QKD PROTOCOLS – SOFTWARE IMPLEMENTATION BENNET-BRASSARD vs. BRUSS

Gabriela MOGOS*, **Gheorghe RADU****

*Escuela Superior Politecnica de Chimborazo, Riobamba, Ecuador,
**"Henri Coandă" Air Force Academy, Braşov, Romania

Abstract: *Quantum cryptography, and especially quantum key distribution systems – Quantum Key Distribution, realizes a quantum key exchange between the sender and the receiver. The quantum key exchange is made in two steps, by a quantum channel and a public channel. The most important characteristic of a quantum key distribution system, and especially of quantum cryptography, is that no attempt to intercept the communication can be performed, and that it also alerts the legitimate parties who communicate.*

The purpose of this paper is to present comparative studies regarding the percentage of errors from the key for two Quantum Key Distribution protocols: Bennett-Brassard and Bruss. The studies were done for two situations: the absence and the presence of cyber-attacks, and they analyze the degree of security of the protocols.

Keywords: *security, quantum cryptography, qubits.*
MSC2010**:** 81P45, 94A15.

1. INTRODUCTION

The security of conventional encryption depends on two main aspects: the encryption algorithm, and the encryption key.

The encryption algorithm, which should be powerful enough in order to make impossible the decryption based only on the encrypted text.

The encryption key should be big enough to assure a powerful encryption, and most of all, it should be secret.

Quantum cryptography offers new methods to secure the communications.

As compared to classical cryptography, which involves different mathematical algorithms to secure the information, quantum cryptography is focused on the physical support of the information.

Using the principles of quantum physics, we can create and implement a communication system with the purpose to always detect any attempt of attack, due to the fact that any attempt to "measure" a quantum carrier of information will modify the carrier particle, and will leave "traces".

The search for good security criteria under stringent conditions led to early studies of quantum eavesdropping, and finally to the first proof of the security of key distribution.

There are several methods of detection of attacks on quantum key distribution systems.
(1)The classical method – the identification of qubits altered by the enemy;
(2) QBER – the estimation of the error rate from the primary key;
(3) Bell's inequality.

Quantum Bit Error Rate (QBER) consists in the calculation of the percentage of errors from the key, obtained at the end of the quantum transmission, after the step of communication of the polarization bases from the public channel.

Quantum Bit Error Rate method for detection of the enemy may be applied to most of the key distribution systems. Each system has its own accepted error rate, and exceeding it means the intervention of an enemy. Using QBER method for determining the percentage of errors from the key, this paper presents a comparative study between two protocols: Bennett-Brassard and Bruss, in the absence of intruders, and in their presence, by an Intercept-Resend cyber-attack.

2. BENNETT-BRASSARD and BRUSS PROTOCOLS – SHORT OVERVIEW

2.1 Bennett-Brassard protocol. Charles Bennett from IBM, together with Gilles Brassard from the University of Montreal (1984; 1985), starting from Stephen Wiesner's study "Conjugate Coding" [3], developed a key distribution protocol using polarized photons.

The polarization states form two orthonormal bases as follows: a linear basis for linear polarization, and a diagonal basis for circular polarization. The states of the diagonal basis are polarization states at $\pm 45^0$ of the states of the rectilinear basis. The Bennett-Brassard protocol (BB84) [1] [2] is as follows:

The Sender sends to *the Receiver* a row of polarized photons.

The Receiver, using randomly one of the two bases, will measure each photon. In the absence of the noise, or of an intruder, *the Sender* and *the Receiver* will obtain the same measurement result if they choose the same basis. Using a public channel, *the Receiver* communicates to *the Sender* the measurement basis he had used, without revealing the result obtained. When the measurement bases are not well chosen, the results will be erased. The sequence of bits thus obtained is called *raw key*. The encryption key obtained with the help of Bennett-Brassard protocol (BB84) is the "one time pad" type, and cannot assure a "perfect security", because there are situations of "denial" of the message ownership (the sender encrypts the message with the key obtained, and after sending it, he pretends that the message was encrypted with another key).

2.2 Bruss protocol. In 1998, Bruss [4] proposes an extension to the Bennett-Brassard protocol into a six-state, with three complementary bases protocol. The six-state protocol is quite similar with BB84, but *the Sender* sends one of six states instead of one of four.

The Receiver chooses to measure randomly in one of the three bases, and again, *the Sender* and *the Receiver* discard any bits for which they used different bases.

The security analysis of the six-state protocol shows that *the Eavesdropper*'s information gain for a given impaired error rate is lower than in the BB84 protocol.

3. BB84 vs. BRUSS

The purpose of this paper is to present a comparative study regarding the percentage of errors from the key obtained by the two protocols.

Consequently, we made a software application for each protocol: Bennett-Brassard and Bruss, and we measured the percentage of errors from the key in two cases: in the absence, and in the presence of a cyber-attack.

We studied the most common cyber-attack on quantum protocols, which is Intercept-Resend attack.

Each simulation was realized with the help of a circuit containing 3 computers o which a module of the application was running, each of them communicating by a switch.

The connection between the computers was made by a UTP cable, simulating the quantum channel, as well as the classical channel.

The modules of each application will run on each of the 3 computers: *the Sender*, *the Receiver*, and in the case of *Intercept-Resend* cyber-attack – *the Eavesdropper*.

The modules are written in C++ language.

In this research, we did not take into consideration the errors appeared due to the equipment.

We tested the application on a variable number of input data (qubits), and we studied how the errors varied.

3.1. The ideal case. After running 10 times of each application, for the ideal case, we obtained the following results for an initial key with sizes ranging from 160 to 2560 qubits.

***Bennett-Brassard protocol* – results**

nr crt	Initial qubits = 160		Initial qubits = 320		Initial qubits = 640		Initial qubits = 1280		Initial qubits = 2560	
	Final bits	QBER (%)	Final bits	Eroare (%)	Final bits	Eroare (%)	Final bits	Eroare (%)	Final bits	Eroare (%)
1	81	50	166	49	298	54	669	48	1312	49
2	86	47	160	50	327	49	664	49	1338	48
3	91	44	157	51	319	51	617	52	1267	51
4	70	57	181	44	309	52	652	50	1331	49
5	78	52	169	48	317	51	640	50	1344	48
6	75	54	149	54	314	51	645	50	1234	52
7	82	49	158	51	316	51	644	50	1300	50
8	84	48	176	45	329	49	626	52	1254	52
9	91	44	159	51	317	51	633	51	1288	50
10	81	50	162	50	313	52	641	50	1337	48

Fig.1. Values of QBER depending on Initial number of qubits.

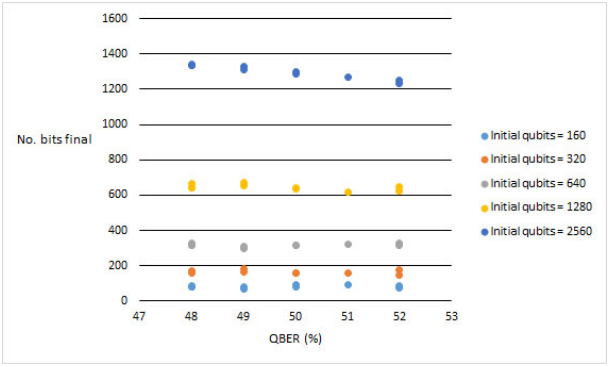

Fig.2. Variation of the error according to the dimension of the input data.

***Bruss protocol* – results**

nr crt	Initial qubits = 160		Initial qubits = 320		Initial qubits = 640		Initial qubits = 1280		Initial qubits = 2560	
	Final bits	QBER (%)	Final bits	Eroare (%)	Final bits	Eroare (%)	Final bits	Eroare (%)	Final bits	Eroare (%)
1	81	50	166	49	298	54	669	48	1312	49
2	86	47	160	50	327	49	664	49	1338	48
3	91	44	157	51	319	51	617	52	1267	51
4	70	57	181	44	309	52	652	50	1331	49
5	78	52	169	48	317	51	640	50	1344	48
6	75	54	149	54	314	51	645	50	1234	52
7	82	49	158	51	316	51	644	50	1300	50
8	84	48	176	45	329	49	626	52	1254	52
9	91	44	159	51	317	51	633	51	1288	50
10	81	50	162	50	313	52	641	50	1337	48

Fig.3. Values of QBER depending on Initial number of qubits.

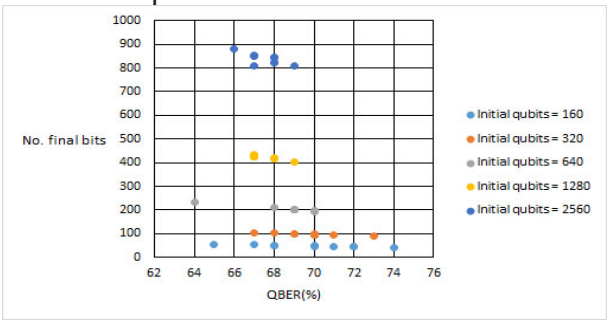

Fig.4. Variation of the error according to the dimension of the input data.

We can see that in the case of Bruss protocol, QBER is bigger than in the case of BB84.

Although the communication is realized in secure conditions, it is important to know that in the case of Bruss protocol, the receiver had to choose a single measurement basis of 3 for reading the qubit, while in the case of BB84 protocol, the receiver needs to decide over one of the two measurement bases.

For the ideal case, we conclude that in Bennett-Brassard protocol, the probability to measure a qubit correctly is 1/4, while in Bruss protocol the probability is 1/6.

3.2. The cybernetic attack – case. The theoretical and practical vulnerabilities of quantum key distribution systems have always constituted the main starting point of the methods of attack on these systems.

In this part of the paper, we propose the implementation of the applications of BB84 and Bruss protocols – with eavesdropper, together with the data sets obtained from running the applications.

The *Intercept-Resend* attack [6] is the most common type of attack used on quantum key distribution systems.

The Eavesdropper interrupts the quantum channel, measures each qubit received from the *sender* in one of the measurement bases (according to the protocol), which he had chosen randomly. Then he sends the qubits read to *the Receiver*, and he will replace the compromised qubits with others, without leaving traces of the attack [5].

After running each application for 10 times, we obtained the following results for an initial key with sizes ranging from 160 to 2560 qubits.

***Bennett-Brassard protocol* - results**

Initial - 160				Initial qubits - 320				Initial qubits - 640				Initial qubits - 1280				Initial qubits - 2560			
No final bits Receiver - Inamic	No final bits Emittor - Inamic - Receiver	QBER Emittor-Inamic (%)	QBER Emittor - Inamic - Receiver (%)	No final bits Receiver-Inamic	No final bits Emittor - Inamic - Receiver	QBER Emittor-Inamic (%)	QBER Emittor - Inamic - Receiver (%)	No final bits Receiver-Inamic	No final bits Emittor - Inamic - Receiver	QBER Emittor-Inamic (%)	QBER Emittor - Inamic - Receiver (%)	No final bits Receiver-Inamic	No final bits Emittor - Inamic - Receiver	QBER Emittor-Inamic (%)	QBER Emittor - Inamic - Receiver (%)	No final bits Receiver-Inamic	No final bits Emittor - Inamic - Receiver	QBER Emittor-Inamic (%)	QBER Emittor - Inamic - Receiver (%)
81	39	50	24	166	80	49	25	298	152	54	24	669	269	48	21	1312	614	49	24
86	41	47	26	160	77	50	24	327	149	49	23	664	307	49	24	1338	666	48	26
91	42	44	26	157	82	51	26	319	155	51	24	617	333	52	26	1267	589	51	23
70	36	57	23	181	79	44	25	309	159	52	25	652	307	50	24	1331	640	49	25
78	43	52	27	169	81	48	25	317	162	51	25	640	294	50	23	1344	640	48	25
75	40	54	25	149	74	54	23	314	160	51	25	645	320	50	25	1234	691	52	27
82	44	49	28	158	76	51	24	316	148	51	23	644	333	50	26	1300	614	50	24
84	41	48	26	176	80	45	25	329	166	49	26	626	346	52	27	1254	666	52	26
91	37	44	23	159	78	51	24	317	168	51	26	633	307	51	24	1288	640	50	25
81	42	50	26	162	83	50	26	313	149	52	23	641	320	50	25	1337	666	48	26

Fig.5. Values of QBER depending on Initial number of qubits.

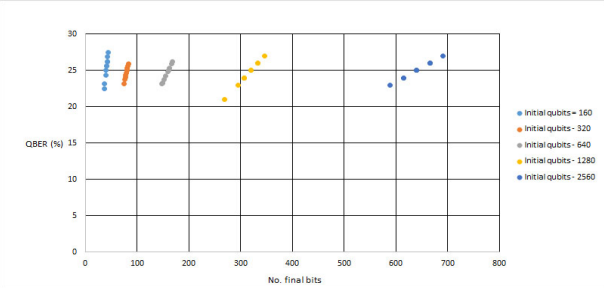

Fig.6. Variation of the error according to the dimension of the input data

***Bruss protocol* - results**

No final bits Receiver - Inamic	No final bits Sender - Inamic - Receiver	QBER Sender-Inamic (%)	QBER Sender - Inamic - Receiver (%)	No final bits Receiver-Inamic	No final bits Sender - Inamic - Receiver	QBER Sender-Inamic (%)	QBER Sender - Inamic - Receiver (%)	No final bits Receiver-Inamic	No final bits Sender - Inamic - Receiver	QBER Sender-Inamic (%)	QBER Sender - Inamic - Receiver (%)	No final bits Receiver-Inamic	No final bits Sender - Inamic - Receiver	QBER Sender-Inamic (%)	QBER Sender - Inamic - Receiver (%)	No final bits Receiver-Inamic	No final bits Sender - Inamic - Receiver	QBER Sender-Inamic (%)	QBER Sender - Inamic - Receiver (%)
48	17	70	11	166	59	49	19	298	110	54	17	669	239	48	19	1312	614	49	24
52	19	68	12	160	57	50	18	327	121	49	19	664	237	49	19	1338	666	48	26
49	18	70	11	157	56	51	18	319	118	51	18	617	220	52	17	1267	589	51	23
47	17	71	10	181	65	44	20	309	114	52	18	652	233	50	18	1331	640	49	25
54	19	67	12	169	60	48	19	317	117	51	18	640	229	50	18	1344	640	48	25
43	15	74	10	149	53	54	17	314	116	51	18	645	230	50	18	1234	691	52	27
46	16	72	10	158	56	51	18	316	117	51	18	644	230	50	18	1300	614	50	24
52	19	68	12	176	63	45	20	329	122	49	19	626	224	52	17	1254	666	52	26
57	20	65	13	159	57	51	18	317	117	51	18	633	226	51	18	1288	640	50	25
45	16	72	10	162	58	50	18	313	116	52	18	641	229	50	18	1337	666	48	26

Fig.7. Values of QBER depending on Initial number of qubits.

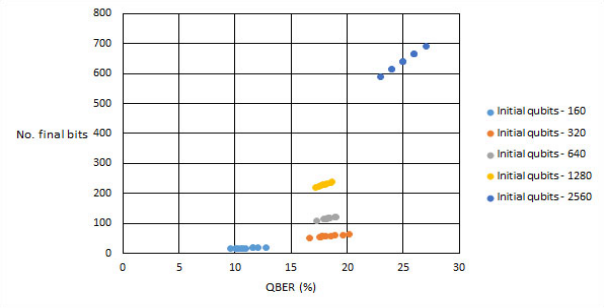

Fig.8. Variation of the error according to the dimension of the input data.

In the case of a cyber-attack, *the Eavesdropper* will send to *the Receiver* a part of the qubits, only the ones which he managed to measure, the rest of the qubits being false.

On his turn, during the process of reconciliation Sender-Receiver, *the Receiver* will introduce his own error when reading the qubits, by randomly choosing the qubits received from the Intruder from the measurement bases.

At the end of the process, both *the Sender* and *the Receiver* will see that the percentage of errors from the key is very big, which proves the existence of an intruder, and they will give up the protocol.

CONCLUSIONS

As a result of the data previously presented, we may conclude that the simplest method to detect the *Intercept-Resend* attacks on Quantum Key Distribution protocols is to measure the percentage of errors from the key.

Consequently, for a simpler detection of the intruders acting by Intercept-Resend attacks, the parties need to run the Quantum Key Distribution protocol for the ideal case (secure communication environment), where the possible errors could be only due to the equipment.

At the end, the parties may establish a maximum admitted upper limit of these errors.

If after running a Quantum Key Distribution protocol in an unsecure environment the value of the errors is higher than the maximum admitted limit, it means that the whole process was compromised by the presence of an intruder.

Thus, for Bruss scheme, the raw key consists of one-third of the qubits received on average, as opposed to one-half for BB84, and we can see, the Bruss protocol remains secure under an eavesdropper attack.

Acknowledgment:
This work was financed by the Prometeo Project of the Ministry of Education Superior, Science, Technology and Innovation of the Republic of Ecuador.

BIBLIOGRAPHY

1. Bennett C.H., Bessette F., Brassard G., Salvail L. and Smolin J. *Journal of Cryptology*, 1992.
2. Bennett C.H. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68, pp. 3121-3124, 1992.
3. Wiesner S. Conjugate coding. *Sigact News* 15, pp.78-79, 1983.
4. Bruss D., *Phys. Rev. Lett. 81*, 3018, 1998.
5. Gisin N., Ribordy G., Tittle W., Zbinden H., Quantum cryptography, *Reviews of Modern Physics*, vol. 74, 2002.
6. Makarov V., Anisimov A., Skaar J., Effects of detector efficiency mismatch on security of quantum cryptosystems, *Physical Review A*, vol. 74, pp. 1-11, 2005.