Quantum key distribution with several intercept–resend attacks via a depolarizing channel

Mustapha Dehmani, Mohamed Errahmani, Hamid Ez-Zahraouy and Abdelilah Benyoussef

LMPHE (URAC 12), Faculté des Sciences, Université Mohammed V-Agdal, BP 1014, Rabat, Morocco
E-mail: ezahamid@fsr.ac.ma

Received 21 February 2012
Accepted for publication 29 May 2012
Published 25 June 2012
Online at stacks.iop.org/PhysScr/86/015803

Abstract
The disturbance effect of a depolarizing channel on the security of the quantum key distribution of the four-state BB84 protocol, with multiple sequential intercept–resend attacks of many eavesdroppers, has been studied. The quantum bit error rate and the mutual information are computed for an arbitrary number $N$ of eavesdroppers. It is found that the quantum error rate decreases with increasing the depolarizing parameter $p$ characterizing the noise of the channel. For $p < 0.165$, there exists a special value $p_0$ of $p$ below which the information is secure and otherwise the information is not secure. The value of $p_0$ decreases with increasing the number of attacks. In contrast, for $p \geq 0.165$, the information is not secure independently of the number of eavesdroppers. Phase diagrams corresponding to the secure—unsecure information are also established.

PACS numbers: 89.20.Ff, 42.25.Ja, 42.25.Kb

1. Introduction

The paths of cryptography and quantum data processing came to a meeting point when Bennett and Brassard [1] developed the first quantum key distribution (QKD) known as the BB84 protocol. This protocol allows two participants to exchange a random secret key that can be used perfectly for protected communications. Many researchers proposed formal pieces of evidence for the QKD safety [2, 3]. The QKD has already come into practice, and the first prototype was developed in 1989 by Bennett et al [4–6]. In spite of its experimental success, several problems are worth noting regarding the deployment of this technology outside of laboratories [7]. One of these factors is the too short distances reached by prototypes; another factor is the depolarizing channel and its effect in the presence of eavesdroppers [8]. In a previous work, we have analyzed the QKD with several intercept and resend attacks [9] and with several cloning attacks [10]. In recent years, the most important problem with practical quantum communication has been the security of information under the effect of disturbances or quantum noise. In general, losses of information may be due to several factors such as the attenuation of photon signal due to a weak pulse laser [11], the detector efficiency mismatch due to high dark counts [12] and the depolarizing channel noise effect [13]. In the first two cases the amount of loss of information, in the absence of eavesdropping, depends strongly on the length of the channel. Consequently, one can easily study the dependence of the quantum bit error rate (QBER) and the mutual information as a function of the length of the channel, even in the presence of eavesdroppers.

However, in the case of the Pauli channel [13], the disturbance depends only on the depolarizing parameter $p$ and on the length of the channel [14, 15]. In recent years, it has been studied from different points of view: theoretical and experimental [11, 14–17].

Our aim in this paper is to study the security of information of the four-state BB84 protocol under the effect of both channel noise and many eavesdroppers with intercept–resend attacks.

The paper is organized as follows. The protocol is detailed in section 2. Section 3 is devoted to the results and discussion, while section 4 is reserved for the conclusion.
2. The Protocol

The BB84 protocol requires two different phases: the first is through the quantum channel physics with one-way, and the second is through a bidirectional traditional ideal channel authenticated [1]. The quantum depolarization channel we will study in this paper leaves intact a qubit \( |\psi\rangle \) with probability \( (1 - p) \) or applies one of the Pauli matrices \( \sigma_i \) with probability \( p/3 \) for each one [13, 14], which is mathematically considered as an operator \( T_p \) defined by

\[
T_p (|\psi\rangle \langle \psi|) = (1 - p) |\psi\rangle \langle \psi| + \sum_{i=1}^{3} \frac{p}{3} \sigma_i |\psi\rangle \langle \sigma_i|.
\]  

(1)

We denote by \( P^o(x_B/x_A) \) the conditional probability that Bob receives a polarized photon \( x_B = 0, 1 \) with respect to that Alice sends a polarized photon \( x_A = 0, 1 \) under the channel noise effect, namely

\[
P^o(0/0) = P^o(1/1) = 1 - \frac{2p}{3}.
\]

(2)

and

\[
P^o(1/0) = P^o(0/1) = \frac{2p}{3}.
\]

(3)

Equations (2) and (3) show that, in the absence of eavesdroppers, the information safety depends only on the depolarizing channel parameter \( p \) with a quantum bit error \( \delta = \frac{2p}{3} \).

In the presence of one eavesdropper within intercept and resend attacks, it is difficult to know on which side of the channel the Pauli transformations corresponding to the channel noise take place. Between Alice and Eve or between Eve and Bob, on the other side, the model we used does not allow us to know with certainty whether the photon sent by Alice is disturbed, under the channel noise, before or after being intercepted by Eve. Physically, these two situations are completely different, and lead to different results. For example, in the case of one eavesdropper, the two situations are considered but with different probabilities \( q \) and \( 1 - q \), respectively, as has been used in [8].

Moreover, in particular cases for which the position of Eve is closer to Alice and the position of Eve is closer to Bob, we consider \( q = 0 \) and \( q = 1 \), respectively.

In the case of many sequential intercept–resend attacks, a state sent by Alice can follow the ways of transmission according to figure 1, where the photon loses its polarization, due to the channel noise, in one of the space intervals located between Alice and Eve, or between Alice and Bob, with the respective probabilities \( q_1, q_2, \ldots, q_l, \ldots, q_{n+1} \) and \( \sum_{i=1}^{n+1} q_i = 1 \).

Alice sends a sequence of photons to Bob by choosing randomly to send 1 or 0. Bob chooses randomly to measure the received photon. Between them, there are \( N \) independent eavesdroppers \( E_i \) (\( i = 1, \ldots, N \)) who intercept sequentially the photon sent by Alice with the respective probabilities \( \omega_i \). The eavesdropper \( E_1 \) intercepts the photon sent by Alice with the probability \( \omega_1 \), measures its polarization and sends it to \( E_2 \); then each eavesdropper \( E_i \) intercepts with the probability \( \omega_i \) the photon sent by \( E_{i-1} \), measures its polarization by choosing randomly a base and returns them to \( E_{i+1} \), in the state of polarization that she has measured and so on until the eavesdropper \( E_N \) who sent its intercepted photon to Bob. However, in the place of the photon that they did not measure, they put randomly 0 or 1 in their chains of bits. Then, Alice and Bob exchange in a traditional way the bases that they used; they remove in their chain of bits those exchanged in different bases. For studying the security of information exchanged between two honest parties Alice and Bob, we introduce the notion of mutual information. In this case, we compute the mutual information between Alice and Bob and the mutual information between Alice and every eavesdropper \( E_m \).

3. Results and discussion

Moreover, it is demonstrated that the binary Shannon entropy allows finding the impact on the information safety [18–20]. However, the mutual information \( I(A, B) \) and \( I(A, E_m) \) between Alice and Bob, and between Alice and the \( m \)th eavesdropper \( E_m \) are given, respectively, as follows:

\[
I(A, B) = 1 + P_{AB}(0/0) \log_2(P_{AB}(0/0))
+ P_{AB}(1/0) \log_2(P_{AB}(1/0)),
\]

(4)

\[
I(A, E_m) = 1 + P_{AE_m}(0/0) \log_2(P_{AE_m}(0/0))
+ P_{AE_m}(1/0) \log_2(P_{AE_m}(1/0)),
\]

(5)

where \( P(x_B/x_A) \) and \( P(x_{E_m}/x_A) \) are the conditional probabilities between Alice and Bob and between Alice and the \( m \)th eavesdropper. Before the establishment of the general expressions of these probabilities to an arbitrary eavesdropper number \( N \), let us consider the simple case of \( N = 1 \).

In this case, Alice sends a polarized photon \( 0 \) or \( 1 \) to Bob. This photon can undergo a depolarization channel according to equation (1) between Alice and Eve with a probability \( q_1 \) or between Alice and Eve with a probability \( 1 - q_1 \).

Hence, we denote hereafter by \( P_{AB}(0/0) \) and \( P_{AE}(0/0) \) the conditional probabilities, in the case of a perfect channel (\( p = 0 \)), that Bob (Eve) receives a polarized photon \( x_B \) (\( x_E \)) with respect to that Alice sends a polarized photon \( x_A = 0, 1 \), namely, \( P_{AB}(0/0) = 1 - \frac{2p}{3} \) and \( P_{AE}(0/0) = \frac{1}{2} + \frac{p}{2} \). However, using equations (2) and (3),
the conditional probabilities $P_{AB}(x_B/x_A)$ between Alice and Bob, under the effect of both channel noise and eavesdropper attacks, are given as follows:

$$P_{AB}(0/0) = P^*(0/0) P^0_{AB}(0/0) + P^*(0/1) P^0_{AB}(0/1)$$
$$= \left(1 - \frac{2p}{3}\right) \left(1 - \frac{\omega}{4}\right) + \frac{3p\omega}{6}, \quad (6)$$

$$P_{AE}(0 \mid 0) = \left( P^0_{AE}(0/0) P^*(0/0) + P^0_{AE}(0/1) P^*(0/1) \right) q_1 + P^0_{AE}(0/0) \left( 1 - q_1 \right) = \frac{1}{2} + \frac{\omega}{4} - \frac{p\omega q_1}{3} \quad (7)$$

with $P_{AB}(0/1) = P_{AB}(1/0) = 1 - P_{AB}(0/0)$, $P_{AB}(1/1) = P_{AB}(0/0)$, $P_{AE}(1/1) = P_{AE}(0/0)$ and $P_{AE}(0/1) = P_{AE}(1/0) = 1 - P_{AE}(0/0)$.

The above results can be generalized to the case of an arbitrary number $N$ of eavesdroppers as follows:

$$P_{AB}(0/0) = \left( \sum_{k=0}^{n} \sum_{i_1, \ldots, i_k=1}^{n} \prod_{j=1}^{k} (1 - \omega_{i_j}) \prod_{l=k+1}^{n} \omega_{i_l} \right) \times \left(1 - \frac{4p}{3}\right) + \frac{2p}{3}, \quad (8)$$

$$P_{AEm}(0/0) = \left( \prod_{j=1}^{i} (1 - \omega_{i_j}) \prod_{l=k+1}^{n} \omega_{i_l} + \frac{1 - \omega_m + 2p\omega_m}{2} \sum_{i=1}^{m} q_i + 1 - \frac{\omega_m}{2} \sum_{k=0}^{m-1} \prod_{j=1}^{i} (1 - \omega_{i_j}) \prod_{l=k+1}^{n} \omega_{i_l} \left( 1 - \sum_{i=1}^{m} q_i \right) \right), \quad (9)$$

with $P_{AB}(1/0) = P_{AB}(0/1) = 1 - P_{AB}(0/0)$, $P_{AB}(1/1) = P_{AB}(0/0)$, $P_{AEm}(1/0) = P_{AEm}(0/0)$ and $P_{AEm}(1/1) = P_{AEm}(0/0)$.

Finally, the lost information between Alice and Bob is given by

$$I_{\text{lost}} = I(A, E) + H(\delta), \quad (10)$$

where $I(A, E)$ corresponds to the maximum of the mutual information intercepted by all the eavesdroppers, namely

$$I(A, E) = \max_{m=1, N} \left[ I(A, E_m) \right] \quad (11)$$

and $H(\delta) = -(1 - \delta) \log_2 (1 - \delta) - \delta \log_2 \delta$ is the binary Shannon entropy corresponding to the amount of lost information under the channel noise, in the absence of any external eavesdropper attack. Hence, the error probability $P_{err}$ is given by

$$P_{err} = \sum_{x_A \neq x_B} \left[ P_{AB}(x_A, x_B) \right]_{p_{\neq 0} \neq 0} - P_{AB}(x_A, x_B) \right]_{p_{\neq 0} = 0} \quad (12)$$

The QBER due to both channel noise and external attacks is the value of the error probability $P_{err}$ for which $22-24$

$$I(A, B) = I(A, E) + H(\delta). \quad (13)$$

For $P_{err} < Q_{\text{BER}}$, $I(A, E) + H(\delta) < I(A, B)$, then the information is secure, while it is not secure for $P_{err} > Q_{\text{BER}}$ for which $I(A, E) + H(\delta) > I(A, B)$.

Equation (8) shows that the amount of information received by Bob is independent of the stochastic parameter $q$ governing in which region in the channel the depolarization of the photon occurs. In contrast, equation (9) shows that the amount of the intercepted information by any eavesdropper $E_m$ depends strongly on the regions located between Alice and $E_m$, where the photon can lose its polarization with different probabilities $q_1, q_2, \ldots, q_m$. Hence, the mutual information is computed numerically for $N = 1, 2$ and 3, where the eavesdropper attack probabilities $\omega_0$ are independent. For $N = 1$, the behavior of the QBER as a function of the depolarizing parameter $p$ is shown in figure 2(a). It is clear that the quantum error decreases with increasing $p$ and depends also on the coefficient $q_1 = q$ that means the dependence of the amount of the intercepted information by Eve on his position in the channel; that is, the intercepted information depends on the region in which depolarization of the photon between Alice and Eve or between Eve and Bob occurs (figure 2(b)). It is clear that the amount of lost information

\[ \text{(Figure 2)} \]
increases with decreasing $q_i$, which means that the amount of information intercepted by Eve becomes very important when depolarization of the photon between Eve and Bob and not between Alice and Eve occurs. Besides, the amount of lost information increases with increasing the depolarizing parameter $p$, passes through a maximum and decreases for a sufficiently large value of $p$. A phase diagram showing the region in the $(p, \omega)$ plane where the information is secure is given in figure 3. It is found that, for a fixed value of the attack probability $\omega$, there is a special value of $p = p_{\text{tr}}$ at which a secure–unsecure transition occurs. Hence, for $p < p_{\text{tr}}$, the amount of lost information is less than that received by Bob, which means that the information is secure. In contrast, for $p > p_{\text{tr}}$, the information is not secure.

To better understand the influence of sequential attacks by three eavesdroppers on the security of the information, we have established numerically the phase diagram in the space parameter $(\omega_1, \omega_2, \omega_3)$, showing a transition between secure and unsecure information for $q_i = q = 1/(N+1)$ and several values of $N$. Now we investigate the security phase diagram (figure 5) and the behavior of the quantum bit error (figure 6) in the particular case corresponding to an arbitrary number of eavesdroppers intercepting the photon with identical

**Figure 3.** Phase diagram in the $(p, \omega)$ plane showing the transition between secure and unsecure information for $N = 1$ and $q_1 = 1/2$.

**Figure 4.** Phase diagram in the space parameter $(\omega_1, \omega_2, \omega_3)$ showing the transition between secure and unsecure information for $N = 3$ and $q_1 = q_2 = q_3 = q_4 = 1/4$ with (a) $p = 0.05$ and (b) $p = 0.1$.

**Figure 5.** Phase diagram in the $(p, \omega)$ plane showing the secure–unsecure transition in the case of $\omega_i = \omega (i = 1, \ldots, N)$ and $q_i = q = 1/(N+1)$ and different values of $N$.

**Figure 6.** The behavior of the quantum bit error as a function of the depolarizing parameter $p$ for $\omega_i = \omega (i = 1, \ldots, N)$ and $q_i = q = 1/(N+1)$ and several values of $N$. 
probabilities \( \omega_i = \omega \), but without sharing the results of their measures. The phase diagram established in figure 5 shows that the secure area decreases with increasing the number of eavesdroppers since the amount of intercepted information increases with \( N \). On the other hand, it is clear from figure 6 that the quantum error depends strongly on the number of eavesdroppers for small depolarizing parameter values, while this dependence is weak for sufficiently large values of \( p \), especially near \( p = 0.165 \).

4. Conclusion

We have studied the effect of both channel noise and many sequential intercept–resend attacks on the security of information in the BB84 protocol. We have shown that the quantum error decreases with increasing the number of sequential attacks and/or the depolarizing parameter. For a fixed depolarizing parameter \( p \), the security of information becomes weak with increasing the number of eavesdroppers, which leads to a secure–unsecure transition at a special number of attacks. This number decreases with increasing the \( p \).

References

[1] Bennett C H and Brassard G 1984 Proc. IEEE Int. Conf. on Computer, Systems and Signal Processing (Bangalore, India) (New York: IEEE Press) p 175
[2] Mayers D 2001 J. ACM 48 351
[3] Biham E, Boyer M, Boykin P O, More T and Roychowdhury V 2000 J. Cryptol. 19 381
[4] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 J. Cryptol. 5 28
[5] Hughes R J, Morgan G L and Peterson C G 2000 J. Mod. Opt. 47 2
[6] Muller A, Zbinden H and Gisin N 1995 Nature 378 449
[7] Lo H-K 2000 Phys. World 13 17
[8] Ben Slamen I, Trabesli O, Rezig H, Bouallegue R and Bouallegue A 2007 J. Comput. Sci. 3 424
[9] Ez-Zahraouy H and Benyoussef A 2009 Int. J. Mod. Phys. B 23 4755
[10] Dehmani M, Ez-Zahraouy H and Benyoussef A 2010 J. Comput. Sci. 6 684
[11] Scarani V, Acin A, Ribordy G and Gisin N 2004 Phys. Rev. Lett. 92 057901
  Fred Fung C-H, Tamaki K and Lo H-K 2006 Phys. Rev. A 73 012337
[12] Makarov V, Anisimov A and Skaar J 2006 Phys. Rev. A 74 022313
  Makarov V, Anisimov A and Skaar J 2008 Phys. Rev. A 78 019905
[13] Adami C and Cerf N J 1997 Phys. Rev. A 56 3470
[14] Bruss D, Fuoro L, Macchiavello C and Palma G M 2000 J. Mod. Opt. 47 325
[15] Scarani V, Pasquiniucci H B, Cerf N J, Dusek M, Lutkenhaus N and Peev M 2009 Rev. Mod. Phys. 81 1301
[16] Bennett C H, DiVincenzo D P and Smolin J A 1997 Phys. Rev. Lett. 78 3217
[17] Bennett C H, Sher P W, Smolin J A and Thapliyal A V 1999 Phys. Rev. Lett. 83 3081
[18] Shor P W and Preskill J 2000 Phys. Rev. Lett. 85 441
[19] Tamaki K, Koashi M and Imoto N 2003 Phys. Rev. Lett. 90 167904
[20] Agnolini S 2007 PhD Thesis Universite Pierre et Marie Curie Paris
[21] Daoud M and Ez-Zahraouy H 2011 Phys. Scr. 84 045018
[22] Kronberg D A and Molotkov S N 2009 Laser Phys. 19 10
[23] Branciard C, Gisin N, Kraus B and Scarani V 2005 Phys. Rev. A 72 032301
[24] Bocquet A, Alleaume R and Leverrier A 2012 J. Phys. A: Math. Theor. 45 025305