International Journal of Information Processing, 9(4), 113-118, 2015
ISSN : 0973-8215
IK International Publishing House Pvt. Ltd., New Delhi, India

Software Implementation of the Quantum Key Distribution Protocol with Ququarts

Gabriela Mogos[a]

[a]Facultad de Informatica y Electronica, Escuela Superior Politecnica de Chimborazo, Panamericana Sur km 1 1/2, Riobamba, EC060155, Ecuador, Contact: gabi.mogos@gmail.com

In quantum key distribution, two parts exploit a quantum channel to create a secret shared key comprising a random string of binary digits. This key can then be used to protect a subsequent communication between them. Quantum cryptography is the latest idea in the long history of secure communications and, if it is to develop, it will have to compete with existing technologies. The practical implementation of quantum information technologies requires, for the most part, highly advanced and currently experimental procedures. Quantum key distribution, has been successfully demonstrated in many laboratories and has reached an advanced level of development. This paper presents a software implementation of quantum key distribution protocol with ququarts, proving security for practical communication systems.

Keywords : Quantum Cryptography, Quantum Key Distribution, Ququarts, Security.

1. INTRODUCTION

The use of quantum systems to provide information security has its origins in a proposal by S Wiesner to use it to make unforgeable banknotes. The rst protocol for quantum key distribution was proposed by Bennett and Brassard in 1984 and is now known universally as the BB84 protocol. It constitutes the first application of the field of quantum information theory which itself is founded on the fundamental axioms of quantum physics. More specifically, quantum cryptography provides a secure protocol to exchange cryptographic keys. This protocol is called quantum key distribution or quantum key exchange.

Quantum key distribution rests on two principles. The first principle is itself one of the fundamental principles in quantum mechanics. The second principle is purely classical in nature. First principle of quantum cryptography (Heisenberg's uncertainty principle): "Every measurement of the unknown state of a quantum system irreversibly perturbs the original state of the system, except if the system was prepared in a state that is compatible with the measurement". Second principle of quantum cryptography (Non-cloning theorem): "Quantum states cannot be perfectly copied".

Based on the mathematical model of the Quantum Key Distribution protocol with ququarts [1], the paper presents practical results obtained as its implementation. For this study were developed software applications for two cases: the absence and the presence of cyber-attacks (the Intercept-Resend attack). This study aims the size of obtained cryptographic keys and the percentage of errors of the protocol, depending on the size of the initial data.

2. QUANTUM KEY DISTRIBUTION WITH QUQUARTS

The quantum key distribution protocol with ququarts [1] uses twelve orthogonal states in a four-state quantum system. Hilbert space associated to these systems has four-dimensions and the 3 mutually unbiased bases, each with four eigenvectors, are defined as follows:

$$A = \{|0\rangle, |1\rangle, |2\rangle, |3\rangle\} \quad (1)$$

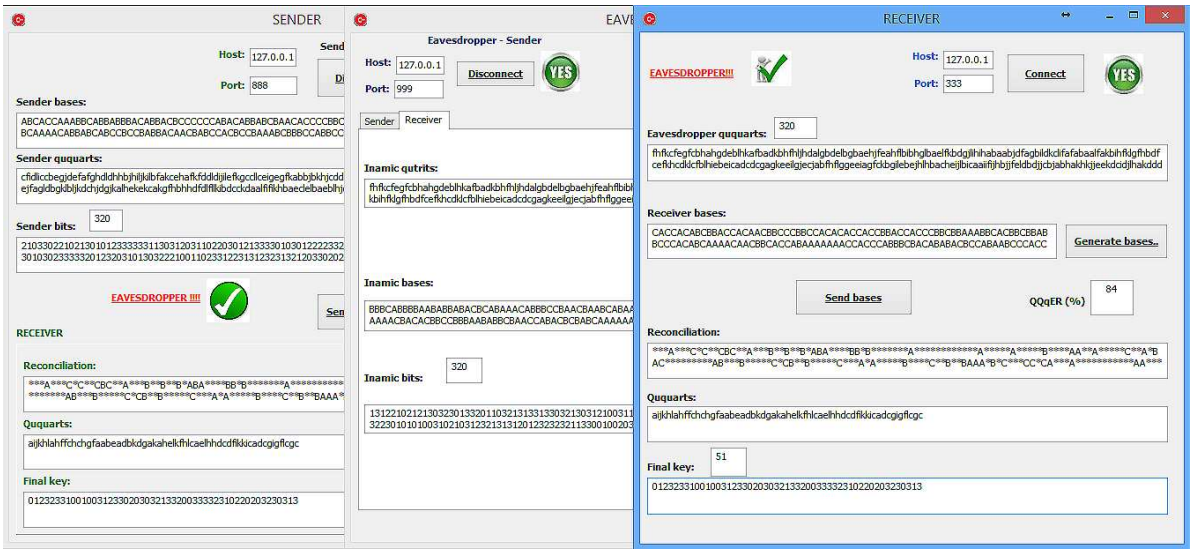

Figure 3. Interfaces on Intercept-Resend Attack.

sets of bits and comparing their parity over the public channel.

If the parities are different then the set contains errors, but if they are the same then the set will have no errors. At the end of the error correction process, the sender and the receiver should share a common bit string, but this may be signicantly shorter than the raw key. Privacy amplication allows the sender and the receiver to reduce the eavesdroppers information. Theoretically, the errors are around of 88%.

In case of Intercept-Resend attack, the Figure 3 presents the interfaces of three modules: the sender, the receiver and the eavesdropper. The simulation run for input data varying between 160 and 2560 ququarts. Practically, the average value of the error rate in this case is 88.94%. The averages of error rate obtained for the various inputs, in the absence and in the presence of an eavesdropper, are shown in Figure 5, as a comparative results. Can notice that the difference between the error rate obtained in the case of a cyber-attack and in its absence, is situated around a mean value of 20%. Therefore, in order to detect the intruder, is necessary to compare the error rate in ideal case (when communication is safe) with error rate in unsafe conditions. If the latter is higher, we can say for sure that on the communication channel is acting an eavesdropper.

5. CONCLUSIONS

Even if the error rate obtained is high, the size of obtained cryptographic key is large. This is because each ququart can carry two-bit classical information. We can conclude that the simplest method to detect the Intercept - Resend attacks on quantum key distribution with ququarts, is to measure the percentage of errors from the key. Consequently, if the errors value is greater than a maximum allowable (secure communication environment), we are sure the protocol has undergone a cyber-attack. Thus, it was proven by the practical model proposed in this paper, observing exactly the mathematical model of the quantum key distribution with ququarts protocol.

REFERENCES

1. Chen P, Yan Song L, Fu Guo D and Long G L. Measuring-Basis Encrypted Quantum Key Distribution with Four-State Systems, *Commun. Theor. Phys. (Beijing, China) 47*, pages 49-52, 2007.
2. Bennett C H, Brassards G, Jean Marc R.

No. crt.	Initial ququarts - 160		Initial ququarts - 320		Initial ququarts - 640		Initial ququarts - 1280		Initial ququarts - 2560	
	No final bits Sender - Inamic - Receiver	QQqER Sender - Inamic - Receiver (%)	No final bits Sender - Inamic - Receiver	QQqER Sender - Inamic - Receiver (%)	No final bits Sender - Inamic - Receiver	QQqER Sender - Inamic - Receiver (%)	No final bits Sender - Inamic - Receiver	QQqER Sender - Inamic - Receiver (%)	No final bits Sender - Inamic - Receiver	QQqER Sender - Inamic - Receiver (%)
1	38	88	84	87	134	90	286	89	591	88
2	32	90	70	89	130	90	262	90	558	89
3	34	89	72	89	126	90	254	90	541	89
4	42	87	78	88	150	88	320	87	623	88
5	38	88	64	89	140	89	288	89	557	89
6	36	89	64	90	138	89	288	89	558	89
7	34	90	66	90	130	90	254	90	524	90
8	36	88	76	88	152	88	304	88	573	89
9	34	89	64	90	134	89	278	89	557	89
10	34	89	72	89	142	89	304	88	590	88
	35.52	**88.77**	**70.32**	**88.94**	**137.20**	**89.19**	**282.21**	**88.90**	**565.91**	**88.92**

Figure 4. The Results on Quantum Key Distribution with Eavesdropper.

	Quantum Error Rate (%)		
	Quantum Key Distribution protocol with ququarts		
	Without attack	With attack	Difference
Initial data - 160	71	89	18.15
Initial data - 320	68	89	21.33
Initial data - 640	68	89	20.81
Initial data - 1280	68	89	21.32
Initial data - 2560	68	89	21.32
Average	**68.34**	**88.94**	**20.51**

Figure 5. Comparative Results.

Privacy Amplification by Public Discussions, *Siam Journal on Computing*, 17(2):210-229, 1988.

3. Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J. Experimental Quantum Cryptography, *Journal of Cryptology*, 5(1):3-28, 1992.
4. Makarov V, Anisimov A, Skaar J. Effects of Detector Efficiency Mismatch on Security of Quantum Cryptosystems, *A Physical Review* , 74:1-11, 2005.
5. Gisin N, Ribordy G, Tittle W, Zbinden H. Quantum cryptography, *Reviews of Modern Physics*, 2002.
6. Macchiavello C, Palma G M and Zeilinger A. Quantum Computation and Quantum Information Theory. *World Scientic*, Singapore, 2000.

Gabriela Mogos is currently the Prometeo researcher at Escuela Superior Politecnica de Chimborazo, Riobamba, Ecuador. She obtained her Bachelor of Science in Physics and Masters degree in Computer Science from Alexandru Ioan Cuza University of Iasi Romania She was awarded Ph. D in Computer Science from Alexandru Ioan Cuza University of Iasi, Romania.