Science Journal Of Mathematics and Statistics
ISSN: 2276-6324
http://www.sjpub.org/sjms.html

Published By
Science Journal Publication
International Open Access Publisher

Research Article **Volume 2012 (2012), Article ID sjms-223, 6 Pages, doi: 10.7237/sjms/223**

Analysis of the Influence of the Rate of Spies' Measure on the Quantum Transmission

B. Ouchao[1] and E.H. El Kinani[2]

[1] Informatics Department, Moulay Ismail University
Faculty of Sciences and Technics
Box 509 Errachidia, Morocco

[2] G.A.A, Mathematical Department, Moulay Ismail University
Faculty of Sciences and Technics
Box 509 Errachidia, Morocco, elkinani_67@yahoo.com

Accepted 12 April, 2012

ABSTRACT- In this paper, we will study the influence of spies rate measure on the quantum transmission by using the entropy measures and java simulation. The quantum transmission adopted here is the BB84 protocol (Charles Bennett and Gilles Brassard). In particular, we estimate the measurement error rate which indicate the presence of spies and we analyze the influence of the the spies rate of measures of on the transmission.

Keywords: BB84, Quantum Distribution of Key, Qubit, simulation, Java.

1 Introduction

Information theory based on probability and statistics theories was first in- troduced by Shannon in 1948 [1]. One of the most quantities of the Shannon theory is the entropy which is a measure of the uncertainty associated with a random variable. In this paper we will analyze the influence of the spies rate measures using entropy measures in quantum transmission and java simula- tion. The paper is organized as follows: First, we recall some definitions and results which will be used later. In section III, we introduce the BB84 protocol either with the presence without the presence spies. In the last section we will present our measures, results, analysis and interpretations.

2 Some preliminary definitions

2.1 Mutual information

In the probability language, we say that two variables are independent if the realization of the one has not effect the realization of the other one[1]. The mutual information is useless if and only if variables are independent.
Let (X, Y) a couple of random variables of density of joined probability given by P (x, y), denote by P_X the probability of the event (X = x), and P_Y is the probability of the event (Y = y) (for all X), then the mutual information in the discrete case is given by the following expression:

$$I(X,Y) = \sum_{xy} P(X,Y)\log_2\left(\frac{P(X,Y)}{P_X P_Y}\right), \quad (1)$$

where $\log_2$ denote the base 2 logarithm function.

$$P_X = \sum_{y} P(X,Y), \quad (2)$$

and

$$P_Y = \sum_{x} P(X,Y). \quad (3)$$

2.2 Qubit

Let's recall that the qubit is the quantum state which represents the smallest unit of storage of quantum information. A general qubit[2] can be represented as a linear combination of states $|0>$ and $|1>$ as:

$\alpha|0> + \beta|1>$,

where α and β are complex probability amplitudes which are constrained by the equation:

$|\alpha|^2 + |\beta|^2 = 1$.

$|\alpha|^2$ is the probability that the qubit will be measured in the state $|0>$ and

$|\beta|^2$ is the probability that the qubit will be measured in the state $|1>$.

3 BB84 protocol in summary

3.1 BB84 protocol without spy

In summary in BB84 protocol[3], Alice uses photons which are coded in a different state of polarization to transmit a message to Bob. There is two possibilities to polarize photons: vertical polarization which is noted by 0 and horizontal polarization which noted by 1.

Alice's Bases	(V_0,V_1)	$(V_0{}^0,V_1{}^0)$	
	(V_0,V_1)		
Alice's photon	0	0	1
Bob's Bases	(V_0,V_1)	(V_0,V_1)	
Photon received by Bob	$(V_0{}^0,V_1{}^0)$ 0	$\frac{1}{0}$ or $\frac{1}{2}$ 2or 1	$\frac{1}{2}$ or $\frac{1}{2}$ 0 or 1
Probability best photon	1		

(V_0,V_1) is a base representing the polarization horizontal-vertical denoted H/V.
$(V_0{}^0,V_1{}^0)$ is a base representing the polarization diagonal-anti-diagonal denoted D/A.

3.2 BB84 protocol with a single spy

Here, we assume that spy can make only a passive attack on the canal. (i.e. authenticated canal). However, toobtain some information, spy will have to make a measure on the photons (qubit). We can calculate the probability of maximal error accepted by Bob and Alice before abandoning the transmission. Indeed, from their finalized key, Alice and Bob will use a part of their photons and will compare the moderate states of polarization and will then evaluate the probability of the error [4],which is given by:

$$P_{error}=\frac{\text{Number of photon common}}{\text{Number of photon transmited in the common base}}.$$

The information theory defines the mutual information, we denote by I_{AB} the mutual information between Alice and Bob and I_{AE} the mutual information between Alice and spy. These two quantities are calculated from P_{error}. The limit P_{error} is obtained where we have $I_{AE} = I_{AB}$. Alice and Bob agree to send the key since the condition $I_{AB} \geq I_{AE}$ is satisfied then spy has less information than Bob. Indeed, when $I_{AB} \geq I_{AE}$, it is always possible for Alice and Bob to transmit a key.

We adopt here the technique "Intercept and resend".[5,6] (i.e. spy intercept the photon and resend it in the same base). If spy chooses the same base as Alice, her will not be detected because the state of polarization of the photon will not infected. On the other hand, if spy chooses a different base, she will have a equal chance to measure both polarization (with the probability p = $\frac{}{2}$) and will more have perturbed the state. The continuation of transmission depends on Bob, if Bob chooses a base different from that Alice, this measure will anyway be given up. If he uses the same base as Alice and spy, nothing allows to detect spy's intervention. If Alice and Bob use the same base and spy different one, she will have perturbed the sent photon and Bob will be lucky on two to have an erroneous measure and the error is detected.

4 Mutual information between Alice and Bob and between Alice and spy.

4.1 Case of a single spy

In that follow, we adopt the following notation "A" means the state of polar- ization which has sent by Alice, "B" the state received by Bob and "E" the one that spy has intercepted. It will know that the mutual information between Alice and Bob is given by:

$$I(A,B) = \sum_{ij} P(A,B)\log_2\left(\frac{P(A,B)}{P(A)P(B)}\right). \quad (4)$$

We suppose here that all photons which were measured in a different base are eliminated.

Cas 1: Evaluation of the probability P(E/A):
1-1) P(E=0 / A=0): probability that spy measures the state 0 knowing Alice sent the state 0.
Two cases appear: either spy measures the photon, or she does not due the measure.

- If spy make measures.
The probability to obtain the state 0 knowing that Alice has send the state 0 is:

$$P_1(E = 0/A = 0) = \frac{3\omega}{4}, \quad (5)$$

where ω is a probability that spy chooses to make the measure.
- If spy does not make the measure, then we have:

$$P_2(E = 0/A = 0) = \frac{1}{2} - \frac{\omega}{2}. \quad (6)$$

Then the probability P(E=0 / A=0) in all cases is :

$$P(E = 0/A = 0) = P_1 + P_2 = \frac{1}{2} + \frac{\omega}{4}. \quad (7)$$

1-2)P (E = 1/A = 0): probability that spy measures the state 1 knowing that
Alice sent the state 0.
Two cases appear: spy measures the photon, or she does not measure it.
- If spy make a measure, then the probability to obtain the state 1 such that
Alice has send the state 0 is:

$$P_1(E = 1/A = 0) = \frac{\omega}{4}. \quad (8)$$

- If spy does not make the measure, then we have:

$$P_2(E = 1/A = 0) = \frac{1}{2} - \frac{\omega}{2}. \quad (9)$$

Then the probability in all cases is :

$$P(E = 1/A = 0) = P_1 + P_2 = \frac{1}{2} - \frac{\omega}{4}. \quad (10)$$

To obtain the probability that Alice make a measure the state 0 (respectively the state 1) and spy make a measure the state 0, we use the following relation: P(X,Y)=P(X/Y).P(Y), then we have:

$$P(0,0) = P(1,1) = \frac{1}{4} + \frac{\omega}{8} \quad \text{and} \quad P(1,0) = P(0,1) = \frac{1}{4} - \frac{\omega}{8}. \quad (11)$$

Cas 2: Evaluation of the probability P(B/A):
2-1)P (B = 0/A = 0): probability that Bob measures the state 0 such Alice sent the state 0. Two cases appear: Spy measures the photon, or she does not measure it. - If spy make a measure, then the probability to obtain the state 0, such that Alice has send the state 0 is:

$$P_1(B = 0/A = 0) = \frac{3\omega}{4}. \quad (12)$$

$$P_2(B = 0/A = 0) = \frac{1}{2} - \frac{\omega}{2}. \quad (13)$$

- If spy does not make the measure, then we have:
In general the probability is:

$$P(B = 0/A = 0) = P_1 + P_2 = 1 - \frac{\omega}{4}. \quad (14)$$

2-2)P (B = 1/A = 0): probability that Bob measures 1 knowing that Alice sent the state 0. Two cases appear: spy measures the photon, or she does not measure it. - If spy make a measure, then the probability to obtain the state 1, such that Alice has send the state 0 is:

$$P_1(B = 1/A = 0) = \frac{\omega}{4}. \quad (15)$$

- spy does not make the measure, then we have:

$$P_2(B = 1/A = 0) = 0. \quad (16)$$

In general the probability is:

$$P(E = 1/A = 0) = P_1 + P_2 = \frac{\omega}{4}. \quad (17)$$

As in Eq.(11), the probability between Alice and Bob is:

$$P(0,0) = \frac{1}{2} + \frac{\omega}{8} \quad \text{and} \quad P(1,0) = \frac{\omega}{8}. \quad (18)$$

Therefore, from the equation (4) and the equations (9-12), we have :

$$I_{AE} = \frac{1}{2}\log_2\left(1 - \frac{\omega^2}{4}\right) + \frac{\omega}{4}\log_2\left(\frac{1+\frac{\omega}{2}}{1-\frac{\omega}{2}}\right), \quad (19)$$

and

$$I_{AB} = \log_2\left(2 - \frac{\omega}{2}\right) - \frac{\omega}{4}\log_2\left(\frac{4}{\omega} - 1\right). \quad (20)$$

We have calculated ω such as $I_{AE} = I_{AB}$, then we have :

$$I_{AE} = I_{AB} \Leftrightarrow \omega = 1. \quad (21)$$

How to Cite this Article: B. Ouchao, E.H. El Kinani, "Analysis of the Influence of the Rate of Spies' Measure on the Quantum Transmission," Science Journal Of Mathematics and Statistics, Volume 2012 (2012), Article ID sjms-223, 6 Pages, doi: 10.7237/sjms/223

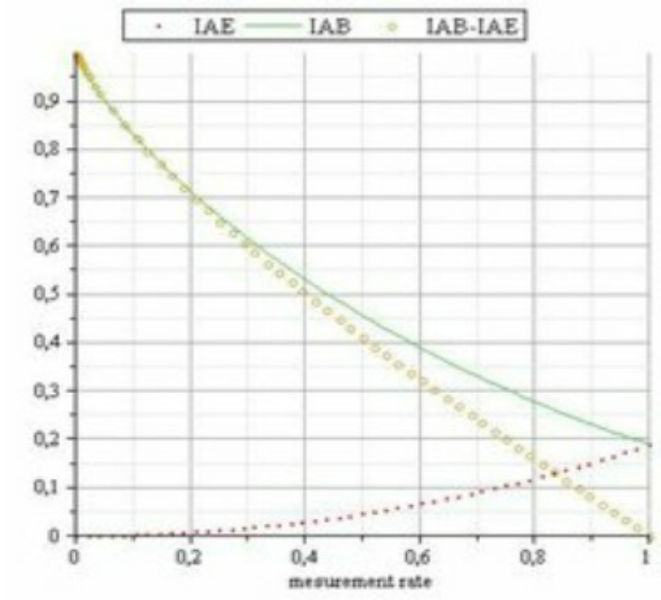
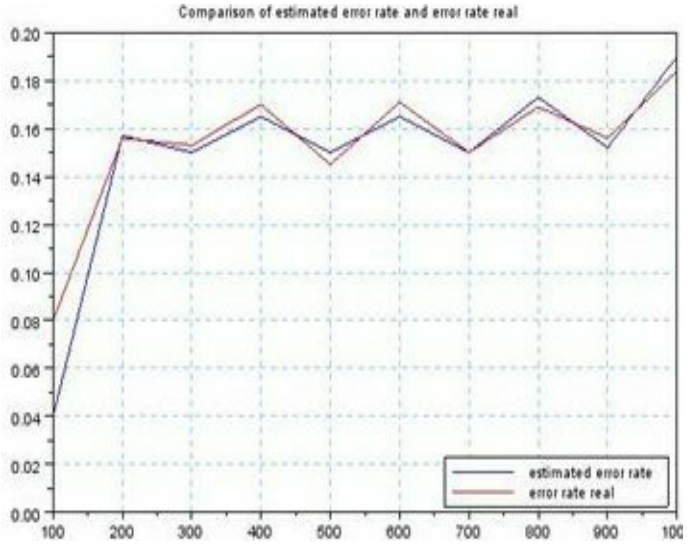


Figure 1: Mutual information as function of rates of measures. The probability of estimated errors noted by Pes err was obtained by the measure do by spy is the sum of the differences of the probability that Alice sends photon of state 0 (respectively state 1) and that Bob receives photon of state

$$P_{es-err} = \left[\left| p(0,1)_{\omega=0} - p(0,1) \right| + \left| p(1,0)_{\omega=0} - p(1,0) \right| \right] = \frac{\omega}{4}. \qquad (22)$$



1 (respectively state 0) in the cases ? = 0 and ? > 0 then:

Figure 2: Statistics $P_{es\ err}$ and P_{error} as function of number of qubits trans- mitted in common base.

Statistics analysis made that when $P_{es\ err} < 0.25$ then we have $P_{es\ err} \approx P_{error}$ this result is illustrated in the figure 2 above. From equation (Eq.19) and (Eq.20), we replace ω with $4P_{error}$ (Eq.22), then we obtain the figure 3 bellow, in which we see that spy can never obtain the complete key as long as $P_{error} < 0.25$.

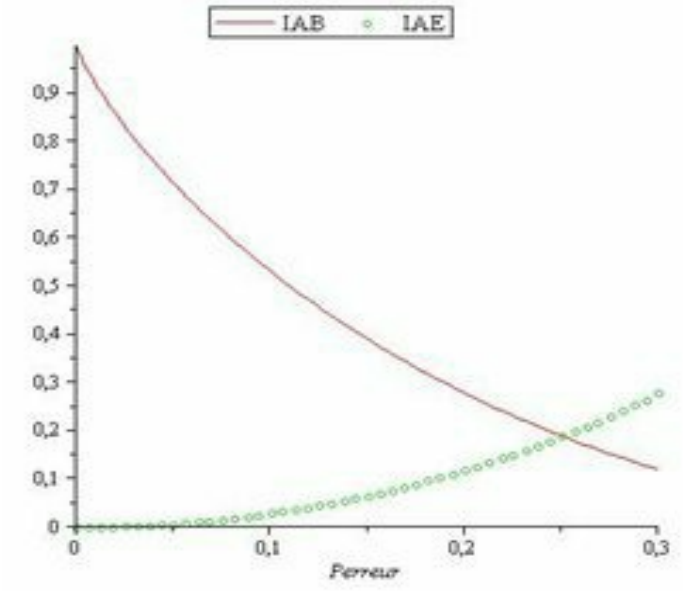


Figure 3: Mutual information as function of P_{error}.

4.2 Case of two spy

Here we denote the rate of measure of the spy_i by ω_i (i=1,2), we adopt also the following: α means the state of polarization which is sent by Alice, E_i what is that spy_i intercepted and β is the state of polarization received by Bob. In that follow, we will compute the probabilities between Alice and spy_2 in one hand, and between Alice and Bob in other hand, in presence of spy_1.

Here we denote the rate of measure of the spy_i by ω_i (i=1,2), we adopt also the following: α means the state of polarization which is sent by Alice, E_i what is that spy_i intercepted and β is the state of polarization received by Bob. In that follow, we will compute the probabilities between Alice and spy_2 in one hand, and between Alice and Bob in other hand, in presence of spy_1.

Case 1: Between Alice and spy_2 :

2-1) P ($E_2 = 0/\alpha = 0$) In this case we have six possibilities:

- spy_1 and spy_2 measure in the same base as Alice.
- spy_1 measures in the same base as Alice and spy_2 in the different base.
- spy_1 measures in the different base as Alice and spy_2 in the same base as Alice.
- spy_1 and spy_2 measure both in the same base which is different from that of Alice.

How to Cite this Article: B. Ouchao, E.H. El Kinani, "Analysis of the Influence of the Rate of Spies' Measure on the Quantum Transmission," Science Journal Of Mathematics and Statistics, Volume 2012 (2012), Article ID sjms-223, 6 Pages, doi: 10.7237/sjms/223

- spy_1 does not measure and spy_2 measures.
- spy_2 does not measure.

Then the probability that spy_2 measures state 0 knowing that Alice sent state 0 is given by:

$$P(E_2 = 0, \alpha = 0) = \frac{1}{2} - \frac{7\omega_1\omega_2}{16} + \frac{\omega_2}{4}. \quad (23)$$

$$P(E_2 = 0, \alpha = 1) = \frac{1}{4} + \frac{3}{16}\omega_1\omega_2 - \frac{(\omega_1 + \omega_2)}{8}. \quad (24)$$

Cas 2: Between Alice and Bob:
2-1) $P(\beta = 0/\alpha = 0)$

$$P(\beta = 0, \alpha = 0) = \frac{1}{16}\omega_1\omega_2 - \frac{1}{8}(\omega_1 + \omega_2) + \frac{1}{2}. \quad (25)$$

2-2) $P(\beta = 0/\alpha = 1)$

$$P(\beta = 0, \alpha = 1) = \frac{1}{8}(\omega_1 + \omega_2) - \frac{1}{8}\omega_1\omega_2. \quad (26)$$

Apply the formula (4) we obtain:

$$I_{AE_1} = \frac{1}{2}\log_2(1 - \frac{\omega_1^2}{4}) + \frac{\omega_1}{4}\log_2(\frac{1 + \frac{\omega_1}{2}}{1 - \frac{\omega_1}{2}}). \quad (27)$$

The figure 4 below shows that the mutual information I_{AE1} believes as long as the spy_1 measures, it does not depend on the measure of the spy_2.

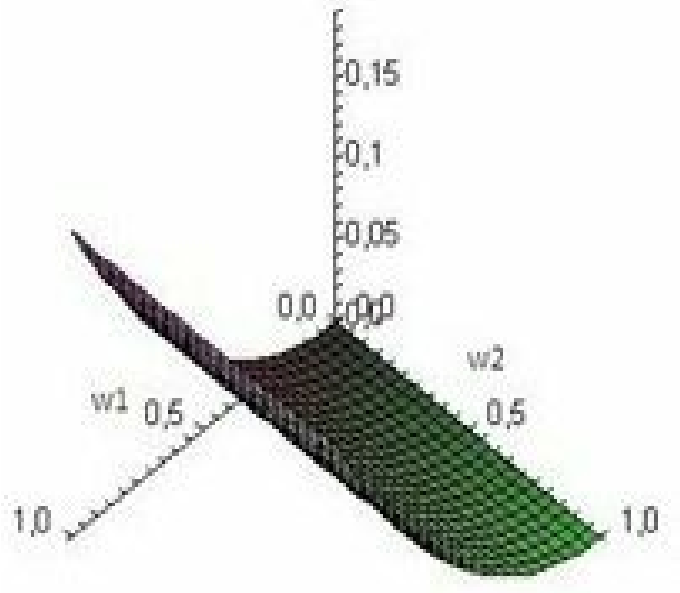


Figure 4: Mutual information I_{AE1} as function of ω_1 and ω_2.

$$I_{AE_2} = \frac{\omega_1\omega_2}{8}\log_2(\frac{F^3}{E}) - \frac{\omega_2}{4}\log_2(\frac{F}{E}) + \frac{\omega_1}{4}\log_2(F) + \frac{1}{2}\log_2(EF), \quad (28)$$

With

$$E = 1 - \frac{\omega_1\omega_2}{6} + \frac{\omega_2}{2} \text{ and } F = 1 + \frac{3}{4}\omega_1\omega_2 - \frac{1}{2}(\omega_1 + \omega_2)$$

However, in the figure 5, we see that the value of the mutual information I_{AE2} is not important when the spy_1 due the measure, indeed his presence perturbs the transmission.

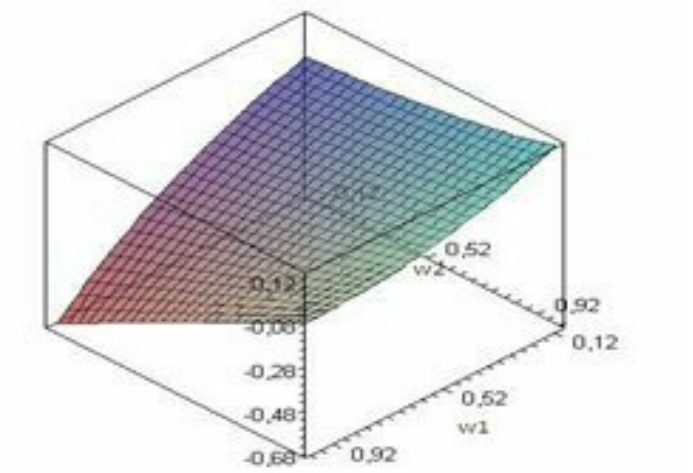


Figure 5: Mutual information I_{AE2} as function of ω_1 and ω_2.

$$I_{AB} = \frac{1}{8}\omega_1\omega_2\log_2(\frac{C}{D^2}) - \frac{1}{4}(\omega_1 + \omega_2)\log_2(\frac{C}{D}) + \log_2(C), \quad (29)$$

With

$$C = \frac{\omega_1\omega_2}{4} - \frac{1}{2}(\omega_1 + \omega_2) + 2 \text{ and } D = \frac{1}{2}(\omega_1 + \omega_2) - \frac{1}{2}\omega_1\omega_2.$$

In the figure 6, we see that in spite of the measures of both spies the value of the mutual information I_{AB} remains valid as long as the rate of the measures does not exceed the value 1.

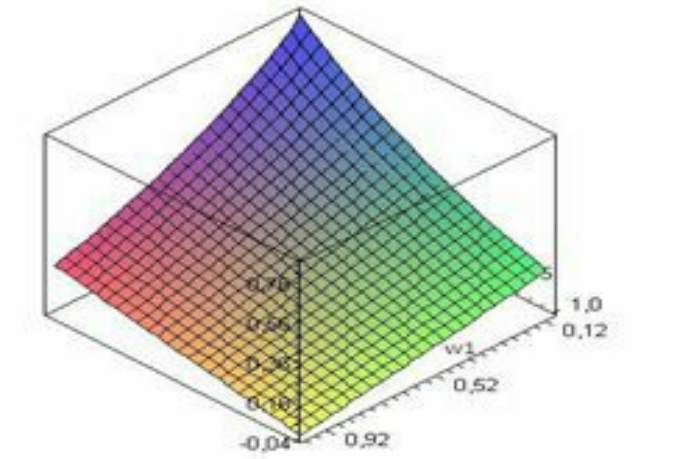


Figure 6: Mutual information I_{AB} as function of ω_1 and ω_2

Note that in the limit $\omega_1 = 0$, we reproduce the case with a single spy Eq.(11) By comparing I_{AB} with I_{AE1} and I_{AE2} as show in both figures 7 and 8, we note that spy_2 does not gain more information as long as he does not measure all the transmitted photons, hence the presence of spy_1 perturbs the transmission since he measures half of the transmitted photons independently of rate of measure of spy_2.

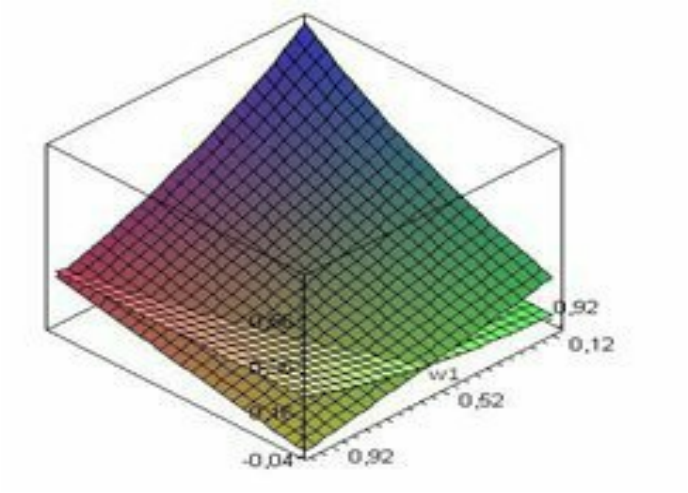


Figure 7: Mutual informations I_{AB} and I_{AE1} as function of rate of measure (ω_1, ω_2).

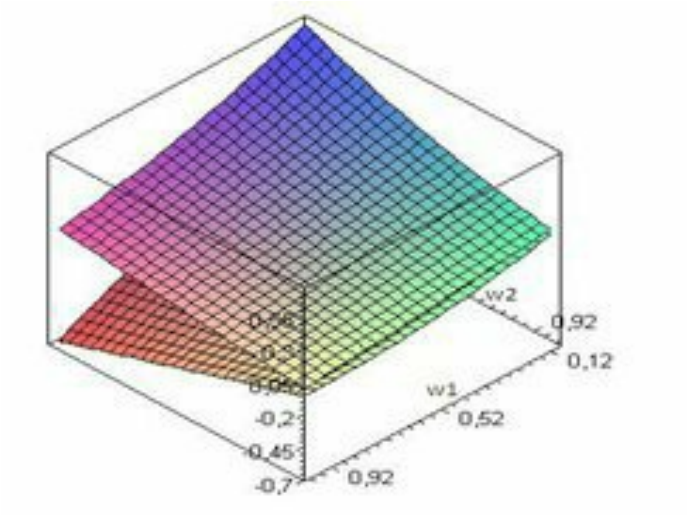


Figure 8: Mutual informations I_{AB} and I_{AE2} as function of rate of measure (ω_1, ω_2).

5 Conclusion

In this paper, by using the entropy measure and java simulation in quantum transmission, we have evaluated the probability of estimated error to see that the transmission is secured or not. In our analysis we have see that the secured zone is obtained when the value of $P_{error} < 0.25$ independently the number of spies. We have also see that when the frequency of measure of the spies increases, the value of the error increases and the exchange of key via the quantum channel is not secure.

References

1. C.E. Shannon, A mathematical theory of communication. Bell Syst. Tech. J. Vol. 27, pp. 379-324; 1948.
2. Bennett, C. H. Brassard, G., Robert, J. -M., Privacy amplification by public discussion, , SIAM Journal on Computing, Vol. 17, no. 2, pp. 210.299, April 1988.
3. Ch.H. Bennett, G.Brassard, Quantum cryptography: Public key distribution and coin tossinh. In Proceedings of the IEEE International Confrence on Computers Systems and Signal Processing, Bangalore, India IEEE, New York, pp. 175-179, 1984.
4. B. Ouchao and E. H. El Kinani, Statistical analysis of common qubits between Alice and Bob in BB84 protocol. Contemporary Engineering Sci- ences, Vol. 4, no.8, 363-370, 2011.
5. J. Preskill. Quantum Computing: Pro and Con. J o u r n a l - r e f : Proc.Roy.Soc.Lond. A454 469-486, 1998.
6. C. Bennett. Notes on the history of reversible computation. IBM J. Res. Dev. 32:16, 1998.

How to Cite this Article: B. Ouchao, E.H. El Kinani, "Analysis of the Influence of the Rate of Spies' Measure on the Quantum Transmission," Science Journal Of Mathematics and Statistics, Volume 2012 (2012), Article ID sjms-223, 6 Pages, doi: 10.7237/sjms/223