Journal of Theoretical and Applied Information Technology
31st May 2017. Vol.95. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

QUANTUM KEY DISTRIBUTION THROUGH AN ANISOTROPIC DEPOLARIZING QUANTUM CHANNEL

[1*] MUSTAPHA DEHMANI, [1]EL MEHDI SALMANI, [1]HAMID EZ-ZAHRAOUY, [1]ABDELILAH BENYOUSSEF

[1] Laboratoire de Magnétisme et de Physique des Hautes Energies Faculté des Sciences, Université Mohammed V-Agdal, Rabat, Morocco
*Corresponding author: dehmani01@yahoo.fr

ABSTRACT

Quantum cryptography is one of the major applications of quantum information theories. However, the Quantum key distribution (QKD) introduced by Bennett and Brassard in 1984 which is known as BB84 protocol, is used to obtain a secure random cryptographic secret key between the expediting Alice and the designating Bob and to detect the presence of eavesdroppers on the quantum channel. This channel is not always perfect; it often undergoes a quantum depolarizing channel which is a model for noise in quantum systems. In this work we study the depolarizing effect with an anisotropic probabilities of Bit-Flip, Phase-Flip and Bit-Phase-Flip in the presence of an eavesdropper for the two methods of attacks, cloning attack and intercept and resend attack, also we prove that the phase flip probability act strongly on the exchanged information safety.

Keywords: *Noise, Depolarizing channel, Eavesdropper, Attack, Phase flip probability*

1. INTRODUCTION

There exist various protocols of (QKD) [1, 2]. We were interested here by known original protocol under the name of BB84 [3]. The protocol will allow Alice and Bob to share a series of random bits. They have one-way quantum channel no sedentary of Alice towards Bob and authenticated bidirectional traditional channel. Other protocols use much attenuated states laser, while taking a discrete measurement. We quote for example protocols DPS (Differential Phase Shift) [4], where information is coded on the successive phases of the impulses, but also protocols with a frequency coding [5, 6,7], and protocols with temporal coding [8, 9]. A protocol in which information is coded over the time of detection of the photons of is developed elsewhere within Thalès Research & Technology France [10]. The (QKD) was already established in practice. The first prototype, developed in 1989 by Bennett and Brassard, [11]. An eavesdropper Eve can know nothing about the key secretes of Alice and Bob. Indeed, several evidence of safety was presented for this protocol, but each one has disadvantages. [12] [13] [14]. It is very important to announce that the quantum channel has properties basically different from the classical channel owing to the principle of superposition of quantum mechanics and non-cloning theorem [15].In a previous work, we have investigated the quantum key distribution with several intercept and resend attacks [16] and with several cloning attacks [17], also we have studied the case of quantum key distribution with several attacks via a depolarizing channel [18-19] and partially non-orthogonal basis states[20].

It is important to remember that in a classical computation, just the transformation bit flip $0 \leftrightarrow 1$ which can impact the transmission, however in a quantum computation; the existence of superposition states brings also the possibility of other basic errors for a single qubit. They are the phase flip and the bit-phase flip. The first changes the phase of the state, and the latter combines phase and bit flips. In this paper we shoes to study the effect of noisy quantum channels specially the depolarizing channel, the effect of bit flip, phase flip and the combined bit and phase flip in the presence of one eavesdropper in the case of intercept and resend attack and cloning attack. The model of noisy quantum channel which is mathematically considered as an operator T_p. The qubit remains intact with the probability $1-p$, while errors are acting on the qubit with probability p. The errors can be one of three types

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

or all types, the bit flip with the probability p_x, the phase flip with the probability p_z and the combined bit-phase flip with the probability p_y.

We suppose that: $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ (1)

Applying the no depolarizing channel:

$$|\psi\rangle \xrightarrow{1-p} |\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (2)$$

Applying the bit flip:

$$|\psi\rangle \xrightarrow{p_x} \sigma_x|\psi\rangle = \alpha|1\rangle + \beta|0\rangle \quad (3)$$

Applying the phase flip:

$$|\psi\rangle \xrightarrow{p_z} \sigma_z|\psi\rangle = -\alpha|0\rangle + \beta|1\rangle \quad (4)$$

Applying the combined bit-phase flip:

$$|\psi\rangle \xrightarrow{p_y} \sigma_y|\psi\rangle = -\alpha|1\rangle + \beta|0\rangle \quad (5)$$

Where σ_x, σ_y, σ_z are the Pauli matrices and .

We consider $p = p_x + p_y + p_z$ (6)

$$T_p(|\psi\rangle) = (1-p)|\psi\rangle\langle\psi| + p_x\sigma_x|\psi\rangle\langle\psi|\sigma_x + p_y\sigma_y|\psi\rangle\langle\psi|\sigma_y + p_z\sigma_z|\psi\rangle\langle\psi|\sigma_z \quad (7)$$

$$T_p(|0\rangle) = (1-p_x-p_y)|0\rangle\langle 0| + (p_x+p_y)|1\rangle\langle 1| \quad (8)$$

$$T_p(|1\rangle) = (1-p_x-p_y)|1\rangle\langle 1| + (p_x+p_y)|0\rangle\langle 0| \quad (9)$$

In the absence of eavesdroppers the information safety depends only from the depolarizing channel, and only the channel effect which generates errors; in this case the quantum error is $Q_{err} = \delta = p_x + p_y$, moreover it's proved that the binary Shannon entropy makes it possible to find the impact on the information safety [21,22,23].

The presence of Eavesdropper is a factor which constitutes source of errors.

For studying the security of information exchanged between tow honest parties Alice and Bob we introduce the notion of mutual information and in this way we calculate the mutual information between Alice and Bob and the mutual information between Alice and the eavesdropper.

$$I(A,B) = 1 + P_{AB}(0/0)Log_2(P_{AB}(0/0)) + P_{AB}(1/0)Log_2(P_{AB}(1/0)) \quad (10)$$

$$I(A,E) = 1 + P_{AE}(0/0)Log_2(P_{AE}(0/0)) + P_{AE}(1/0)Log_2(P_{AE}(1/0)) \quad (11)$$

Another important parameter to study security of a quantum cryptography protocol is secure information (or secret information) given by this equation:

$$I_S = I(A,B) - I(A,E) - H(\delta) \quad (12)$$

We compute also the Error probability P_{err} given by the expression (13) in the case of intercept and resend attack, and expression (14) in the case of cloning attack.

$$P_{err} = \sum_{x_A,x_B} \left| P_{AB}(x_A,x_B)|_{\omega=0} - P_{AB}(x_A,x_B)|_{\omega\neq 0} \right| \quad (13)$$

$$P_{err} = \sum_{x_A,x_B} \left| P_{AB}(x_A,x_B)|_{\theta=0} - P_{AB}(x_A,x_B)|_{\theta\neq 0} \right| \quad (14)$$

We will also deduce the quantum error $Q_{err} = P_{err}$ for which $I(A,B) = I(A,E) + H(\delta)$.

Our study consists in checking the effect of all parameters of the depolarizing channel in for quantum key distribution in the presence of eavesdropper.

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. MODEL

In the case of cloning attack, Alice sends a photon in a quantum state. Eve will create a clone of each transmitted photon and returns a photon (presumed identical) to Bob. Let us notice that Eve did not make yet of measurement and did not choose base. Then, Alice and Bob communicate their bases and keep only those which they have in common. Eve, having listened to that, can thus each time choose good base to measure her photons

However I, the case of intercept and recend attack; Alice sends a sequence of photons to Bob while choosing randomly to send 1 or 0. Bob chooses randomly to measure the received photon. Between them, is an Eavesdropper, Eve, who intercept certain photons with a probability ω, measurement their polarization by choosing a base

Journal of Theoretical and Applied Information Technology
31st May 2017. Vol.95. No 10

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

randomly and returns them to Bob in the state of polarization which it measured. At the place of the photons which Eve does not measure, she puts randomly 0 or 1 in her sequence of bits. Then, Alice and Bob exchange in a classical way the bases which they used, and then they remove from their sequence of bits the states for which they used different bases. In the remaining bits, they take a small sample of bits and count the error count which they have, although they chose the same base to measure the photon. From this error count, they can determine the maximum quantity of information which Eve has.

On the quantum channel, noise can disturb the transmission of the photons; these noises can be placed between Alice and Eve with a probability q or between Eve and Bob with a probability $1 - q$.

2.1 The Mutual information between Alice and Bob: $I(A,B)$

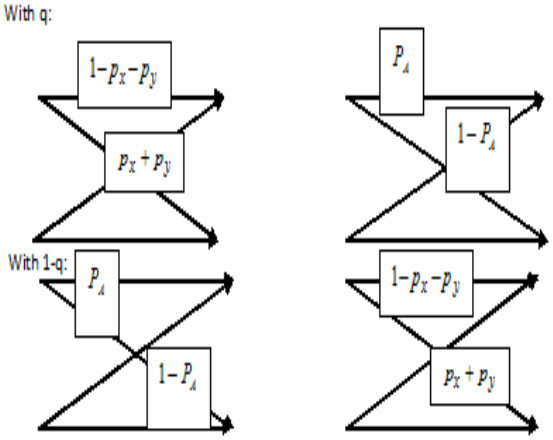


Figure. 1: Analysis Model (Alice – Bob)

With $P_A = (1+\cos(\theta))/2$ in the case of cloning attack and $P_{AB}(0/0)$ will be in the form (15)

$$P_{AB}(0/0) = P_{AB}(1/1) = (1-p_x-p_y)(1+\cos(\theta))/2 + (p_x+p_y)(1-\cos(\theta))/2 \quad (15)$$

Also, in the case of intercept and resend attack $P_A = 1-\omega/4$ and $P_{AB}(0/0)$ will take the form (16)

$$P_{AB}(0/0) = P_{AB}(1/1) = \left(1-p_x-p_y\right)\left(1-\frac{\omega}{4}\right) + (p_x+p_y)\frac{\omega}{4} \quad (16)$$

$$P_{AB}(0/1) = P_{AB}(1/0) = 1 - P_{AB}(0/0) \quad (17)$$

2.2 The Mutual information between Alice and E : $I(A,E)$

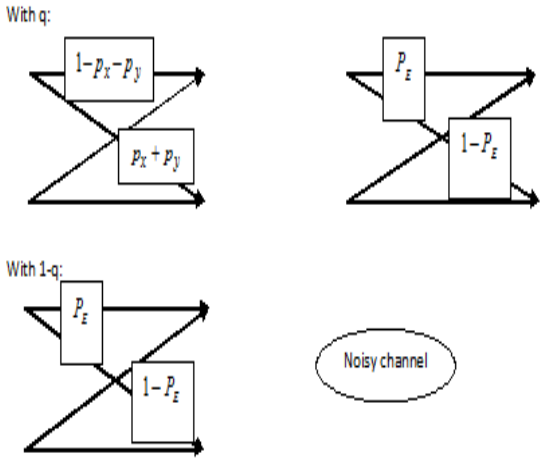


Figure. 2: Analysis model in the presence of eavesdropper (Alice – Eve)

With $P_E = (1+\sin(\theta))/2$ for the cloning attack and $P_{AE}(0/0)$ is written as (18).

$$P_{AE}(0/0) = P_{AE}(1/1) = (1+\sin(\theta))/2 - q(p_x+p_y)(1+\sin(\theta))/2 + q(p_x+p_y)(1-\sin(\theta))/2 \quad (18)$$

Also, in the case of intercept and resend attack

$P_E = 1/2 - \omega/4$ and

$$P_{AE}(0/0) = P_{AE}(1/1) = \left(\frac{1}{2}+\frac{\omega}{4}\right) - q(p_x+p_y)\left(\frac{1}{2}+\frac{\omega}{4}\right) + q(p_x+p_y)\left(\frac{1}{2}-\frac{\omega}{4}\right) \quad (19)$$

$$P_{AE}(0/1) = P_{AE}(1/0) = 1 - P_{AE}(0/0) \quad (20)$$

3. RESULT AND DISCUSSION

The first remark is that the phase flip probability p_z is not present in the formula: there is no phase flip but this parameter acts implicitly on information safety seen that the depolarizing parameter is the sum of probabilities related to the three components of the channel noise $p = p_x + p_y + p_z \le 1$, moreover the phase flip is always present in the channel effect in spite of presence eavesdropper.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The phase diagram established in the sp parameter (p , θ) represented in Fig.3 sh the transition line between secured and unsecu area in the presence of eavesdropper for diffe values of the phase flip probabilities compare case of isotropic probabilities of bit flip, phase and combined phase and bit flip. The n important result deduced from this diagram is the secured Area increase by increasing the pl flip probabilities.

Also the figure.4 shows the quantum error a function of the depolarizing parameter p different values of the phase flip probabilities. clear that the variations of phase flip probabil influence strongly on quantum error.

A few examples of the secret information I_s between honest parties as a function of the depolarizing parameter p are giving in Figure.5, it can be seen that the phase flip probability act on the secret information I_s and more the phase flip probability increases more information circulated on the channel is secured .

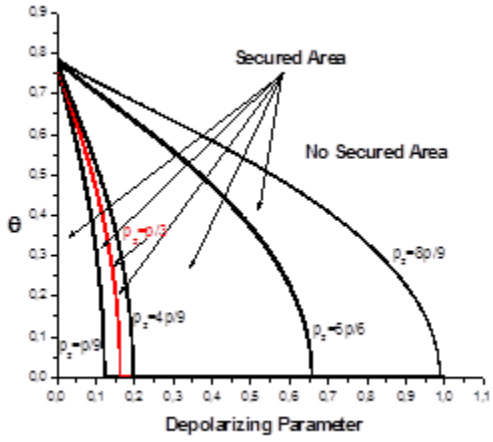


Figure. 3: Phase Diagram In The (p , θ) Showing The Transition Between Secured And Unsecured Information For Different Values Of The Phase Flip Probabilities.

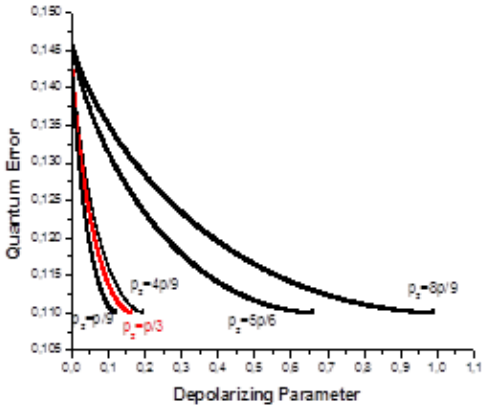
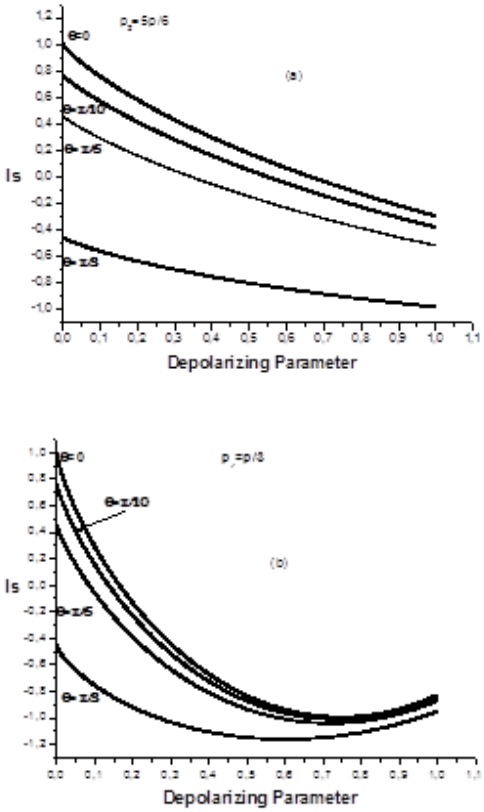


Figure. 4: The Behavior Of The Quantum Error As A Function Of The Depolarizing Parameter p For Different Values Of The Phase Flip Probabilities



ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

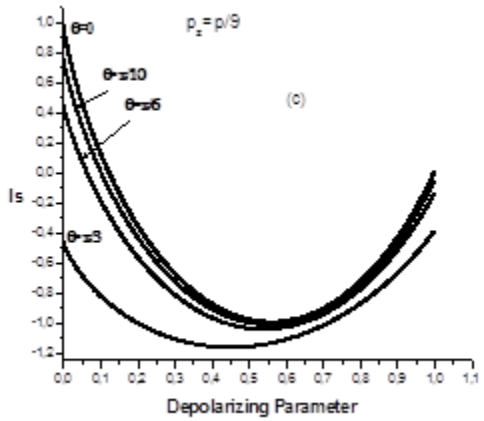


Figure. 5: Examples Of The Secret Information I_s *Between Honest Parties As A Function Of The Depolarizing Parameter* p *(A) For The Phase Flip Probabilities Of* $p_z = \frac{5p}{6}$*,(B) For The Phase Flip Probabilities Of* $p_z = \frac{p}{3}$ *And (C) For The Phase Flip Probabilities Of* $p_z = \frac{p}{9}$

By analogy, and noting that the formulas of mutual information in the case of cloning attack and intercept and resend attack do not differ too much; It can be concluded that even for intercept and resend attack the phase flip probability acts in an identical way on the security of the information.

4. CONCLUSION

We studied the quantum key distribution with cloning and intercept and resend attacks via an anisotropic depolarizing channel and showed that information safety depends strongly on the phase flip probability in spite of the type of the attack. Also the security of the information conveyed on the channel increases by increasing the phase flip probability.

REFRENCES:

[1] Charles H. Bennett,"Quantum cryptography using any two non-orthogonal states ", Phys. Rev. Lett. 68, 3121, May 1992.

[2] Artur Ekert, "Quantum cryptography based on Bell's theorem", Phys. Rev. Lett., vol. 67, no 6, pp. 661-663, août 1991.

[3] Charles H. Bennett et Gilles Brassard. Quantum cryptography : Public-key distribution and coin tossing. Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179, 1984.

[4] K. Inoue, E. Waks et Y. Yamamoto," Differential Phase Shift Quantum Key Distribution", Phys. Rev. Lett. 89, 037902, June 2002 .

[5] P. C. Sun, Y. Mazurenko et Y. Fainman," Long-distance frequency-division interferometer for communication and quantum cryptography", Opt. Lett. Vol. 20, Issue 9, pp. 1062-1064, (1995)

[6] Y. T. Mazurenko, R. Giust et J. P. Goedgebuer, "Spectral coding for secure optical communications using refractive index dispersion", Optics Comm, Vol.133, pp.87-92 (1997).

[7] Jean-Marc Mérolla, Yuri Mazurenko, Jean-Pierre Goedgebuer, and William T. Rhodes "Single-Photon Interference in Sidebands of Phase-Modulated Light for Quantum Cryptography" , Phys. Rev. Lett. 82, 1656, February 1999.

[8] Thierry Debuisschert and William Boucher," Time coding protocols for quantum key distribution",Phys. Rev. A 70, 042306, 8 October 2004.

[9] D. Stucki, N. Brunner, N. Gisin, V. Scarani et H. Zbinden, "Fast and simple one-way quantum key distribution", Applied Physics Letters 87, 194108 (2005).

[10] William Boucher and Thierry Debuisschert, "Experimental implementation of time-coding quantum key distribution", Phys. Rev. A 72, 062325 December 2005.

[11] Charles Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin, "Experimental quantum cryptography", Journal of Cryptology, vol. 5, no 1, pp. 3 -28, (1992).

[12] Dominic Mayers. Unconditional security in quantum cryptography. Journal of the ACM (JACM), Vol 48, Issue 3, pp.351-406, May 2001.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[13] Eli Biham, Michel Oscar Boykin, Tal Mor, and Vwani Roychowdhury "A proof of the security of quantum key distribution (extended abstract)",Proceedings of the thirty-second annual ACM symposium on Theory of computing, pp.715-724 (ACM, New York, 2000).

[14] Hoi-Kwong Lo et Hoi Fung Chau., "Unconditional security of quantum key distribution over arbitrarily distances", Science, vol. 283, pp. 2050 -2056, 1999.

[15] W. K. Wootters, and W. H. Zurek, "A Single Quantum Cannot be Cloned," Nature (London) 299, pp.802–803, (1982).

[16] H. Ez-Zahraouy and A. Benyoussef, " Quantum Key Distribution With Several Intercept and Resend attacks" Int. J. Mod. Phys. B 23 , 4755 (2009).

[17] M. Dehmani, H. Ez-Zahraouy and A. Benyoussef, "Quantum Cryptography with Several Cloning Attacks", Journal of Computer Science 6 (7), pp. 684-688, (2010).

[18] M. Dehmani, H. Ez-Zahraouy , M.Errahmani and A. Benyoussef, "Quantum key distribution with several intercept–resend attacks via a depolarizing channel" Phys. Scr. 86 (2012).

[19] M. Dehmani, H. Ez-Zahraouy and A. Benyoussef, "Quantum Key Distribution with Several Cloning Attacks via a Depolarizing Channel", Journal of Russian Laser Research, Volume 36, Issue 3, pp 228–236, May 2015.

[20] M. Dehmani, H. Ez-Zahraouy and A. Benyoussef, " Quantum key distribution with several intercepts and resend attacks with partially non-orthogonal basis states". Optik - International Journal for Light and Electron Optics, vol 125:2, pp.624-627, (2014).

[21] Peter W. Shor , and J. Preskill , "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Physical Review Letters 85, pp.441-444 (2000).

[22] K. Tamaki, M. Koashi, and N. Imoto, "Unconditionally Secure Key Distribution Based on Two Nonorthogonal States", Phys. Rev. Lett. 90, 167904 (2003).

[23] V. Scarani, Helle Bechmann-Pasquinucci, N.J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, "The security of practical quantum key distribution", Rev. Mod. Phys. 81, 1301, September 2009.