Journal of Computer Science 3 (6): 424-429, 2007
ISSN 1549-3636

Stop Conditions Of BB84 Protocol Via A Depolarizing Channel (Quantum Cryptography)

Iyed Ben Slimen, Olfa Trabelsi, Houria Rezig, Ridha Bouallègue and Ammar Bouallègue
Laboratoire Systèmes de Communication Ecole Nationale d'Ingénieurs de Tunis
1002 Le Belvédère, Tunis, Tunisia

Abstract: BB84 (Bennett and Brassard 1984) is one of the well known protocols of quantum keys distribution. It is built to allow two interlocutors commonly called Alice and Bob to share two similar binary keys and to detect the eavesdropper presence (the eavesdropper is commonly called Eve). However, Eve presence in a disturbed environment causes errors to the sifted keys and decreases the amount of secure information between Alice and Bob. One of the most important stages in BB84 protocol is to decide by using error probability estimation if we can continue the protocol phases or no. Indeed, this decision is function of some factors like: what is the amount of information that we will lose in the error correction phase? What is the degree of errors detected in our sifted keys? What is the origin of these errors: Eve strategy or the channel disturbance? For these reasons, we will study in this study some conditions to stop BB84 protocol in the context of depolarizing channel. We implement two types of eavesdropping strategy: Intercept and Resend and Cloning Attack.

Key words: Error probability, secure information, decision threshold, sifted keys

INTRODUCTION

It's known that the security of symmetric cryptography is mathematically proven [1]: Eve cannot have information about message transmitted by Alice to Bob if they use two common binary random keys at the same message length. To have unique keys for each message is impossible; this fact isn't allowed by transmission supports and techniques. Quantum cryptography or Quantum Distribution keys (QKD) is a new field of cryptography specialized to resolve this problem of sharing keys between these two interlocutors [2]. Since 1984, more and more protocols are implemented beginning by BB84 [1, 3] and arriving to SARG04 (Scarani-Acin-Ribordy-Gisin 2004) [4]. Note that BB84 and SARG04 are not different in quantum phase which is our study subject. It also approaches experimental results exposed in article [4] with multiple attacks. Moreover, it's obvious that security research is oriented to experiments reality which can't envisage future problems. Technology developments will permits to Eve more and more efficient procedures that can't be realized actually. Having theory models is so necessary to estimate future problems of security. For example, we note that cloning attack can't be experimentally implemented with our actual technology means but its optimality obliges the researchers to consider it in models as forecast to future Eve strategies [5, 6]. For these reasons, beginning with security notions our contribution consists of giving some criteria to stop or continue BB84 (or SARG04) protocol. We model errors origins like Eve presence and depolarizing channel - equivalent channel with Binary Symmetric channel in classical terms [7].

This study will be divided into four parts: the first relates to a necessary detailed description of our error sources models. The second and third parts will provide the stop conditions and criteria of the BB84 protocol after the quantum communication: we begin with Intercept and Resend spread in its use and finish with cloning attack which danger comes form its optimality. We will end carrying out comparative discussions between the various eavesdropping techniques and gives efficiency study by knowing depolarizing parameter.

Error sources modelling: Protocol BB84 like any other protocol of quantum cryptography is based on two principal phases: a quantum phase via a one-way physical quantum channel and a public phase using an authenticated two-way classic ideal channel [8, 9]. We note that the channel notion changes according to study point of view [10]. Indeed, in this article we use the term "channel" without adjective for all imperfections which

Corresponding Author: Iyed Ben Slimen, Laboratoire Systèmes de Communication Ecole Nationale d'Ingénieurs de Tunis 1002 Le Belvédère, Tunis, Tunisia

lead to the sifted keys - binary sequences obtained after public discussion compatibility of bases. Consequently, it includes the eavesdropping strategy used and the physical quantum channel (sources, detectors, optical fibers…). During our study, we chose as physical channel model the depolarizing one which is mathematically considered as unitary operator T_p [7]

$$T_p(|\psi\rangle) = (1-p)|\psi\rangle\langle\psi| + \sum_{i=1}^{3}\frac{p}{3}\sigma_i|\psi\rangle\langle\psi|\sigma_i^{\uparrow} \quad (1)$$

Depolarizing channel leaves intact a qubit $|\psi\rangle$ with probability (1-p) or applies one of the Pauli matrices σ_i ($\neq$ identity matrix) with probability p/3 for each one; p is called the depolarizing parameter.

Another error source that we must consider is the eavesdropping presence. Indeed, considering the effects independence of the eavesdropper and the depolarizing channel, a state sent by Alice can follow one of the two transmission ways (Fig.1) with respective probabilities (1-q) and q. Considering only the depolarizing channel effect (without Eve presence), we show in other work that the error probability P_e is equal to 2p/3 [11].

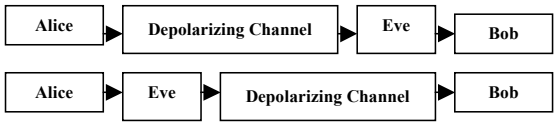

Fig. 1: Analysis model

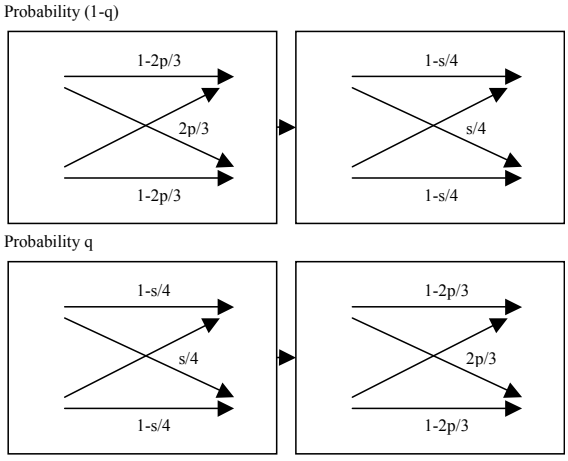

Fig. 2: Analysis model with intercept and resend eavesdropping (Alice-Bob)

Stop conditions (Intercept and resend eavesdropping case): Intercept and Resend is the most known eavesdropping strategy that can be implemented with actual technology means [5]. In the explanation terms: Eve replaces Bob by applying random bases measurements to some qubits and each result will be sent to Bob without any change. After Alice and Bob public discussion about their bases measurements choices (to eliminate incompatible ones), Eve, by observing the two interlocutors decision to build sifted keys via the authenticated public channel, construct her one by leaving bits that correspond to Alice and Bob incompatibility measurements. We define for this eavesdropping strategy the probability s that one qubit sent by Alice to Bob is eavesdropped. If we consider only Eve effect, we can prove that the error probability is equal to s/4 [12]. Thus, our analysis model (Fig.1) can be transformed with another form (Fig.2). By computing conditional probabilities (equations 2 and 3) between Alice and Bob, we show that they are independent of q and that error probability is given by equation 4.

$$p(0/1) = p(1/0) = \frac{2p}{3}(1-\frac{s}{4}) + \frac{s}{4}(1-\frac{2p}{3}) \quad (2)$$

$$p(0/0) = p(1/1) = (1-\frac{2p}{3})(1-\frac{s}{4}) + \frac{sp}{6} \quad (3)$$

$$P_e = \frac{s}{4} + \frac{p}{3}(2-s) \quad (4)$$

Immediately, average mutual information between Alice and Bob is obtained by using this equation:

$I_{AB}=p(0/0)\log_2(2p(0/0)) + p(1/0)\log_2(2p(1/0))$ (5)

Moreover for computing average mutual information between Alice and Eve we use an analogue model to that given in Fig.2 (Fig.3).

Conditional probabilities between Alice and Eve are with q = ½:

$$p(0/1) = p(1/0) = \frac{p}{3}\left(\frac{1}{2}+\frac{s}{4}\right) + \left(1-\frac{p}{3}\right)\left(\frac{1}{2}-\frac{s}{4}\right) \quad (6)$$

$$p(0/0) = p(1/1) = \frac{p}{3}\left(\frac{1}{2}-\frac{s}{4}\right) + \left(1-\frac{p}{3}\right)\left(\frac{1}{2}+\frac{s}{4}\right) \quad (7)$$

Note: q is not valid for s = 0.

Thus, average mutual information between Alice and Eve is computed:

$I_{AB}= p(0/0)\log_2(2p(0/0)) + p(1/0)\log_2(2p(1/0))$ for $s\neq 0$

$I_{AB}= 0$ for $s = 0$ (8)

An important parameter to study security of a quantum cryptography protocol is secure information (or secret information) given by this equation [5]:

$$I_s = I_{AB} - I_{AE} \quad (9)$$

Like error probability, this parameter can be plotted as function of depolarizing parameter p and eavesdropping probability s. We can define a threshold of secure information ε below that BB84 protocol must be stopped. But, the only parameter that can be easily reached by the two interlocutors is error probability. Alice and Bob can choose random bits which are compared by public discussion and thus permit to have

an error rate (an estimation of error probability). It should be noted that bits used to estimate this probability must be eliminated in order to avoid the increase of Alice-Eve average mutual information[1, 2]. We represent in (Fig.4) secure information as function of error probability for different p and s values.

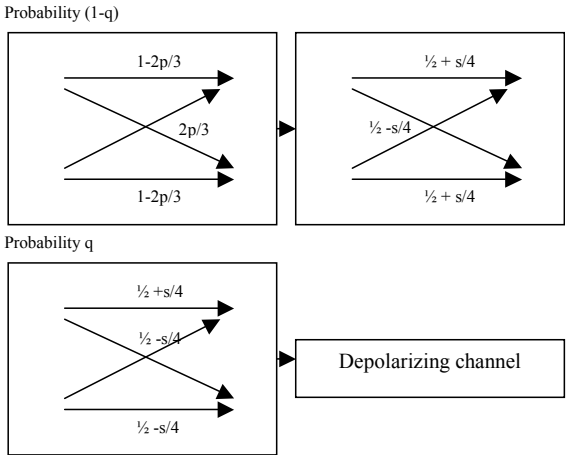

Fig. 3: Analysis model with intercept and resend eavesdropping (Alice-Bob)

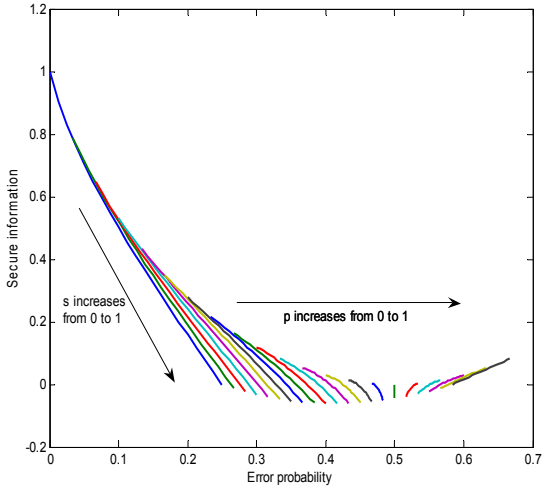

Fig.4: Secure information as function of error probability (for Intercept and Resend eavesdropping)

If the two interlocutors choose a decision threshold of secure information ε below that they stop protocol, they choose in other terms a decision threshold of error probability P_{emax} - a limit of error probability tolerated between Alice and Bob. Note that if we haven't an estimation of our channel p-value we can work with p = 0. For this condition, some thresholds are presented in Table. 1

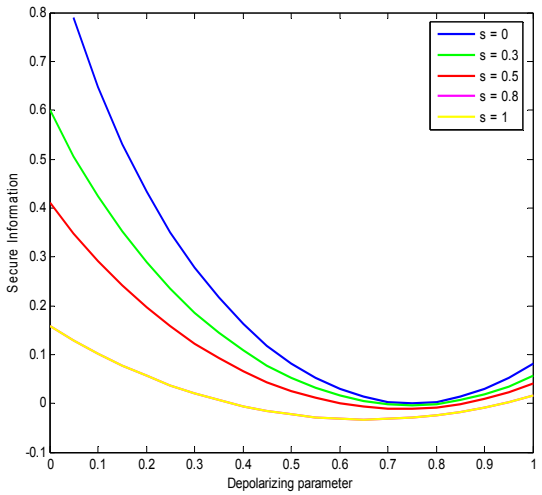

Fig.5: Secure Information as function of depolarizing parameter for different s-values (for Intercept and Resend eavesdropping)

Table 1: Threshold decision of error probability as function of threshold decision of secure information (for Intercept and Resend eavesdropping)

ε	1	0.7064	0.5020	0.1594	0
P_{emax}	0	0.05	0.1	0.2	0.25

In order to have an efficient protocol ε must be between two values: a min value ε_{min} and a max value ε_{max}. If we choose ε out of this stroke, the protocol will be automatically stopped (efficiency problem). These limit-values are function of depolarizing parameter (Fig.5). As you see, we can consider that ε_{max} as secure information for s = 0 and ε_{min} as secure information for s = 1. It should be noted that $\varepsilon_{min} \geq 0$; for this reason $\varepsilon_{min} = 0$ ∀ p (Table.2).

Table 2: Secure information stroke as function of depolarizing parameter (for Intercept and Resend eavesdropping)

P	0	0.2	0.5	075	1
ε_{min}	0	0	0	0	0
ε_{max}	1	0.4335	0.0817	0	0.0817

Stop conditions (cloning attack case): Cloning attack eavesdropping is an optimal attack. Indeed, Optimality comes owing to the fact that we obtain the minimum of secure information with this strategy compared to the others. In the explanation terms: Eve uses a unitary operator U called cloning transform. This operator can approach the cloning act which is impossible in quantum theory (non-cloning theorem) [5]:

$$U : H_{AE} \rightarrow H_{AE}$$
$$U\left(|0\rangle_{yA}|0\rangle_{yE}\right) = |0\rangle_{yA}|0\rangle_{yE}$$
$$U\left(|1\rangle_{yA}|0\rangle_{yE}\right) = \cos(\theta)|1\rangle_{yA}|0\rangle_{yE} + \sin(\theta)|0\rangle_{yA}|1\rangle_{yE}$$
$$\theta \in \left[0, \frac{\pi}{2}\right] : attack\ \ force \quad and \quad H_{AE} = H_A \otimes H_E \tag{10}$$

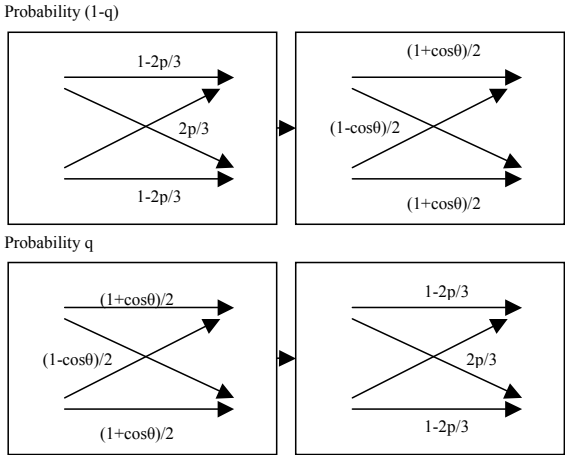

Fig. 6: Analysis model with cloning attack eaves dropping (Alice-Bob)

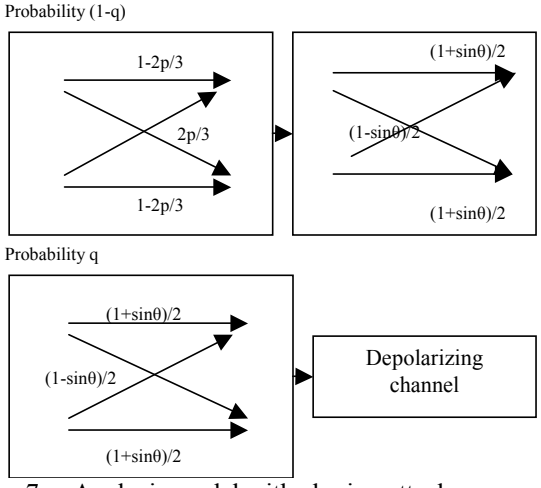

Fig. 7: Analysis model with cloning attack eaves dropping (Alice-Bob)

The symbols H_A and H_E indicate respectively the spaces states of Alice and Eve. Moreover, note that this operator is defined in y-base (diagonal base). If $|\psi\rangle$ is the ket sent by Alice, Eve apply the unitary operator U and send only the qubit concerned by Alice [12]. She stores her qubit and decides to measure it after public discussion between the tow interlocutors about their compatibility bases. So, if we consider only Eve effect, we can prove that the error probability is equal to (1-cosθ)/2. Thus, our analysis model (Fig.1) can be transformed with another form (Fig.6).

By computing conditional probabilities (equations 11 and 12) between Alice and Bob, we show that they are independent of q and that error probability is given by equation 13.

$$p(0/1) = p(1/0) = p\left(\frac{1+\cos\theta}{3}\right) + \left(\frac{1-\cos\theta}{2}\right)\left(1-\frac{2p}{3}\right) \tag{11}$$

$$p(0/0) = p(1/1) = \left(1-\frac{2p}{3}\right)\left(\frac{1+\cos\theta}{2}\right) + \left(\frac{1-\cos\theta}{3}\right)p \tag{12}$$

$$P_e = \frac{1-\cos\theta}{2} + \frac{2p\cos\theta}{3} \tag{13}$$

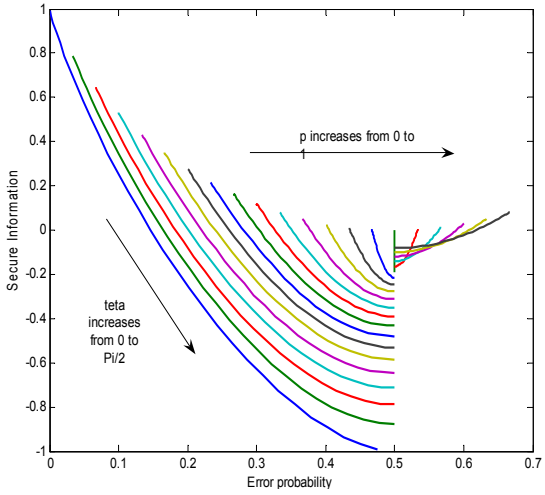

Fig.8 Secure information as function of error probability (for Intercept and Resend eaves dropping)

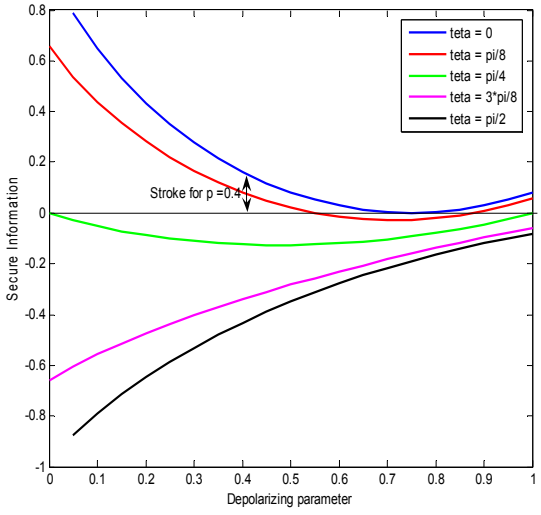

Fig. 9: Secure Information as function of depolarizing parameter for different θ-values (for cloning attack eaves dropping)

Immediately, Information between Alice and Bob is obtained by using equation 5. Moreover for

computing Information between Alice and Eve we use an analogue model to that given in Fig.2 (Fig.7).
Conditional probabilities between Alice and Eve are with q = ½:

$$p(0/1) = p(1/0) = \frac{p}{3}\left(\frac{1}{2} + \frac{\sin\theta}{2}\right) + \left(1 - \frac{p}{3}\right)\left(\frac{1}{2} - \frac{\sin\theta}{2}\right) \quad (14)$$

$$p(0/0) = p(1/1) = \frac{p}{3}\left(\frac{1}{2} - \frac{\sin\theta}{2}\right) + \left(1 - \frac{p}{3}\right)\left(\frac{1}{2} + \frac{\sin\theta}{2}\right) \quad (15)$$

Note: q is not valid for s = 0.

Thus, information between Alice and Eve is computed also by using equation 8. In addition to that, we determine the secure information immediately. This parameter can be plotted as function of depolarizing parameter p and attack force θ. We can define also a threshold of secure information (and obviously of error probability) ε below that BB84 protocol must be stopped. We represent in Fig.7 secure information as function of error probability for different p and θ values. It also could be noted that if we haven't an estimation of our channel p-value we can work with p = 0. For this condition, some thresholds are presented in Table. 3

Table.3: Threshold decision of error probability as function of threshold decision of secure information (for Cloning attack eavesdropping)

ε	1	0.5859	0.4598	0.1758	0
P_{emax}	0	0.0480	0.0711	0.1135	0.1464

Similarly and for protocol efficiency, ε must be between two values: ε_{min} and ε_{max} (Fig.9).

DISCUSSION

The choice of decision threshold is so crucial to continue or stop the BB84 protocol. This choice must be below a maximum value- function of depolarizing parameter:

$$\varepsilon_{max} = \frac{2p}{3}\log_2\left(\frac{4p}{3}\right) + \left(1 - \frac{2p}{3}\right)\log_2\left(2 - \frac{4p}{3}\right) \quad (16)$$

Note that this equation is independent of eavesdropping technique. Indeed, some remarks must be given:

* If we don't know the p-value, the choice of ε must be uniform between 0 and 1. The probability $p(\varepsilon \le \varepsilon_{max}) = \varepsilon_{max}$ can define the protocol efficiency. This efficiency is function of p; it decreases by increasing p (for $p \le 0.75$).
* If we know a max value of p (for example $p_1 \le 0.75$) we can compute immediately $\varepsilon_{max}(p_1)$ and effectively we can increase efficiency to the maximum by choosing ε uniformly between 0 and $\varepsilon_{max}(p_1)$. Indeed, we obtain $p(\varepsilon \le \varepsilon_{max}) = 1$.
* If we know exactly the p-value for the depolarizing channel, by choosing ε uniformly between 0 and $\varepsilon_{max}(p)$ the efficiency is 100%. In addition to that, this information (knowing p-value) increases the possibility of having more secret after error correction [13].

Note: The efficiency notion discussed in this part concerns only the efficiency of our choice of decision threshold.

Moreover, we can prove that upper and lower bound given in article [14] for BB84 protocol with one-way communication corresponds to our model: depolarizing channel + attack cloning (by varying p). It also approaches experimental results exposed in article [15] with multiple attacks.

REFERENCES

1. Gisin, N., G. Ribordy, W. Tittel and H. Zbinden, 2002. Quantum Cryptography, Reviews of modern physics, 74: 145-195.
2. Nielson, M. and I. Chuang, 2000. Quantum Computation and Quantum Information, Cambridge University Press.
3. Zbinden, H., N. Gisin, B. Huttner, A. Muller and W. Tittel, 1998. Practical Aspects of Quantum Cryptographic Key Distribution, J. Cryptology.
4. Branciard, C., N. Gisin, B. Kraus and V. Sacarni, 2005. Security of two Quantum Cryptography protocols using the same four qubits states, Physical Review A, Vol. 72.
5. Florence, D., V. Didier and W. Vincent, 2003. La Cryptographie Quantique, Printemps des Sciences.
6. Fushs, C., N. Gisin, R. Griffiths, C. Niu and A. Pres, 1997. Optimal eavesdropping in Quantum Cryptography. I", Physical Reviews, 56: 1163.
7. Paquin, C., 2000. Les codes correcteurs Quantiques et leurs applications Cryptographiques, Université de Montréal.
8. Bennett, C. and G. Brassard, 1984. Quantum Cryptography Public Key Distribution and Coin Tossing, Proceedings of IEEE Inter. Conference on Computers. Systems and Signal Processing, India, pp: 175-179.
9. Hendrych, M., 2002. Experimental Quantum Cryptography Palacký University.

10. Moon, K., 2005. Error Correction Coding: Mathematical Methods and Algorithms.
11. Trabelsi, O., I. Ben Slimen, H. Rezig and A. Bouallègue, 2007. On the security of BB84 and Six-States over a Quantum depolarizing channel with Intercept/Resend attack, TIEGERA, Hammamet.
12. Ben Slimen, I. and H. Rezig, 2005. Etude et calcul des paramètres informationnels pour les protocoles crypto-optiques par méthode statistique, JFMMA and Telecom'05, Rabat.
13. Brassard, G. and L. Salvail, 1993. Reconciliation of a secret key through public discussion, Advances in Cryptology - Eurocrypt'93, pp: 410-423.
14. Gottesman, D. and Hoi-Kwong Lo, 2003. Proof of Security of Quantum Key Distribution with two-way classical communications, IEEE Transactions on Information Theory, 49: 457-475.
15. Renner, R., 2005. Security of Quantum Key Distribution, Swiss Federal Institute of Technology Zurich.