\,|1\rangle_X|C\rangle_A + \sqrt{Q}\,|0\rangle_X|D\rangle_A, \tag{7}$$

where the states $|A\rangle_A$ and $|C\rangle_A$ of the four-level probe belong to one two-dimensional subspace H_{AC} and the states $|B\rangle_A$ and $|D\rangle_A$ – to another two-dimensional subspace H_{BD}, and $H_{AC}\perp H_{BD}$ and Q is the error rate introduced by Eve into the quantum channel. It is assumed traditionally that all the errors in the quantum channel are related to the eavesdropping. In addition,

$$\langle A|C\rangle = \langle B|D\rangle = \cos\varphi = 1 - 2Q. \tag{8}$$

It is easy to show that the unitary transformation U described above can be also written in the form

$$|\bar{0}\rangle_X|\chi\rangle_A \to \sqrt{1-Q}\,|\bar{0}\rangle_X|A'\rangle_A + \sqrt{Q}\,|\bar{1}\rangle_X|B'\rangle_A, \tag{9}$$

$$|\bar{1}\rangle_X|\chi\rangle_A \to \sqrt{1-Q}\,|\bar{1}\rangle_X|C'\rangle_A + \sqrt{Q}\,|\bar{0}\rangle_X|D'\rangle_A, \tag{10}$$

where the states $|A'\rangle_A$ and $|C'\rangle_A$ also belong to one two-dimensional subspace H'_{AC} and the states $|B'\rangle_A$ and $|D'\rangle_A$ – to another two-dimensional subspace H'_{BD}, and $H'_{AC} \perp H'_{BD}$. In addition,

$$\langle A'|C'\rangle = \langle B'|D'\rangle = \cos\varphi = 1 - 2Q. \tag{11}$$

Having performed the interaction, Eve allows the qubit X to propagate further along the quantum channel and places the probe system A to the quantum memory. After Eve performs this procedure with all $2n + 2\delta$ qubits, her quantum memory contains the same number of probe systems. At the basis reconciliation stage, Eve intercepts the sequences of bits r and r' in the classical channel and discards all the probe systems for which bits in these sequences are different. At the error estimate stage, Eve intercepts the numbers of δ bits of the random sampling in the classical channel and discards the corresponding probe systems. Then, she applies the unitary transformation V to each probe system to which the condition $r = r' = 1$ corresponds. This transformation $V|Z'\rangle = |Z\rangle$ maps the primed states on the unprimed states, where Z takes the values A, B, C, and D. Then, each probe system is subjected to the projective measurement distinguishing the orthogonal subspaces H_{AC} and H_{BD}. The detection of the subspace H_{AC}, whose probability is $1 - Q$, means that this bit in the sequence of Bob is the same as that in the sequence of Alice. The detection of the subspace H_{BD}, whose probability is Q, means that this bit in the sequence of Bob is erroneous. In the latter case, Eve applies to the probe system the unitary transformation W satisfying the relation $W|B\rangle = |A\rangle$, $W|D\rangle = |C\rangle$. As a result, before the error correction stage, Eve has the sequence of n systems, each of them being either in the state $|A\rangle$ or the state $|C\rangle$ corresponding to 0 or 1 in the sifted sequence of Alice.

The standard approach to the analysis of individual eavesdropping is based on the assumption that at the instant of eavesdropping Eve measures her probe systems. It has been proved [4] that in this case the optimal strategy for Eve will be the projective measurement of each probe system in the symmetrically straddling basis, i.e. in the basis consisting of the orthogonal vectors $\{|\zeta_0\rangle$ and $|\zeta_1\rangle\}$ in the subspace H_{AC} making equal angles γ with vectors $|A\rangle$ and $|C\rangle$ (Fig. 1). Having obtained the result $|\zeta_0\rangle$, Eve writes 0 into her intercepted sequence, and having obtained $|\zeta_1\rangle$, she writes 1. The error probability q upon determining the bit value from Fig. 1 and (8) is

$$q = \sin^2\gamma = \frac{1}{2}\left[1 - \sqrt{1-(1-2Q)^2}\right]. \tag{12}$$

At the error correction stage, Eve intercepts the data on the division of the sifted sequence into blocks and divides her intercepted sequence into bit triplets in the same way. Then, like Bob, she selects the value, which is represented by the majority in the triplet, and writes it into her corrected

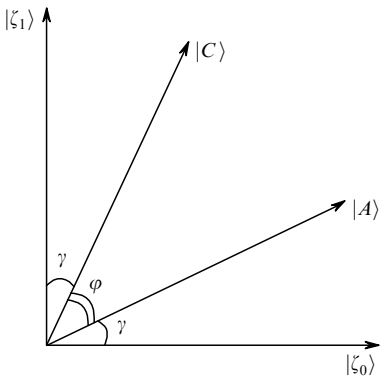

Figure 1. Measurement basis used to distinguish the states $|A\rangle$ and $|C\rangle$ upon the standard individual attack against the BB84 protocol.

sequence. The error probability of Eve in the determination of the block value is $q_B = 3(1-q)q^2 + q^3$, and her information on the corrected sequence (per bit) is

$$I_E^{(s)} = 1 - h_2(q_B). \tag{13}$$

The optimality of the standard attack is provided by the fact that measurements in the straddling basis are optimal for distinguishing two nonorthogonal pure states. Let us now assume that Eve preserved her probe systems in the quantum memory until the error correction stage. Having intercepted in the classical channel the data on the division of the sifted sequence into blocks, she divides her probe systems in the same way. Now each of the blocks of the three probe systems is either in the state $|A\rangle|A\rangle|A\rangle$ or the state $|C\rangle|C\rangle|C\rangle$. It is known that these two states can be best distinguished in the class of individual measurements in the basis making different angles with vectors $|A\rangle$ and $|C\rangle$ [10]. It is reasonable to assume that the optimal individual eavesdropping will be related to the same basis.

Consider the projective measurement of the subspace H_{AC} in the basis $\{|\xi_0\rangle, |\xi_1\rangle\}$, for which the relations $\langle\xi_0|A\rangle = \cos\alpha$, $\langle\xi_1|C\rangle = \cos\beta$ are fulfilled, and in the general case $\alpha \neq \beta$ (Fig. 2). The angle α will be used as a parameter specifying the basis, and $\beta = \pi/2 - \varphi - \alpha$. Eve subjects all the three probe systems in the block to the above-described measurement. Having obtained the result $|\xi_0\rangle$ or $|\xi_1\rangle$, Eve writes 0 or 1 into her intercepted sequence.

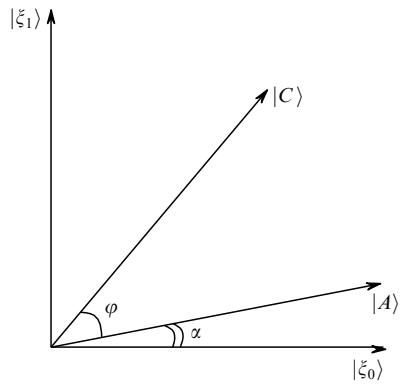

Figure 2. Measurement basis used to distinguish the states $|A\rangle$ and $|C\rangle$ upon the individual attack (optimised taking into account the error-correcting protocol) against the protocol BB84.

The probability of the correct determination of the value 0 is $p_0 = \cos^2\alpha$. The error probability of determining 1 is $q_1 = \cos^2(\alpha+\varphi)$. Then, Eve assigns the value 0 to a bit of the corrected sequence only in the case when all the three bits in the block are zero. Otherwise, the value 1 is assigned to this bit. Thus, the probability of correct determination of the bit value upon the interception of the Alice's block containing three zeroes is p_0^3, while the error probability upon the interception of a block containing three unities is q_1^3. Correspondingly, the information of Eve on the corrected sequence is

$$I_{\mathrm{E}}^{\alpha} = 1 - [h_2(p_0^3) + h_2(q_1^3)]/2\,. \tag{14}$$

The maximum value of this expression for the angle α varying from 0 to $\pi/4 - \varphi/2$

$$I_{\mathrm{E}}^{(\mathrm{m})} = \max_{\alpha} I_{\mathrm{E}}^{\alpha} \tag{15}$$

can be easily calculated numerically. This is the maximum information that Eve can obtain about the corrected sequence for the optimal choice of the measurement basis corresponding to an angle α_{m}. Figure 3 presents the dependences of $I_{\mathrm{E}}^{(\mathrm{m})}$ on Q together with the information $I_{\mathrm{E}}^{(\mathrm{s})}$ of Eve for the standard attack and the information $I_{\mathrm{B}} = 1 - h_2(Q_{\mathrm{B}})$ of Bob on the corrected sequence of Alice. One can clearly see that the eavesdropping taking the ECP into account is more informative.

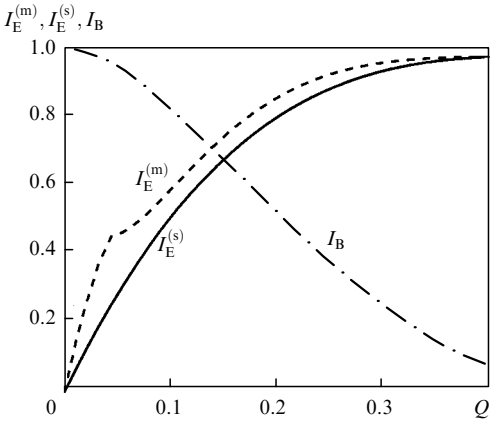

Figure 3. Dependences of the amount I of intercepted information on the corrected key on the error rate Q in the sifted key upon the individual attack against the protocol BB84 with the triple repetition error-correcting code.

Note that to perform an attack optimised taking the ECP into account, there is no need for Eve to retain the probe systems until the error correction stage if she knew the ECP already at the quantum transmission stage. Immediately after the basis reconciliation stage, she can measure her systems in the basis corresponding to the angle α_{m} and postpone the determination of the block values until the error correction stage. Thus, the optimisation uses not the correcting information itself but only the knowledge of the specific choice of the ECP. This gives the method for security against the attack. In quantum key distribution systems, we can recommend the ECP coding with the help of a special short key. For example, before the beginning of a quantum transmission, the N-fold repetition protocol can be agreed, while the value of N will be communicated only at the error correction stage. As a result, because different values of N correspond to different angles α_{m} of the optimal measurement, Eve will not be able to optimise her measurement without using a more durable quantum memory.

Thus, we have shown that during the attack on a quantum cryptography line, the eavesdropper knowing the error-correcting protocol chosen by the user can optimise his attack to increase the amount of intercepted information. This possibility has been demonstrated by the example of the attack of the simplest class – the individual attack, and it has been shown that this attack does not require additional resources of the quantum memory compared to the standard individual attack. The further consideration of individual eavesdropping taking into account the ECP based on the Shannon calculations of information is presented in [11].

Acknowledgements. This study was supported by the INTAS and the European Commission (Specific Targeted Research Project EQUIND, Engineered Quantum Information in Nanostructured Diamond, funded by the FP6 IST directorate as Contract No. 034368).

References

1. Kilin S.Ya. *Usp. Fiz. Nauk*, **169**, 507 (1999).
2. Kilin S.Ya., in *Progress in Optics* (Amsterdam: Elsevier, 2001) Vol. 42, p. 1.
3. Gisin N., Ribordy G., Tittel W., Zbinden H. *Rev. Mod. Phys.*, **74**, 145 (2002).
4. Fuchs C.A., Gisin N., Griffiths R.B., Niu C.-S., Peres A. *Phys. Rev. A*, **56**, 1163 (1997).
5. Bennett C.H., Brassard G., in *Proc. of IEEE Intern. Conf. on Computers, Systems and Signal Processing* (New York: IEEE, 1984) p. 175.
6. Shannon C.E. *Bell Syst. Techn. J.*, **27**, 379 (1948).
7. Maurer U.M. *IEEE Trans. Inf. Theory*, **39**, 733 (1993).
8. Csiszar I., Korner J. *IEEE Trans. Inf. Theory*, **24**, 339 (1978).
9. Koenig R., Maurer U., Renner R. *IEEE Trans. Inf. Theory*, **51**, 2391 (2005).
10. Fuchs C.A. Preprint of Los-Alamos National Laboratory; quant-ph/9601020.
11. Horoshko D. *Proc. SPIE Int. Soc. Opt. Eng.*, **6726**, 67263Q (2007).