# **QKD** Simulation

Gabriela Mogos

Facultad de Informatica y Electronica, Escuela Superior Politecnica de Chimborazo, Riobamba, Ecuador gabi.mogos@gmail.com

### Introduction

The goal of this study is to understand the alternatives to classical protocols for obtaining cryptographic keys that can be used as substitutes, should quantum computers be realized.

This study explores quantum alternatives to traditional key distribution protocols and involves implementations of Quantum Key Distribution protocol - Bennett-Brassard (BB84) on 2 cases: with and without cyber-attacks.

## Implementation

#### I. Bennett-Brassard without eavesdropper

The study will present the results obtained from the Bennett-Brassard (BB84) protocols software implementation. To implement BB84 protocols, we used C ++ language.

On first BB84 simulator, the emitter and the receiver will communicate safety, without the presence of the eavesdropper. To obtain the cryptographic key, both of them will execute the stages of the Bennett - Brassard protocol: bases reconciliation, reconciliation and privacy amplification secret key.

The equipment used for the deployment of simulation of BB84 protocol are computers connected by switches. Each computer has a static IP to communicate over the switch and on each computer will run specific programs: the Emitter and Receiver, respectively.

© EMITTER		- 🗆 🗡	٥		RECEIVER	×
Host: 127.0.0.1 Emitter Port: 888 Disc	connect		Emitter - Receiver	<	Host: 127.0.0.1	Disconnect
Emitter bases:					Porc 979	
DOLLILLDOLDLDODDDOLDLIDDDODDLDLDDDODDLDLDODLUDDLDDDDDDDDDD	XILIDDLILDDLDDDDDDDDDDDDDDDDDDDDDDDDDDD	Generate bases	Qubits emitter:			
Emitter qubits:			dcabababcdbdbcdccdd ccddcdbdadccdbbcdbb	bcabadcdddacbadddccbbaddad cbaaaabccbbbcbbbdcddbbd	bbbbdccaaadcaaaddbaaadbaa caddaadbcbbbccbdbbbbbbbbbb	bcdcbcdccbbcaddaccdbddbddaccbd bbcbcbacacadcddadddcadaacadddb
dcabababcdbcdccddcabadcdddachadddccbbaddacbbbbdccaaadcaaa adccbbcdbbbcabbbcbbbbcb	vddbaaadbaabcdcbcdccbbcaddaccd xaabbcbcbacacadcddadddcadaacad	bddbddacdbdcddd Iddbdbcfbddbdbdcdbd	Receiver bases:			
Emitter bits: 320			LDDLDDDLLDLDDDLDLD			Generate bases
1000000000000000000000000000000000000	00011100011001010101010101011011011101	0001111111000110011 0010000111101011101 52		Send ba	ses 🕢	
Reconciliation:			Reconciliation:			
"อาเมาของการของการและการของการของการของการของการของการของการของการของการของการของการของการของการของการของการของ	L1,D1,L1,10,L1,111,1,11,11,11,11,11,11,11,11,11,11,	00*L00L00L**L*D00 L*L****D0*****D0***DL	**************************************		10************************************	ւլ *****Ղ **ԾՂ Ղ ԾԼՇՕ ՂՇՕԼՇՕԼ *ՂԼԼԼ Ծ *Ծ Ղ *Ծ *ԾԾՕՇՕԼ ****Ղ Ղ *
Qubits:			Qubits:			
cbbdbdccdbaacbdcbacdcaaadbadbabcbadaccbddbddabccddbaad dccbbdacdbbddabccacbddddbbcbbbbabacdbbccaadccaadcbddadcd	bbbcbbbddbbdaadbbbbccbdbbbaai b	bccacdcddaaaddcddbbb	dbdbdccdbaadbddbdda bbdcdbbdacdbbdbbdda	:dcaaadbadbabcbadccbdbddabc abccacbddddcbbcbbbabacdbbcc	xddcbaccbbaabbbbcbbbddbbd aadcaadcbddadcdcb	aadbbbccbdbbaabccadcddaaddcdcb
Final key: 169			Final key: 169			
0111110011000110100100001101101010100001111	0011110111111110011111001111 11010101	1001000010110001101	011111001100011010 100011010111100111	10 10000 110 110 10 10 1100 11111 100 11111111	10 100 110 1000 1 100 1 111 1 1 1 1 1 10 100 1 1 10000 1 1000 10 1 1 1	11111001111100111110010000101 010101

Fig.1. Bennett-Brassard protocol ideal - without eavesdropper

We tested the application on a variable number of input data (qubits) and have studied how vary QBER.

After running 10 times the simulation program QKD - ideal, we obtained the following results for an initial key with sizes ranging from 320 to 2560 qubits:

Initial qub	oits = 160	Initial qubi	its = 320	Initial qub	its = 640	Initial qubi	ts = 1280	Initial qubi	its = 2560
No. final bits	QBER (%)	No. final bits	QBER (%)	No. final bits	QBER (%)	No. final bits	QBER (%)	No. final bits	QBER (%)
81	50	166	51	298	46	669	52	1312	51
86	53	160	50	327	51	664	51	1338	52
91	56	157	49	319	49	617	48	1267	49
70	43	181	56	309	48	652	50	1331	51
78	48	169	52	317	49	640	50	1344	52
75	46	149	46	314	49	645	50	1234	48
82	51	158	49	316	49	644	50	1300	50
84	52	176	55	329	51	626	48	1254	48
91	56	159	49	317	49	633	49	1288	50
81	50	162	50	313	48	641	50	1337	52

Fig.2. Values of QBER and Final key depending on Initial number qubits



Fig.3. Graphic representation of QBER and Final key depending on Initial number qubits

Analyzing the data obtained we can conclude that quantum bit error rate – QBER the final key is around 50%.

#### **II. Bennett-Brassard with eavesdropper**

The attack used by the enemy in BB84 simulation program is *Intercept-Resend* method. The *Intercept-Resend* attack, called the Fake-State, is the most common type attack used on quantum key distribution systems.

The Eavesdropper, interrupting the quantum channel, measure each qubit received from the Emitter and, then, the Eavesdropper transmits to Receiver other polarized qubits without leaving traces of the attack.

Use of two polarization bases, gives the Eavesdropper a chance to get about 50% of measurements compatible with qubits transmitted by the Emitter.

EMITTER -	C EAVESDROPPER - 🗖 🗙
Host: 127.0.0.1 Eavesdropper Port: 088 Disconnect	Eavesdropper - Emilter         Eavesdropper - Encidence           Nost: 227.0.0.1         Disconnect         127.0.0.1           Port: 1979         Port: 144         Connect
DODUDDOUDDODUDDODUDDOULDDOULDDODODULDDOUDDOU	emitter Receptor
dddabcrbbdrchdcaaddddabcadcabaddchadbbadbdaaccordabbaadbdaadbdcrcdabaacbddabbdcbbaaccbdaad bdbbddbbdabdacbdddabbdddabaacaaabcddbdcabdddaaabaddcaaabadaccaadbaaccdccadbdcddbbaacccbdbacccbdbaccbddca	Kitabi cibicicibiciasididde arfabadd a bibba da contable adhida tabbo contabe and do contabe and do contabe and do contabe and do biblicibid contabe and and an an and an and an an and an
mitter bits: 320	Eavesdropper bases:
110 000 1100 10 000 000 01110 000 000 0	IDE COROLA LA LIZOLI DA LILIU AL LICOCOCOLULIA LA LIZOLI DA LIZOLI
U         I         I           0         1         0         1           0         1         0         0	Reconclusion:
ecconciliation: +00x+00x+-01x+01x+0-0+01x+01x+00x+00x+-00x+00x+00x+-00x+00x+-00x+00x+	00.0001-01-00-0011-01-00-0-11-00-0-0-0-
Qubits:	Qubits:
ddacthdhdaddababadoradabcraachdcabdchcacccadbdoddbd bddabddbdddacaccdbcabddaadcccabaacddocch aaabacacaabcaaccadaadbaabbbabddadchcabdcaadcaacdbdcdabd	disch belad sha bad chab darada boraard sa boraard sa boraard sa bad bab bab da bab bab da da bab bab da da bab bab
inal key: 164	Final key: 164
1100010110110101010101010100000100001100110000	1100010110110101010101010000010000010000

Fig.4. Intercept-Resend attack (Emitter - Eavesdropper)

C RECEIVER		0	EAVESDROPPER	×				
		Eavesdr	pper - Emitter	Eavesdropper - Receiver				
EAVESDROPPER Port	2127.0.0.1 2333 Connect	Host: 127.0.0.1 Port: 999	nect (TB)	Host: 127.0.0.1 Port: 444				
Qubits eavesdropper: 320		Emitter Receptor						
daddabddabcdddadbabaabaccdcdbbbabcdbdababdcdabdbdcdb cbdcbbddbdbacacacacdbacbccbdcabbaadbdbabdcaccddcacdadadcc	cddcabdbcadbcacddabcdddaccabcabbbdbdccbdcb badabadbcadbbadcdbbbacaabbdadcddaabbadcd	Qubits emitter:						
Receiver bases:		dddabccbbdccbdcdaaddddabc aabddbbbddabbdcdacaaacbcd	adcabaddcbadbbbadbdaacccdabbaadbddadaabdcccda bdcabdbddcaaabadacccadbaaccdcccadbdcdcbbaaccd	baadbbdcabdcddbbcabacccbcacdcbdcdbdcdbdbbddcbbddcbdddc dbacccbddcadbbcbcdbdasasaabaaccacadacdbadaabbacaaccca				
	SUDDDDULDDUDDUDDUDDUDDUDDUDDUDDUDDUDDUDDU	Eavesdropper bases:						
			ILLDILLDDDDDDDLLLDLDLDLDDDDDDDLLLDDDLDDDLDDDD	DOLLDLDDDLDDDDDDDDDDDDDDDDDDDDDDDDDDDD				
Obtain final key	QBER (%) 48	Ba	ses to Emitter					
Reconciliation:		Reconciliation:						
D-0LL-LD-0-L-100L-0-0-0LDL-0-00L-LL-LD0-LLD-00DL-LLLD0-DLDD-0LD0-LD-L-00LD LLLLL-0-LD		00.001-01-01-0-0114-11-00-0-11-101-0-1-0-1-						
Qubits:		Qubits:						
ddaccbcbdaddababadcdbabdacadabccaacbdcabccaacbcdbdb cdbdasabacacaabcaaccadaadbaabbbabddadcbcabdcaadcaa	ddacthchaddababaducthabdacadabccaachdcabccaachdcbhchdobbchddabddbddacaccdbcabdaadcccabacddcccbddadbcdbdaaabacacaabaaccadaa dbaabbbabddadcbcabdcaacthdcdabd							
Final key: 167	Final key: 167			Final key: 164				
110001010110101010101010101001001000000	110001011011010101011011010000101000000							

Fig.5. Intercept-Resend attack (Emitter - Eavesdropper)

The probability Eavesdropper chooses the incorrect basis is 50%, and if Receiver measures this intercepted qubits, he gets a random result, i.e., an incorrect result with probability of 50%. The probability an intercepted qubits generates an error in the key string is then  $50\% \times 50\% = 25\%$ .

## Conclusions

Even if the main disadvantage of quantum key distribution algorithms present the final key is the small size compared to the initial size of the transmitted key, the focus is on getting a unique secret keys with a satisfactory size.

The final key, obtained with any of quantum key distribution scheme can be used together with one-time pad algorithm to create a perfectly safe cryptosystem.

## Acknowledgment

This work was financed from Secretaría de Educación Superior, Ciencia, Tecnología e Innovación (SENESCYT) of Ecuador, through Prometeo project.

## References

1. S. Wiesner, Conjugate coding, Sigact News, vol. 15, no. 1,78(1983); original manuscript written circa 1970.

2. C.H.Bennett, G.Brassard, S.Breidbart and S.Wiesner, Quantum cryptography, or unforgeable subway tokens, Advances in cryptography: Proceedings of Crypto'82, August 1982, plenum, New York, pp. 267275.

3. C.A.Fuchs, N.Gisin, R.B.Griffiths, C.S.Niu, and A.Peres, Optimal eavesdropping in quantum cryptography. I. Information bound and optimal strategy, Physical Review A 56, 1163 (1997).