International Journal of Electrical and Computer Engineering (IJECE)
Vol. 8, No. 5, October 2018, pp. 2988~2993
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i5.pp2988-2993

BB84 with Both Several Cloning and Intercept-resend Attacks

Mustapha Dehmani, El Mehdi Salmani, Hamid Ez-Zahraouy, Abdelilah Benyoussef
Laboratoire de Matière Condensée et Sciences Interdisciplinaires, Faculté des Sciences,
Université Mohammed V-Agdal, Morocco

Article Info

Article history:

Received Dec 11, 2017
Revised Apr 25, 2018
Accepted Jul 9, 2018

Keyword:

Cloning attacks
Eavesdroppers
Intercept-resend attacks
Quantum cryptography
Quantum error

ABSTRACT

The goal of the protocol QKD BB84 is to allow a transmitter and a receiver which uses a quantum channel to exchange their keys and to detect the presence of eavesdropping attacks. In the present research, we investigate the effect of several eavesdroppers with both intercept-resend and cloning attacks. We will propose the different possible cases of the positioning of the eavesdroppers and their strategies of attacks; also we will calculate the mutual information for each case. The explicit expressions of the mutual information and quantum error clearly show that the security of the exchanged information depends on the numbers of the eavesdroppers and their attacks parameters on the quantum channel.

Corresponding Author:

Mustapha Dehmani,
Laboratoire de Matière Condensée et Sciences Interdisciplinaires,
Faculté des Sciences, Université Mohammed V-Agdal, Rabat, Morocco.
Email: dehmani01@yahoo.fr

1. INTRODUCTION

The theory of information introduced by Claude Shannon in the forties [1],[2] is strongly exploited in quantum information specially the cryptography. The field of quantum information is always very young and it develops with great speed by comparing with the other axes of research theoretical and experimental. This is possible as a result of the experiments of quantum optics: Schrödinger's cats can be created and observed [3],[4],[5]. These developments certainly seemed impossible before the founders of quantum mechanics. Many scientific deceplins use quantum fundamentals to develop its techniques and algorithms [6]. There is also a design tool for quantum computers, since the invention of quantum error corrector codes [7]. This gives us more hope since much is to be done in this vast field of quantum information theory. Indeed the quantumcryptography has become a necessity with this development and BB84 is the first protocol to have been imagined and implemented [8]. The information is coded on the polarization of single photons, choosing two non-independent polarization basesto ensure safety.This protocol has undergone several variants [9],[10], and has been implemented many times.Furthermore, the quantum key-policy attribute-based encryption scheme was devellioped by using the qutrits [11].

BB84 protocol was implemented fairly quickly, first in the form of a demonstration of principle then more operational devices [12],[13]. Quantum key distribution, often simply called quantum cryptography, is currently the only domain of quantum information where commercial systems are available.The development of cryptographic systems in the presence of noise has also stimulated research into classical information processing algorithms useful in quantum cryptography, such as reconciliation and privacy enhancement algorithms [14],[15],[16].

Other key distribution protocols have been proposed, either with qubits [12], or more recently with continuous variables. Other cryptographic applications have been studied, such as secret sharing or the Byzantine chord problem. The more specific exploitation of quantum entanglement has also led to dense coding [17], quantum teleportation [18] and other applications, also recently a new stady of Quantum password sharing scheme using trusted servers is published [19]. In a previous work, we have presented the quantum key distribution with several intercept and resend attacks [20] and with several cloning attacks [21], and we have investigated the cases of quantum key distribution with several attacks via a depolarizing channel [22] [23] and partially non-orthogonal basis states [24]. Our aim in this paper is to study the effect of two groups of eavesdropping strategy; intercept-resend and cloning attacks on the behaviour of the mutual information between honest parties and the quantum error rate within the BB84 protocol. 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. RESEARCH METHOD

The quantum key distribution (QKD) can use several photon properties for the purpose of encoding information such as polarization, phase, quantum correlations or wavelength. The only requirement on quantum states is that they belong to mutually non-orthogonal Hilbert space basis. We use the polarization coding and we consider two bases: the first called rectilinear is represented by the Horizontal and Vertical polarization$\left|H\right\rangle,\left|V\right\rangle$ and the second is called diagonal and is generated by 45° of polarization$\left|A\right\rangle$ and 135° $\left|D\right\rangle$

$$\left|A\right\rangle=\frac{\sqrt{2}}{2}\left(\left|H\right\rangle+\left|V\right\rangle\right) \text{ and } \left|D\right\rangle=\frac{\sqrt{2}}{2}\left(\left|H\right\rangle-\left|V\right\rangle\right)$$

These four states satisfy the following relations:

$$\left\langle H\middle|V\right\rangle=\left\langle A\middle|D\right\rangle=0$$
$$\left\langle H\middle|H\right\rangle=\left\langle V\middle|V\right\rangle=\left\langle A\middle|A\right\rangle=\left\langle D\middle|D\right\rangle=1 \; \left|\left\langle H\middle|A\right\rangle\right|^2=\left|\left\langle H\middle|D\right\rangle\right|^2=\left|\left\langle V\middle|A\right\rangle\right|^2=\left|\left\langle V\middle|D\right\rangle\right|^2=\frac{1}{2}$$

All measurements made in the diagonal (rectilinear) base for photons prepared in the rectilinear (diagonal) base will give random results with equal probabilities. On the other hand, measurements made in a base identical to that of preparation of the states will produce deterministic results. At first, both parties who wish to communicate, traditionally called Alice and Bob agree that, for example, ($\left|H\right\rangle,\left|A\right\rangle$) represent the "0" value of the bit, and ($\left|V\right\rangle,\left|D\right\rangle$) have "1". Alice, the sender generates a sequence of random bits that she wants to transmit randomly; independently for each bit she chooses its coding base, rectilinear or diagonal.

Subsequently, Bob receives these photons and uses a filter to read them. Nevertheless, some photons will be useless; it is the photons that have been polarized in a different base. These photons must not be taken into account in the key. To do this, a channel, which can be public, is used between Alice and Bob to determine which photons are useless. In our work we shoes to study when N+S eavesdroppers E_i (i = 1,…..,N+S), were placed between Alice and Bob. These eaves droppers form two groups, each groupwill adopt a strategy of attacks; cloning or intercept-resend attacks, according to the model represented in Figure 1 and Figure 2.

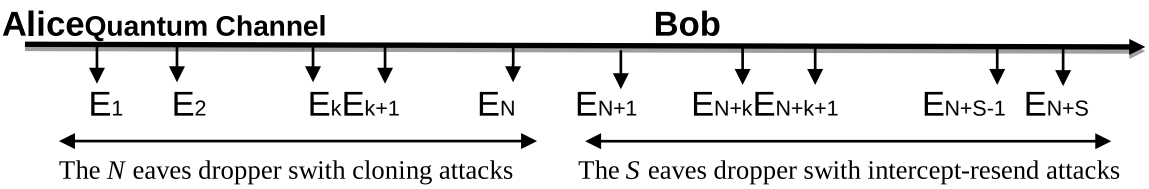
Alice
Quantum Channel
Bob
E1
E2
Ek
Ek+1
EN
EN+1
EN+k
EN+k+1
EN+S-1
EN+S
The N eaves dropper swith cloning attacks
The S eaves dropper swith intercept-resend attacks

Figure 1. Model of N cloning attacks followed by S intercept-resend attacks

According to Figure 1, Alice send a photon polarized which represents randomly 1 or 0, with equal probability 1/2, to Bob. Between two groups of eavesdroppers is placer on the quantum channel, the first one use cloning attack. Each eavesdropper $E_i\,(i=1,...,N)$ clone with an operator U defined as:

$$U(\,|0\rangle_A|0\rangle_{E_i)} = |0\rangle_A|0\rangle_{E_i} \quad \text{and} \quad U(|1\rangle_A|0\rangle_{E_i}) = |1\rangle_A|1\rangle_{E_i}$$

E_i will use U in the base y which will be defined as follows:

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

θ_i is the cloning angle, and it defined the force of attacks.

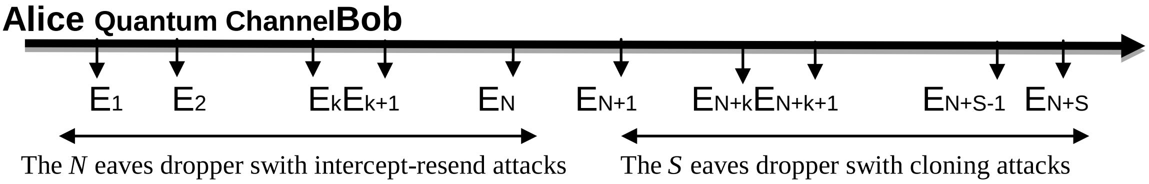
Alice Quantum ChannelBob
E1
E2
EkEk+1
EN
EN+1
EN+kEN+k+1
EN+S-1
EN+S
The N eaves dropper swith intercept-resend attacks
The S eaves dropper swith cloning attacks

Figure 2. Model of N intercept-resend attacks followed by S cloning attacks

The second group use intercept-resend attacks. Each eaves dropper $E_i(i = N+1,...,N+S)$ intercepts, with probability ω_i, the photon emitted by the eaves dropper E_{i-1}, measures its polarization state and resends it, in its measured polarization state, to the eavesdropper E_{i+1}. However, in the second figure (Figure 2) the roles of the groups of eaves droppers are reversed, ie Alice send a polarised photon and each eavesdropper $E_i(i = 1,...,N)$ from the first group intercepts the photon with probability ω_i and each eavesdropper $E_i(i = N+1,...,N+S)$ from the second group use the cloning operator U defined above.

3. RESULTS AND ANALYSIS

In this section we calculate the quantum error Q_{err} and the mutual information between Alice and Bob and between Alice and the mth eavesdroppers defined as follow:

$$I(A,B) = 1 + P_{AB}(0/0)Log_2(P_{AB}(0/0)) + P_{AB}(1/0)Log_2(P_{AB}(1/0))$$
$$I(A,E_m) = 1 + P_{AE_m}(0/0)Log_2(P_{AE_m}(0/0)) + P_{AE_m}(1/0)Log_2(P_{AE_m}(1/0))$$

With $P_{AB}(1/0) = 1 - P_{AB}(0/0)$ and $P_{AE_m}(1/0) = 1 - P_{AE_m}(0/0)$

$P(y/x_A)$ is the conditional probability that Bob or E_m receive a photon polarized horizontally (vertically) y = 0,1 with respect that Alice send a photon polarized horizontally (vertically) X_A = 0,1. All this conditional probabilities depend on the models attacks described in the previous section; In fact, we will study the quantum key distribution and the two cases will be distinguished if the group of cloning attacks is placed first or last. The lost information between Alice and Bob corresponds to the maximum information copied by the entire eavesdroppers:

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

The error probability P_{err} is given by:

$$P_{err} = \sum_{x_A,x_B} \left| P_{AB}(x_A,x_B)\Big|_{\substack{\theta_i=0\\ \omega_j=0}} - P_{AB}(x_A,x_B)\Big|_{\substack{\theta_i\neq0\\ \omega_{j+1}\neq0}} \right|$$

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 $P_{err}>Q_{err}$, $I(A,E)>I(A,B)$

3.1. Quantum Key Distribution in the Presence of N Cloning Attacks Followed by S Intercept-Resend Attacks

Based on Figure 1, the quantum error Q_{err} and the mutual information $I(A,B)$ between Alice and Bob arecalculated according to conditional probability:

$$P_{AB}(0/0)=P_{AB}(1/1)=\left[\sum_{k=0}^{S}\frac{2^{S-k}+1}{2^{S-k+1}}\sum_{i_1,\ldots,i_k=1,S}\prod_{j=1}^{k}(1-\omega_{i_j})\prod_{l=k+1}^{S}\omega_{i_l}\right]\left(1+\prod_{i=1}^{N}\cos(\theta_i)\right)/2$$

If all eavesdroppers collaborate between them and use the same cloning angle θ and identical attack probabilities ω, $P_{AB}(0/0)$ will be:

$$P_{AB}(0/0)=P_{AB}(1/1)=\frac{1}{4}\left(1+(1-\frac{\omega}{2})^{S}\right)\left(1+\cos^{N}(\theta)\right)$$

Since both types of attacks act on the quantum states viheculated on the channel, the conditional probabilities between Alice and Bob are different compared to those published in the case of several attacks of intercept and resend only [20] or cloning only [21]. However, the mutual information $I(A,E_m)$ between Alice and each eavesdropper E_m is calculated according to conditional probability $P_{AE_m}(0/0)$. In fact, this probability changes according to the position of the eavesdropper:

If $m\le N$:

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

$$P_{AE_m}(0/0)=P_{AE_m}(1/1)=\frac{1}{2}\left(1+\cos(\theta)^{m-1}\sin(\theta)\right)$$ if all eaves droppers E_m (with $m<N$) have the same cloning angle θ.

These results fit perfectly with those found in the case of several cloning attacks [21] Else if $m>N$: In this case the two types of attacks will occur, and this will clearly appear in the formulas of conditional probabilities between Alice and every eveas dropper.

$$P_{AE_m}(0/0)=P_{AE_m}(1/1)=\left(1+\left[\prod_{i=1}^{m-1}\left(1-\frac{\omega_i}{2}\right)\frac{\omega_m}{2}\right]\prod_{i=1}^{n}\cos(\theta_i)\right)/2$$

Also, $P_{AE_m}(0/0)=P_{AE_m}(1/1)=\left(1+\left[\left(1-\frac{\omega}{2}\right)^{m-1}\frac{\omega}{2}\right]\cos^{N}(\theta)\right)/2$ if all eaves droppers choose identical attack parameters θ and ω.

3.2. Quantum Key Distribution in the Presence of N Intercept-Resend Attacks Followed by S Cloning Attacks

In this case and according to the model of Figure 2, $P_{AB}(0/0)$ is written in the form:

$$P_{AB}(0/0)=P_{AB}(1/1)=\left[\sum_{k=0}^{N}\frac{2^{N-k}+1}{2^{N-k+1}}\sum_{i_1,\ldots,i_k=1,N}\prod_{j=1}^{k}(1-\omega_{i_j})\prod_{l=k+1}^{N}\omega_{i_l}\right]\left(1+\prod_{i=1}^{S}\cos(\theta_i)\right)/2$$

And if $\forall i \le N\ \omega_i = \omega$ and $\theta_j = \theta\ \forall N < j \le S$, $P_{AB}(0/0) = \frac{1}{4}\left(1+(1-\frac{\omega}{2})^N\right)\left(1+\cos^S(\theta)\right)$

The position of each eaves dropper E_m with its strategy of attack is a decisive element for the calculation of the conditional probabilities $P_{AE_m}(0/0)$ and subsequently the mutual information $I(A,E_m)$. If $m \le N$: All eaves droppers use intercept-resend attacks and the conditional probabilities will be identical to those published in a previous work [20]

$$P_{AE_m}(0/0) = P_{AE_m}(1/1) = \frac{1-\omega_m}{2} + \sum_{k=0}^{m-1}\frac{2^{m-k}+1}{2^{m-k+1}}\sum_{i_1,...,i_k=1,m-1}\prod_{j=1}^{k}(1-\omega_{i_j})\prod_{l=k+1}^{m}\omega_{i_l}$$

Also $P_{AE_m}(0/0) = P_{AE_m}(1/1) = \frac{1}{2}\left[1+\frac{\omega}{2}(1-\frac{\omega}{2})^{m-1}\right]$ if $\omega_i = \omega\ \forall i \le N$

However if $m > N$: The state arriving at the eaves dropper E_m underwent before N intercept-resend attacks and all E_m (with $m > N$) choose to use the cloning attacks.

$$P_{AE_m}(0/0) = P_{AE_m}(1/1) = \left(1+\left[\sum_{k=0}^{N}\frac{2^{N-k}+1}{2^{N-k+1}}\sum_{i_1,...,i_k=1,N}\prod_{j=1}^{k}(1-\omega_{i_j})\prod_{l=k+1}^{N}\omega_{i_l}\right]\prod_{i=1}^{m-1}\cos(\theta_i)\sin(\theta_m)\right)/2$$

Indeed in this last case if all $E_i(i=1,...,N)$ have an identical attack probability $\omega_i = \omega$ and all $E_j(j=N+1,...,N+S)$ have an identical cloning angle $\theta_j = \theta$, the conditional probability $P_{AE_m}(0/0)$ will be: $P_{AE_m}(0/0) = P_{AE_m}(1/1) = \frac{1}{2}\left(1+(1-\frac{\omega}{2})^N\right)\left(1+\cos(\theta)^{m-1}\sin(\theta)\right)$

4. CONCLUSION

We have studied the quantum key distribution of BB84 protocol in the presence of several eavesdroppers with two different attack strategies cloning and intercept-resend attacks based on the calculations of the quantum error Q_{err} and the mutual information $I(A,B)$ between Alice and Bob and $I(A,E_m)$ between Alice and each eavesdropper E_m and We have detailed all the cases according to the eavesdropping position with the attacks type used. It is clear that the attacksparameters ω_i and θ_j , the number of theeavesdroppers, and their positioning on the quantum channelact strongly on the information security of the quantum key distribution

REFERENCES

[1] C. Shannon. "A Mathematical Theory of Communication", *Bell System Technical Journal*, 1948,vol. 27, pp. 623-656,

[2] C. Shannon, "Communication in the Presence of Noise", *Proc. IRE*, 1949, vol. 37, pp. 10-21.

[3] A. Ourjoumtsev, H. Jeong, R. Tualle-Brouri, and P. Grangier, “Generation of optical Schrödinger cats from photon number states”, *Nature*, 2007, vol. 448, pp. 784-786.

[4] A. Ourjoumtsev, R. Tualle-Brouri, J. Laurat, and P. Grangier, “Generating Optical Schrödinger kittens for quantum information processing”, *Science*, vol. 312, pp. 83-86, 2006.

[5] S. Gleyzes, S. Kuhr, C. Guerlin, J. Bernu, S. Deléglise, U.B. Hoff, M. Brune, J.M.Raimond, and S. Haroche,” Quantum jumps of light recording the birth and death of a photon in a cavit”, *Nature*, vol. 446, pp. 297-300, 2007.

[6] S. Wu, “A Quantum Chaos Clonal Multiobjective Evolutionary Method Reasearch”, *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 3, No. 1, pp. 226-234, 2016.

[7] A.R. Calderbank and P.W. Shor, “Good quantum error-correcting codes exist”, *Physical Review A*, vol. 54, pp. 1098-1105, 1996.

[8] C. Bennett et G. Brassard. "Quantum Cryptography : Public Key Distribution and Coin Tossing", *IEEE Conf. on Computers, Systems and Signal Processing, Bangalore*, India p. 175 1984.

[9] C.H. Bennett. "Quantum cryptography using any two nonorthogonal states", *Phys. Rev. Lett*, vol. 68, pp. 3121-3124, 1992.

[10] D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States", *Phys. Rev. Lett*, Vol. 81, No. 14, pp. 3018–3021, 1998.

[11] G. Mogos "Quantum Key-Policy Attribute-Based Encryption", *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 7, No. 2, pp. 542 -550, 2017

[12] N. Gisin, G. Ribordy,W. Tittel, and H. Zbinden, "Quantum cryptography", *Review of Modern Physics*, vol. 74, no. 1, pp. 145-195, 2002.

[13] P. Grangier, J. Rarity, and A. Karlsson, "Quantum interference and cryptographic keys: novel physics and advancing technologies (QUICK)", *The European Physical Journal D*, vol. 18, no. 2, pp. 139-139, 2002.

[14] U.M. Maurer, "Secret key agreement by public discussion from common information", IEEE Transactions on Information Theory, vol. 39, pp. 733–742, 1993

[15] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion", *In Advances in cryptology–Eurocrypt'93, number 765 in Lecture Notes in Computer Science*, pages 410–423, 1993.

[16] C. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, "Generalized privacy amplification", *IEEE Transactions on Information Theory*, vol. 41, no. 6, pp. 1915– 1935, 1995.

[17] C. Bennett and S. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states", *Physical Review Letters*, vol. 69 pp. 2881– 2884, 1992.

[18] C. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels", *Physical Review Letters*, vol. 70, pp. 1895–1899, 1993.

[19] G. Mogos, "Quantum password sharing scheme using trusted servers", *International Journal of Information & Network Security (IJINS)* Vol. 2, No. 3, pp. 203-206, 2013.

[20] H. Ez-Zahraouy and A. Benyoussef, "Quantum key distribution with several intercepts and resend attacks", *Int. J. Mod. Phys. B*, vol. 23, pp. 4755-4765, 2009.

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

[22] M. Dehmani, H. Ez-Zahraouy , M. Errahmani and A. Benyoussef, "Quantum Key Distribution with Several Cloning Attacks via a Depolarizing Channel", *Phys. Scr*, vol. 86, 2012.

[23] M. Dehmani, H. Ez-Zahraouy and A. Benyoussef "Quantum key distribution with several cloning attacks via a depolarizing channel", *Journal of Russian Laser Research*, vol. 36 No. 3, pp. 228-236, 2015.

[24] 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, pp. 624-627, 2014.