Journal of Computer Science 6 (7): 684-688, 2010
ISSN 1549-3636

Quantum Cryptography with Several Cloning Attacks

Mustapha Dehmani, Hamid Ez-Zahraouy and Abdelilah Benyoussef
Laboratory of Magnetism and High Energy Physics,
Faculty of Science, University Mohammed V-Agdal, Rabat, Morocco

Abstract: Problem statement: In a previous research, we investigated the quantum key distribution of the well known BB84 protocol with several intercept and resend attacks. In the present research, we studied the effect of many eavesdroppers cloning attacks of the Bennett-Brassard cryptographic protocol on the quantum error and mutual information between honest parties and information with sender for each eavesdropper. **Approach:** The quantum error and the mutual information were calculated analytically and computed for arbitrary number of cloning attacks. Our objective in this study was to know if the number of the eavesdroppers and their angle of cloning act on the safety of information. **Results:** It was found that the quantum error and the secured/no secured transition depend strongly on the number of eavesdropper and their angle of attacks. The particular cases where all eavesdroppers collaborate were also investigated. **Conclusion:** Furthermore, the cloning attack's quantum error is lower than the intercept and resends attacks one, which means that the cloning attacks is the optimal one for arbitrary number of eavesdropper.

Key words: Quantum, cryptography, cloning, eavesdroppers

INTRODUCTION

The quantum mechanics is used by Wiesner (1983) to serve safety of information and he introduces the concept of quantum conjugate coding. Several theoretical and experimental works have been done in this area. However satisfactory proofs of the unconditional security have been developed (Christandl *et al*., 2004; Mayers, 1996; Shor and Preskill, 2000; Lo and Chau, 1999). Many experiment results have been for short distance (Bennett *et al*., 1992) and long distances (Huttner *et al*., 1995). Quantum cloning is one of method to measure information from input state. However several theoretical studies have been established, namely optimal universal quantum cloning (Brub *et al*., 1998). Pauli cloning machine of a quantum bit (Cerf, 2000) quantum copying beyond the no-cloning theorem (Buzek and Hillery, 1996) in a network (Buzek *et al*., 1997). The cloning of sequences of qubits encoded in the same basis has been studied with the six state BB84 protocols (Lamoureux *et al*., 2006).

The safety of BB84 (Bennett and Brassard, 1984) rests on the impossibility of the perfect cloning. If a eavesdropper has a perfect copying machine, it would be enough for him to copy the qubits that it intercepts, then to send a copy to the receiver and to keep the other until the transmitter and the receiver announce their bases of measurement. In impossibility of doing it, the eavesdropper can decide to copy the qubits in an optimal approximate way. It is thus essential for the transmitter and the receiver to know what eavesdropper can do of better like cloning and the consequences that has on the correlations which they measure to check the safety of their key, so the Cloning attack eavesdropping is an attack which makes it possible to obtain the minimum of secure information exchanged between a transmitter and a receiver called Alice and Bob. This type of attacks is very optimal compared to intercepts and resend attacks: The eavesdropper named Eve employs a unit operator U called cloning transform. This operator can approach the act of cloning which is impossible inside theory of quantum.

The goal of this study is to study the case of several eavesdroppers on a quantum channel. It is about a more real approach for Cloning attack which will act on the behavior of mutual information between Alice and Bob like the quantum error misses within the BB84 protocol. This study will be focused on two behaviors different from the eavesdroppers, the first relates to random eavesdroppers and the second relates to eavesdroppers which communicate between them and in this case we will see the relation between the quantum error probability and the number of eavesdroppers.

Corresponding Author: Mustapha Dehmani, Laboratory of Magnetism and High Energy Physics, Faculty of Sciences, University Mohammed V-Agdal, Rabat, Morocco

MATERIALS AND METHODS

Alice encodes each random bit into the polarization state of a single photon, selects randomly; one of bases from a set of two orthogonal or conjugates bases of a quantum bit (qubit). She sends randomly 1 or 0, with equal probability 1/2, to Bob. Bob measures each photon by selecting at random between two polarization analyzers. the mutual information between Alice and Bob can be described by a joint probability $P(x_A, x_B)$, where x_A and x_B are random variables representing the photon polarization state prepared by the sender (Alice) and the measurement results obtained by the receiver (Bob). However, $x_A = 0$ (1) if the photon emitted by Alice is polarized vertically (horizontally) and $x_B = 0$ (1) if the measured photon by Bob is polarized vertically (horizontally). Between them, a number N of eavesdropper $E_i (i = 1,\ldots,N)$, each eavesdropper E_i clone with a unitary cloning transform U such as:

$$U\left(|0\rangle_A|0\rangle_{E_i}\right) = |0\rangle_A|0\rangle_{E_i}$$

and

$$U\left(|1\rangle_A|0\rangle_{E_i}\right) = |1\rangle_A|1\rangle_{E_i}$$

In all what follows E_i will use U in the base y which will be definite as follows:

$$U\left(|0\rangle_{yA}|0\rangle_{yE_i}\right) = |0\rangle_{yA}|0\rangle_{yE_i}$$
$$U\left(|1\rangle_{yA}|0\rangle_{yE_i}\right) = \cos(\theta_i)|1\rangle_{yA}|0\rangle_{yE_i} + \sin(\theta_i)|0\rangle_{yA}|1\rangle_{yE_i}$$
$$\theta_i \in [0, \pi/2]$$

This θ_i is a parameter controls by E_i and measurement the force of the attack. After the cloning, E_i keeps the photon which belongs originally to its state space and to Bob the photon returns which belonged to the state space of Alice.

The mutual information between Alice and Bob:

$$I(A,B) = 1 + P_{AB}(0/0)\text{Log}_2(P_{AB}(0/0)) + P_{AB}(1/0)\text{Log}_2(P_{AB}(1/0))$$

$P_{AB}(x_B/x_A)$ is the conditional probability that Bob receive a photon polarized $x_B = 0,1$ with respect that Alice send a photon polarized $x_A = 0,1$. However, the probability that Bob receive a photon polarized vertically ($x_B = 0$) with respect that Alice sends a photon polarized vertically ($x_A = 0$) is given by:

$$P_{AB}(0/0) = P_{AB}(1/1) = \left(1 + \prod_{i=1}^{n}\cos(\theta_i)\right)/2 \text{ and } P_{AB}(1/0) = P_{AB}(0/1) = \left(1 - \prod_{i=1}^{n}\cos(\theta_i)\right)/2$$

The mutual information between Alice and the eavesdropper number m:

$$I(A,E_m) = 1 + P_{AE_m}(0/0)\text{Log}_2(P_{AE_m}(0/0)) + P_{AE_m}(1/0)\text{Log}_2(P_{AE_m}(1/0))$$

$P_{AE_m}(x_{E_m}/x_A)$, is the conditional probability that the eavesdropper intercept a photon polarized vertically (horizontally) (x_{E_m} =0,1) with respect that Alice send a photon polarized vertically (horizontally) (x_A = 0,1):

$$P_{AE_m}(0/0) = P_{AE_m}(1/1) = \left(1 + \prod_{i=1}^{m-1}\cos(\theta_i)\sin(\theta_m)\right)/2$$

$$P_{AE_m}(0/1) = P_{AE_m}(1/0) = \left(1 - \prod_{i=1}^{m-1}\cos(\theta_i)\sin(\theta_m)\right)/2$$

The lost information between Alice and Bob corresponds to the maximum information copied by the entire eavesdropper:

$$I(A,E) = \underset{i=1,m}{\text{Max}}[I(A,E_i)]$$

The error rate or the error probability P_{err} is given by:

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

The quantum error Q_{err} is the value of the error probability P_{err} for which I(A,B) = I(A,E). However, for $P_{err} < Q_{err}$, I(A,E) < I(A,B), while for $P_{err} > Q_{err}$, I(A,E) > I(A,B):

$$P_{err} = \left(1 - \prod_{i=1}^{n}\cos(\theta_i)\right)/2$$

In the particular case, where the eavesdroppers communicate between them:

$$P_{err} = \left(1 - \cos(\theta)^n\right)/2$$

While, in the case of alternating collaboration with alternating angles (θ_1,θ_2) the error probability takes two different form depending on the parity of the number of the eavesdropper. In the case of an even number of eavesdropper the error probability is given by:

$$P_{err} = \left(1 - \cos(\theta_1)^{n/2} \cos(\theta_2)^{n/2}\right) / 2$$

In the case of an odd number it is given by:

$$P_{err} = \left(1 - \cos(\theta_1)^{(n+1)/2} \cos(\theta_2)^{(n-1)/2}\right) / 2$$

RESULTS

We will study the variations of mutual information according to the number of the eavesdroppers and their angles of attack. Figure 1a shows the variations of the mutual information between Alice and Bob I(A,B) represented in green color and the mutual information I(A,E) intercepted by the Eavesdropper represented in red color as a function of the attack angles θ_1 and θ_2. The point of intersection of the curve I(A,B) and I(A,E) defines the secured-no secured transition for the various values of the angle of attack θ_2 from the second eavesdropper.

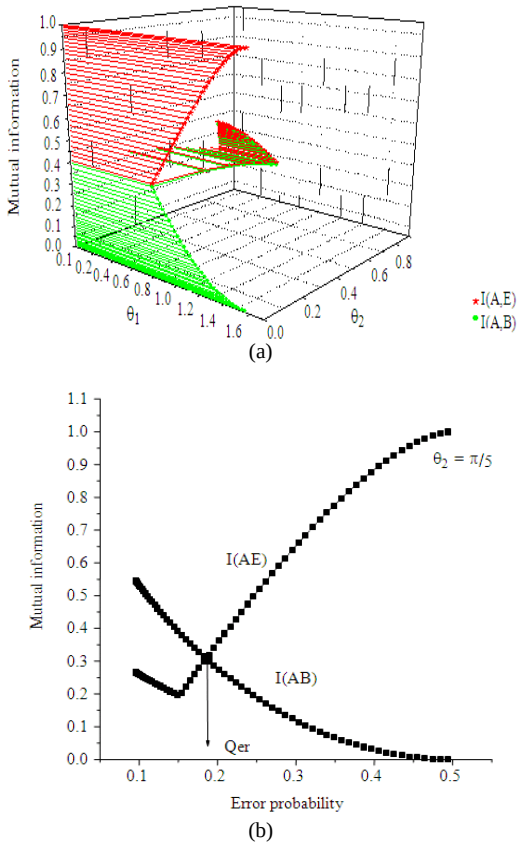

Fig. 1: The mutual information between honest parties I(A,B) and loosed information I(A,E) (a) as a function of the attack angles (θ_1,θ_2), (b) as a function of the error probability. Numerical results are obtained for N = 2 and $\theta_2 \geq \pi/5$

Figure 1b shows the variations of information mutual between Alice and Bob I(A,B) and the quantity of information I(A,E) according to the error probability, the point of intersection of both curves defines the quantum error for $\theta_2 = \pi/5$.

Figure 3 shows the results corresponding to the case of three eavesdroppers (N = 3) where red color in the space θ_1, θ_2 and θ_3 correspond to the secured region, otherwise the information is not secured.

In the particular case in which we assume that eavesdropper collaborate between them, in the sense to have, for example, identical cloning angle ($\theta_1 = \theta$, i = 1,…, N), it is found, in one hand, that the quantum error, calculated numerically, increases as a non linear function of the number of eavesdropper for sufficiently small number N of eavesdropper (Fig. 4).

DISCUSSION

We note that in the secured phase, the error probability is smaller than the quantum error, while in the no secured phase the error probability is greater than the quantum error. At the transition, the error probability Perr coincides with the quantum error Qerr. Phase diagram established in the space parameter (θ_1,θ_2) and presented in Fig. 2, shows the transition line between secured and no secured phases. In contrast to the case of the protocol with one eavesdropper for which the secured-no-secured transition occurs at a cloning angle $\theta_1 = \pi/4$, the region of secured phase depends on both angle θ_1 and θ_2.

The phase diagram described in Fig. 2 proves that for $\theta_1 < \theta_{1c} \approx 0.64$, the transition line is independent of the cloning angle θ_1, for $\theta_1 > \theta_{1c}$, the transition depends strongly on the values of the cloning angle of the second eavesdropper. It's important to note that the transition angle θ_{tr1} increases with decreasing θ_2 and QKD may be secured in the case of collaborating eavesdroppers in case of $\theta_1 < \theta_{1c} \approx 0.64$.

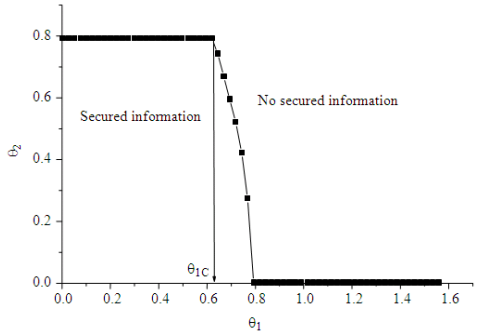

Fig. 2: The (θ_1,θ_2) phase diagram showing the transition between secured and no secured information in the case of two (N = 2) eavesdroppers

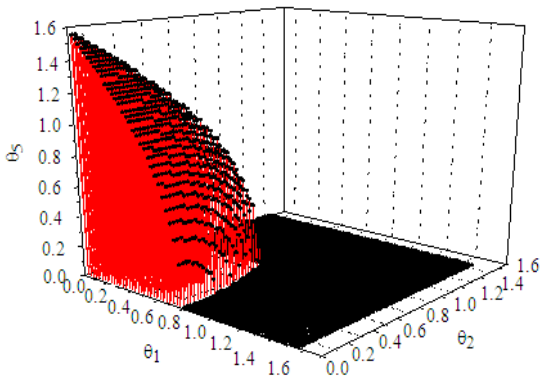

Fig. 3: Phase diagrams obtained in the case N = 3

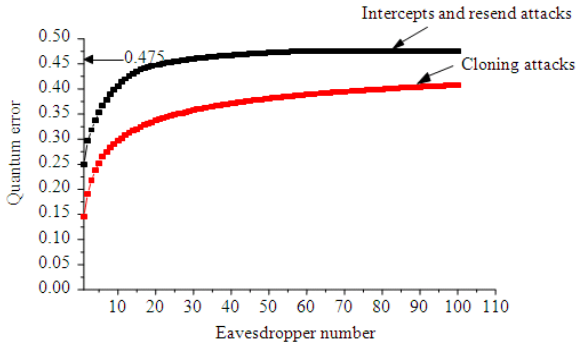

Fig. 4: The behavior of the quantum error as a function of the number of eavesdropper in the case where $\theta_i = \theta$ (i = 1,…,N) for cloning attacks and The behavior of the quantum error as a function of the number of eavesdropper in the case where $\omega_i = \omega$ (i = 1,…,N) for intercepts and resend attacks

However, the problem of three eavesdroppers becomes more complicated and especially in the case where the three eavesdroppers attack the information independently, i.e., when θ_1, θ_2 and θ_3 are completely independent (Fig. 3). For $\theta_1 \leq \pi/4$ and $\theta_2 \leq \pi/4$, the secured space shrinks as long as θ_3 increases. The safety of information depends strongly on the behavior of the 3rd eavesdropper. If $\theta_1 \geq \pi/4$ and $\theta_2 \geq \pi/4$ we obtain a no secured space and does not depend on θ_3.

It is clear from Fig. 4, that knowing the quantum error one can easily estimate the number of eavesdropper in the channel and the way with which collaborate. We note that, for a fixed number of eavesdroppers, the quantum error computed in the case of intercepts and resend attacks (Ez-Zahraouy and Benyoussef, 2009), is greater than the one obtained in the cloning attacks. Which means clearly that cloning attacks is very optimal compared to the intercepts and resends one.

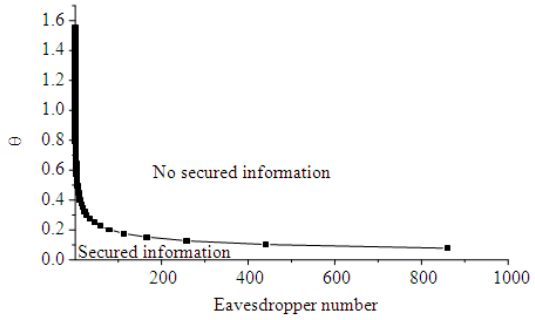

Fig. 5: Phase diagram in the (N,θ) plane showing the secured-no secured transition in the case where $\theta_i = \theta$ (i = 1,…N)

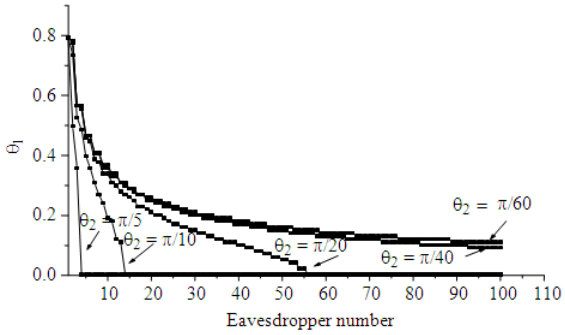

Fig. 6: Phase diagram in the (N, θ_1) plane for different values of θ_2

On the other hand, Fig. 5 shows that the secured-no secured transition occurs under the effect of the number of eavesdropper for a fixed value of the cloning angle θ. In other word, with increasing the number of eavesdropper in a quantum channel we can pass from the secured phase to the no secured one. This result means that the information may be secured in the case of a small number of eavesdroppers, but it is not secured when this number becomes sufficiently large.

If the eavesdroppers use two angle of cloning θ_1 and θ_2 periodically the zone of transition secured-no secured depends at the same time on N Eavesdropper Number and θ_2 this case is presented in Fig. 6.

CONCLUSION

We have studied the effect of cloning attacks of several eavesdroppers on the mutual information between honest parties and the quantum error. We have shown that a transition between secured and no secured information occurs, depending on cloning attack force θ_i of different eavesdropper and/or their number N.

Jointly, we have shown that the behavior of the quantum error depends strongly on these probabilities and undergoes three kinds of behavior as a function of these probabilities. However, in the particular case where eavesdroppers have identical probability of intercepting attacks, we have shown that the cloning attacks is very optimal compared to intercepts and resend attacks.

REFERENCES

Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing. Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Dec. 1984, Bangalore India, pp: 175-179.

Bennett, C.H., F. Bessette, G. Brassard, L. Salvail and J. Smolin, 1992. Experimental quantum cryptography. J. Cryptol., 5: 3-28.

Brub, D., D.P. DiVincenzo, A. Ekert, C.A. Fuchs, C. Macchiavello and J.A. Smolin, 1998. Optimal universal and state-dependent quantum cloning. Phys. Rev. A., 57: 2368-2378. DOI: 10.1103/PhysRevA.57.2368

Buzek, V. and M. Hillery, 1996. Quantum copying: Beyond the no-cloning theorem. Phys. Rev. A., 54: 1844-1852. DOI: 10.1103/PhysRevA.54.1844

Buzek, V., S. Braunstein, M. Hillery and D. Brub, 1997. Quantum copying: A network. Phys. Rev. A., 56: 3446-3452. DOI: 10.1103/PhysRevA.56.3446

Cerf, N.J., 2000. Quantum cloning and the capacity of the Pauli channel. Phys. Rev. Lett., 84: 4497-4497.

Huttner, B., N. Imoto, N. Gisin and T. Mor, 1995. Quantum cryptography with coherent states. Phys. Rev. A., 51: 1863-1869.

Christandl, M., R. Renner and A. Ekert, 2004. A Generic. security proof for quantum key distribution. e-print. http://arxiv.org/abs/quant-ph/0402131

Ez-Zahraouy, H. and A. Benyoussef, 2009. Quantum key distribution with several intercepts and resend attacks. Int. J. Mod. Phys., B23: pp 4755-4766. DOI: 10.1142/S0217979209053631

Lamoureux, L.P., H. Bechmann-Pasquinucci, N.J. Cerf, N. Gisin and C. Macchiavello, 2006. Reduced randomness in quantum cryptography with sequences of qubits encoded in the same basis. Phys. Rev. A., 73: 032304. DOI: 10.1103/PhysRevA.73.032304

Lo, H.K. and H.F. Chau, 1999. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 283: 2050-2056. DOI: 10.1126/science.283.5410.2050

Mayers, D., 1996. Quantum key distribution and string oblivious transfer in noisy channels. Proceedings of the 16th Annual International Cryptology Conference on Advances in Cryptology, Aug. 18-22, Springer-Verlag, London, UK, pp: 343-357. http://portal.acm.org/citation.cfm?id=646761.706026

Shor, P.W. and J. Preskill, 2000. Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett., 85: 441-444.

Wiesner, S., 1983. Conjugate coding. Sigact News, 15: 78-78.