"HENRI COANDA"
AIR FORCE ACADEMY
ROMANIA

"GENERAL M.R. STEFANIK"
ARMED FORCES ACADEMY
SLOVAK REPUBLIC

INTERNATIONAL CONFERENCE of SCIENTIFIC PAPER
AFASES 2015
Brasov, 28-30 May 2015

COMPARATIVE ANALYSIS OF QUANTUM KEY DISTRIBUTION PROTOCOLS WITH TWO, THREE AND FOUR-STATE SYSTEMS

Gabriela Mogos*

* Facultad de Informatica y Electronica, Escuela Superior Politecnica de Chimborazo, Riobamba, Ecuador

Abstract: *Cryptographic protocols can be classified by the type of security against eavesdropping which they provide. There exist mathematically secure schemes whose security relies on mathematical proofs or conjectures about the complexity of deciphering the message without possessing the correct key. The majority of current secure public Internet connections rely on such schemes. Alternatively, a cryptographic setup may provide a physically secure method for communicating. In these setups the security is provided by the physical laws governing the communication protocol.This paper presents a comparative study of three quantum key distribution protocols with two, three and four-state systems, respectively. Starting with the same dimension of input data, the percentage of errors is analyzed by comparison with the dimensions of the cryptographic keys obtained in the case of each protocol.*

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

1. INTRODUCTION

Quantum information theory describes the communication and processing of information with symbols encoded in quantum mechanical systems, that is, as quantum signs, which by their nature are subject to physical constraints differing from those on classical signs. The development of quantum information theory has involved the replacement or generalization of traditional information-theoretic concepts so as to describe situations involving such signs, something that is necessary because quantum mechanical systems are described by non-standard probability distributions.

A central theme of such a study is the ways in which quantum mechanics opens up possibilities that go beyond what can be achieved classically.

This paper presents a comparative study of three quantum key distribution protocols: Bennett-Brassard; Bechmann-Pasquinucci, and Peres and Chen, Yan-Song, Deng, and Long, concerning the percentage of errors from the key compared with the dimensions of cryptographic keys obtained, and initial data.

It is important to mention that the protocols studied use for encoding the information of two, three, and four-state quantum systems.

For the performance of this study we developed software applications simulating each protocol, and we used the same dimension of input data at the measurement of the errors.

The applications simulating the protocols were realized in C++ language. The equipment used in the simulation process consists of two computers connected by a switch.

The modules of the application will run on each of the two computers: *the Sender* and *the Receiver*. In the research, we did not take into consideration the errors appeared due to the equipment and the presence of an eavesdropper.

2. THE QUANTUM KEY DISTRIBUTION PROTOCOLS

2.1 The Quantum Key Distribution protocol with Two-State Systems. In 1984 by Bennett-Brassard [8], using quantum bi-dimensional systems (*qubits*) realized the first quantum distribution key protocol.

The quantum bi-dimensional systems are represented by states of photon polarization, forming two orthonormal bases: linear and diagonal.

$$\begin{aligned} L &= \{|0^0\rangle, |90^0\rangle\} && \textit{- linear} \\ D &= \{|45^0\rangle, |135^0\rangle\} && \textit{- diagonal} \end{aligned} \qquad (1)$$

2.2 The Quantum Key Distribution protocol with Three-State Systems. In 2000, Helle Bechmann-Pasquinucci and Asher Peres [9] (BPP) extended the quantum key distribution protocol for the three-state systems, the so-called *qutrits*. For qutrits, bases called Mutually Unbiased Bases (MUB) are used, obtained by the application of transformed Fourier discrete. For the protocol BPP, four measurement bases are used, each having three individual vectors.

$$\begin{aligned} A &= \{|\alpha\rangle, |\beta\rangle, |\gamma\rangle\} \\ B &= \{|\alpha'\rangle, |\beta'\rangle, |\gamma'\rangle\} \\ C &= \{|\alpha''\rangle, |\beta''\rangle, |\gamma''\rangle\} \\ D &= \{|\alpha'''\rangle, |\beta'''\rangle, |\gamma'''\rangle\} \end{aligned} \qquad (2)$$

2.3 The Quantum Key Distribution protocol with Four-State Systems. In 2006, a research team from China [7] proposed a key distribution scheme using quantum systems with four-dimensions (*ququarts*).

The Quantum Key Distribution protocol with Four-State Systems [7] uses twelve orthogonal states in a four-state quantum system. Hilbert space associated to these systems has four-dimensions, and the three mutually unbiased bases (MUB), each with four eigenvectors, are defined as follows:

$$Z-MUB=\begin{cases} |Z\rangle_0 = |0\rangle \\ |Z\rangle_1 = |1\rangle \\ |Z\rangle_2 = |2\rangle \\ |Z\rangle_3 = |3\rangle \end{cases}$$

$$X-MUB=\begin{cases} |X\rangle_0 = \frac{1}{\sqrt{4}}(|0\rangle + |1\rangle + |2\rangle + |3\rangle) \\ |X\rangle_1 = \frac{1}{\sqrt{4}}(|0\rangle + e^{2\pi i/4}|1\rangle + e^{4\pi i/4}|2\rangle + e^{6\pi i/4}|3\rangle) \\ |X\rangle_2 = \frac{1}{\sqrt{4}}(|0\rangle + e^{4\pi i/4}|1\rangle + e^{8\pi i/4}|2\rangle + e^{12\pi i/4}|3\rangle) \\ |X\rangle_3 = \frac{1}{\sqrt{4}}(|0\rangle + e^{6\pi i/4}|1\rangle + e^{12\pi i/4}|2\rangle + e^{18\pi i/4}|3\rangle) \end{cases} \qquad (3)$$

$$Y-MUB=\begin{cases} |Y\rangle_0 = \frac{1}{\sqrt{4}}(e^{-\pi i}|0\rangle + |1\rangle + |2\rangle + |3\rangle) \\ |Y\rangle_1 = \frac{1}{\sqrt{4}}(e^{-\pi i}|0\rangle + e^{2\pi i/4}|1\rangle + e^{4\pi i/4}|2\rangle + e^{6\pi i/4}|3\rangle) \\ |Y\rangle_2 = \frac{1}{\sqrt{4}}(e^{-\pi i}|0\rangle + e^{4\pi i/4}|1\rangle + e^{8\pi i/4}|2\rangle + e^{12\pi i/4}|3\rangle) \\ |Y\rangle_3 = \frac{1}{\sqrt{4}}(e^{-\pi i}|0\rangle + e^{6\pi i/4}|1\rangle + e^{12\pi i/4}|2\rangle + e^{18\pi i/4}|3\rangle) \end{cases}$$

3. COMPARATIVE ANALYSIS

Quantum Bit (Trit) Error Rate 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 measurement bases from the public channel. Quantum Bit (Trit) Error Rate method may be applied to most of the key distribution systems, for detection of the enemy. Each system has its own accepted error rate, and exceeding it means the intervention of an enemy.

By quantum key distribution [1,2], two entities, *the Sender and the Receiver,* establish together a unique and secure key, which may be used with a secure encryption algorithm, like *one-time pad* [3,4].

A classical scheme of quantum key distribution uses two communication channels, a classical one, and a quantum one, and it has the following main steps:

1. *The Sender and the Receiver* generate random and independent sequences of bits/trits;

2. *The Sender and the Receiver* use a quantum key distribution protocol to compare the sequences of bits/trits, and to establish together a unique and secret key;

3. *The Sender and the Receiver* perform a procedure of error correction.

4. *The Sender and the Receiver* appreciate (according to the error rate) if the transmission was intercepted by *the enemy;*

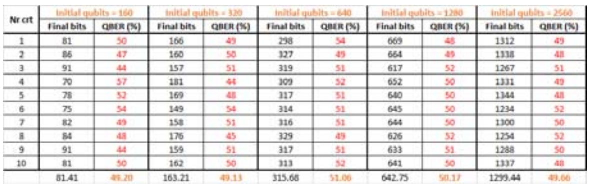
5. *The Sender and the Receiver* communicate through a public channel and perform a procedure called *privacy amplification* [5,6];

6. *The final secret unique and secure key* is obtained.

We tested the applications on a variable number of input data (quantum systems), and studied how the quantum errors varied.

The first important step of the protocol is when *the Receiver* measures the quantum systems received from *the Sender*. Taking into account that the Receiver chooses the measurement bases randomly, we may speak of the appearance of significant errors in the protocol.

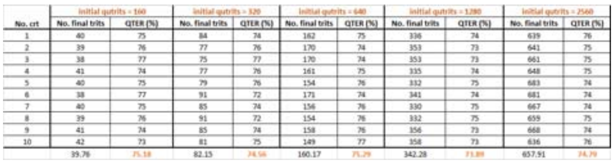
After running 10 times each application, we obtained the results shown in fig.1., fig.2. and fig.3., for an initial key with dimensions ranging from 160 to 2560 quantum systems.



Nr crt	initial qubits = 160		initial qubits = 320		initial qubits = 640		initial qubits = 1280		initial qubits = 2560	
	Final bits	QBER (%)	Final bits	QBER (%)	Final bits	QBER (%)	Final bits	QBER (%)	Final bits	QBER (%)
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
	81.41	49.20	163.21	49.13	315.68	51.06	642.75	50.17	1299.44	49.66

Fig. 1. Quantum Key Distribution protocol with Two-State Systems.

In the case of Quantum Key Distribution protocol with Two-State Systems - Bennett-Brassard – the Receiver needs to choose between the two measuring bases (linear and diagonal), therefore the probability to choose correctly is 1/2. After running the software application, we obtained an average error of 49.83%.

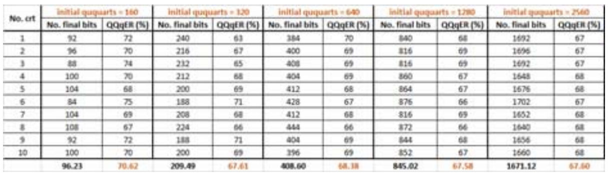


No. crt	initial qutrits = 160		initial qutrits = 320		initial qutrits = 640		initial qutrits = 1280		initial qutrits = 2560	
	No. final trits	QTER (%)	No. final trits	QTER (%)	No. final trits	QTER (%)	No. final trits	QTER (%)	No. final trits	QTER (%)
1	40	75	84	74	162	75	336	74	639	76
2	39	76	77	76	170	74	353	73	641	75
3	38	77	75	77	170	74	353	73	661	75
4	41	74	77	76	161	75	335	74	648	75
5	40	75	79	76	154	76	332	75	683	74
6	38	77	91	72	171	74	341	74	681	74
7	40	75	85	74	156	76	330	75	667	74
8	39	76	91	72	154	76	332	75	659	75
9	41	74	85	74	158	76	356	73	668	74
10	42	73	81	75	149	77	358	73	636	76
	39.76	75.18	82.15	74.56	160.17	75.29	342.28	73.89	657.91	74.79

Fig.2. Quantum Key Distribution protocol with Three-State Systems.

In the case of Quantum Key Distribution protocol with Three-State Systems - Bechmann-Pasquinucci and Peres – the Receiver needs to choose among the 4 measuring bases (A, B, C, D), the probability of choosing correctly is 1/4.

After running the software application, the error rate in the case of this protocol is of approximately 74.73%.



No. crt	initial ququarts = 160		initial ququarts = 320		initial ququarts = 640		initial ququarts = 1280		initial ququarts = 2560	
	No. final bits	QQqER (%)	No. final bits	QQqER (%)	No. final bits	QQqER (%)	No. final bits	QQqER (%)	No. final bits	QQqER (%)
1	92	72	240	63	384	70	840	68	1692	67
2	96	70	216	67	400	69	816	69	1696	67
3	88	74	232	65	408	69	816	69	1692	67
4	100	70	212	68	404	69	860	67	1648	68
5	104	68	200	69	412	68	864	67	1676	68
6	84	75	188	71	428	67	876	66	1702	67
7	104	69	208	68	412	68	816	69	1652	68
8	108	67	224	66	444	66	872	66	1640	68
9	92	72	188	71	404	69	844	68	1656	68
10	100	70	200	69	396	69	852	67	1660	68
	96.23	70.62	209.49	67.61	408.60	68.38	845.02	67.58	1671.12	67.60

Fig.3. Quantum Key Distribution protocol with Four-State Systems.

In the case of Quantum Key Distribution protocol with Four-State Systems, the Receiver needs to choose among the 3 measuring bases, therefore the probability of choosing correctly is of 1/3. The average error obtained after running the application is of 68.35%.

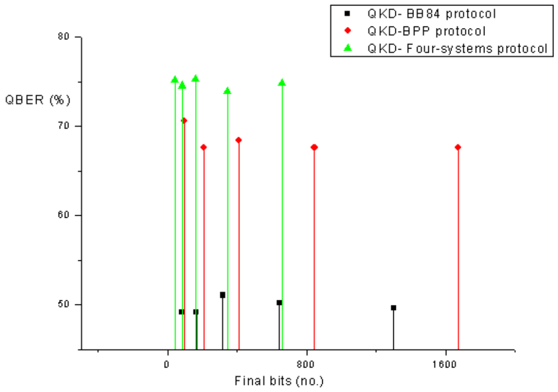


Fig.4. Variation of the error according to the dimension of the input data for all protocols.

We can see that the biggest errors are obtained in the case of Quantum Key Distribution protocol with Three-State Systems, when the Receiver needs to choose among several measuring bases than in the case of the other two protocols.

Quantum Key Distribution protocol with Four-State Systems is the most efficient of the three presented previously, because a quantum system with four-states transports two classical bits.

Consequently, even if the error rate registered by Quantum Key Distribution protocol with Four-State Systems is higher than for Quantum Key Distribution protocol with Two-State Systems, the dimension of the cryptographic key is bigger in the case of the protocol with four-state systems (average value of 257.8 bits) than in the case of two-state systems (average value of 209.17 bits).

4. CONCLUSIONS & ACKNOWLEDGMENT

Quantum Key Distribution (QKD) was demonstrated only for mathematical models of quantum key distribution systems. In practice, this unconditional security cannot be reached, due to technical imperfections of the devices used for polarization, and reading of photon polarization, respectively, involved in quantum key exchange.

The results obtained highlighted first the agreement between the theoretical model and the practical one in what concerns the average error of each protocol, and secondly, the dimension of the cryptographic key obtained in ideal working conditions.

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

REFERENCES

1. Bouwmeester D., Ekert A. & Zeilinger A., The Physics of Quantum Information. Quantum Cryptography, Quantum Teleportation, Quantum Computation, *Springer*, p. 314, (2000).
2. Bruss D., Optimal Eavesdropping in Quantum Cryptography with Six-States, *Physical Review Letters*, vol. 81, nr. 14, pp. 3018-3021, (1998).
3. Vernam G., Secret signaling system, *U.S. patent No. 1310719*, (1919).
4. Vernam G., Cipher printing telegraph system for secret wire and radio telegraphic communications, *Journal of IEEE*, vol. 55, pp. 109-115, (1926).
5. Bennett C.H., Brassards G. & Jean-Marc R., Privacy amplification by public discussions, *Siam Journal on Computing*, vol. 17, no. 2, pp. 210-229, (1988).
6. Bennett C.H., Bessette F., Brassard G., Salvail L., & Smolin J., Experimental quantum cryptography, *Journal of Cryptology*, vol. 5, no. 1, pp. 3-28, (1992).
7. Chen Pan, LI Yan-Song, Deng Fu-Guo, and Long Gui-Lu, Measuring-Basis Encrypted Quantum Key Distribution with Four-State Systems, *Commun. Theor. Phys.* (Beijing, China) 47, pp. 49–52, (2007).
8. Bennett C.H. and Brassard G., Proceedings IEEE Int. Conference on Computers, *Systems and Signal Processing, IEEE*, New York, (1984).
9. Bechmann-Pasquinucci H. and Peres A., Quantum Cryptography with 3-state systems, *Physical Review Letters 85*, 3313, (2000).