THE PUBLISHING HOUSE
OF THE ROMANIAN ACADEMY

PROCEEDINGS OF THE ROMANIAN ACADEMY, Series A,
Volume 21, Number 1/2020, pp. 85–91

EFFICIENCY OF THE QUANTUM KEY DISTRIBUTION SYSTEMS – A COMPARATIVE STUDY OF BB84 PROTOCOL WITH ITS IMPROVED VERSIONS

Liliana ZISU

"Ferdinand I" Military Technical Academy Doctoral School, Bucharest, Romania
E-mail: liliana.zisu@gmail.com

Abstract. The efficiency of quantum key distribution systems plays an important role in deciding the feasibility of practical quantum cryptographic systems. BB84, the first quantum protocol for key distribution, proposed by Charles Bennett and Gilles Brassard in 1984, allows two remote parties to create and share a secret key with approximately 25% efficiency. There are two remarkable methods that improve essentially the efficiency of the BB84 protocol. First method involves the assignment of significantly different probabilities to the different polarization bases during both transmission and reception of the photons. The second method uses the quantum memory, a device to store the received photons. The paper simulates the two methods using C# applications and performs a statistical analysis by comparing them with the original BB84 protocol.

***Key words**:* quantum cryptography, quantum key distribution, BB84, efficiency.

1. INTRODUCTION

Quantum cryptography, the principles of which are based on the laws of quantum physics, allows the creation and sharing of an encryption key, thus solving the problem of key distribution existing in classical cryptography. Although its debut takes place in the 1970s, with Weisner's work, "Conjugate Coding" [1], the first key distribution quantum protocol was created in 1984 by Charles Bennett and Gilles Brassard [2]. It has become the standard quantum cryptography protocol on which most quantum protocols are based. The second notable protocol was proposed by Ekert in 1991, but unlike BB84, which uses single photons and is based on the Heisenberg principle, E91 [3] uses entangled photons and relies on Bell's theorem. After these revolutionary protocols, a number of other protocols followed, being more or less improved versions of the first two. Among these, we mention the six-state protocol proposed by Pasquinucci and Gisin in 1999 [4], which is identical to the BB84 protocol, except that it uses six polarization states.

In 2001 Mayers [5] demonstrates theoretically the unconditional security of the protocol, stating that a secure key sequence can be generated whenever the channel bit error rate is less than approximately 7%. Also in 2001, Wang Xiangbin [6] proposes the use of quantum memory and more states of polarization to maximize efficiency and security and in 2005 the method proposed by Hoi-Kwong Lo, H.F. Chau and M. Ardehali [7] by allocating different probabilities to different polarization bases doubles significantly the protocol efficiency.

The basic model of a quantum key distribution protocol involves two users, Alice (transmitter) and Bob (receiver), connected through two communication channels: a quantum one and a classical one. The quantum channel is used to transmit the key and the classical one to transfer the information. Eve is considered to be the intruder who wishes to intervene in the communication process between Alice and Bob.

The most important distribution key distribution feature allows the two users, participants in the communication process, to detect the presence of a third person wishing to obtain information about the key. According to quantum mechanics, the process of measuring a quantum system disrupts the system. Anyone who tries to get the key will have to measure it and therefore will produce detectable errors. If the transmission was disrupted, the intruder having too much information about the key, the quantum communication process is abandoned or resumed.

2. BRIEF DESCRIPTION OF THE PROTOCOLS

2.1. BB84

The BB84 protocol uses single photons to encode bits in the following way: the transmitter sends a series of photons, polarized in four polarization directions:↑, →, ↗ and ↖. The first two directions are orthogonal in the rectilinear base (+) and the other two are orthogonal in the diagonal base (*x*). Each direction is associated with a bit, the 0 bit value to the → and ↗ polarization states and the 1 bit value to the ↑ and ↖ polarization states.

The procedure of the protocol is as follows:

- Alice prepares n independent qubits in the state: $|Q_A\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \ldots |\psi_n\rangle$, where ψ_k is the k-th qubit, $1 \le k \le n$.The state of each qubit is randomly chosen from a set of four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

The state of a single qubit can be visualized using the Bloch sphere (Fig. 1).

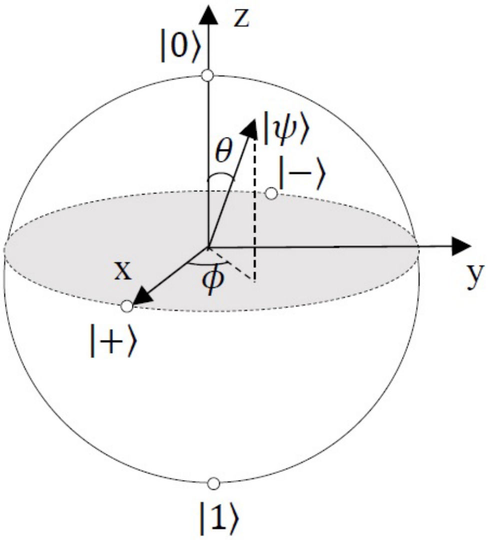


Fig. 1 – Representation of qubits on Block sphere.

- Alice sends the qubits to Bob.
- Bob measures the qubits randomly using the two polarization bases.
- On the public channel, Bob announces the polarization bases used. If Alice and Bob measured the same base, the corresponding bit is added to the key. Otherwise, it will be dropped. The key thus obtained is called the sifted key.
- Bob and Alice correct the errors that occurred in the photon transmission process. At this stage, known as reconciliation, an interactive binary search for error is performed. The transmitter and receiver divide the bit sequence into bit blocks and compare the parity of each block. If the parity of a bit block differs, they will divide the block into smaller blocks and compare their parity. This process will be repeated until the bit that is different will be discovered and removed. Bob estimates the error rate and if it does not exceed 11%, the key is created. Communication for error correction is made on an unsecured public channel. The key obtained is called raw key.
- Bob and Alice check on the public channel if they are in the possession of the same bits, revealing some of the raw key bits. The expected length of the remaining key is $n/4$.
- Transforming the original key into another key that reduces Eve's information is called privacy amplification

2.2. Efficient BB84 with quantum memory (EBB84-QM)

Wang Xiangbin, proposed a general efficient protocol that works in the following way:

- Alice prepares n independent qubits in the state: $|Q_A\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes |\psi_3\rangle \ldots |\psi_n\rangle$, where ψ_k is the k-th qubit, $1 \le k \le n$. The state of each qubit is randomly chosen from a set of $2m$ states $V = \{|\psi_1\rangle, |\psi_2\rangle, \ldots |\psi_m\rangle, |\psi'_1\rangle, |\psi'_2\rangle, \ldots |\psi'_m\rangle\}$, where $(|\psi_1\rangle, |\psi'_1\rangle) = R_0(\theta_i, \phi_i)(|0\rangle, |1\rangle)$, $1 \le i \le m$. R_0 is a rotating operator and θ_i, ϕ_i are two independent rotating angles in *xz* plane and *xy* plane, respectively. Each state $|\psi_1\rangle$ is determined by two criteria, one being the subset from which it must be chosen i.e. $\{|\psi_k\rangle\}$ and $\{|\psi'_k\rangle\}$ and the other is the R_0 operator. For simplicity, the rotation operator corresponding to the k^{th} qubit is noted with $R_0(k)$. For example, if $|\psi'_k\rangle = R_0(\theta_i, \phi_i)$, then $R_0(k) = R_0(\theta_x, \phi_x)$. So Alice associates each individual state with 0 bit if it is from the $\{|\psi_k\rangle\}$ subset or the classical bit 1 if it is from subset $\{|\psi'_k\rangle\}$, so it has a string of classical bits, S_C.
- Alice sends the qubits to Bob.
- Bob stores the qubits and informs Alice through the classical public channel that he has received them.
- Alice announces the information $\{R_0(k)\}$, $1 \le k \le n$.
- Bob measures each qubit according to the bases announced by Alice accordingly. Bob randomly chooses a subset G of the measurements results and compares them with the corresponding records in the S_A made by Alice. The comparison is made through the public channel. If all the results are the same, it implies the lack of an intruder. Without the disclosed photons in subset G, Alice's initial S_C recording is now the shared key.
- For the noisy channel, error correction follows for privacy amplification.

If the value of all $\phi_i = 0$ and the values of θ_i is randomly chosen from the set $\{0, \pi/2\}$, then the efficient BB84 protocol is obtained.

2.3. Efficient BB84 without quantum memory (EBB84-WQM)

The first major ingredient of the scheme, proposed by Hoi-Kwong Lo, H.F. Chau and M. Ardehali, is the assignment of significantly different probabilities to the different polarization bases. The second major ingredient of the scheme is a refined analysis of accepted data. The accepted data is divided into various subsets according to the basis employed and estimate an error rate for each subset separately.

Procedure of efficient quantum key distribution scheme:

- Alice and Bob pick a number $0 \le p \le 1/2$ whose value is made public. Alice sends a sequence of N photons to Bob (N is a large number). The value of p is chosen so that $N(p^2 - \delta') = m_1 = \Omega(\log N)$, where δ' is some small positive number and m_1 is the number of test photons in the rectilinear basis in penultimate step.
- Bob measure polarization of each received photon and announces the bases he used (but not the results) through the public channel.
- Alice tells Bob which of his measurement have been done in the correct bases. They then throw away the two cases when they have used different bases.
- From the subset where they both use the rectilinear basis, Alice and Bob randomly pick a fixed number say m_1 photons and publicly compare their polarizations. (For a large N, it is highly likely that at least m_1 photons are transmitted and received in the rectilinear basis. If not, they abort).

  They estimates the error $e_1 = r_1/m_1$, where r_1 is the number of mismatches. Similarly for diagonal base, they estimates the error $e_2 = r_2/m_2$.

  The test samples m_1 and m_2 are should be sufficiently large and at least of order $\Omega(\log k)$, where k is the length of the final key.

If $e_1, e_2 < e_{\max} - \delta_e$, where $e_{\max}$ is a prescribed maximal tolerable error rate and δ_e is a small positive parameter, they proceed to the next step. Otherwise, they restart the whole procedure.

- Reconciliation and privacy amplification. For simplicity $m_1 = m_2 = N(p^2 - \delta')$ Alice and Bob randomly pick $n = N\left[(1-p^2) - p^2 - \delta'\right]$ photons from those untested photons that are transmitted and received in the diagonal basis. Alice and Bob then independently convert the polarizations of those n photons into a raw key.

3. SIMULATION AND RESULTS

3.1. Characteristics of the simulators

The simulators were built on three aspects: ideal conditions (in the absence of any errors, whether they are generated by noise, the photon detector imperfection or the presence of an intruder), the real environment and in the absence of an intruder, real environment and in the presence of an intruder.

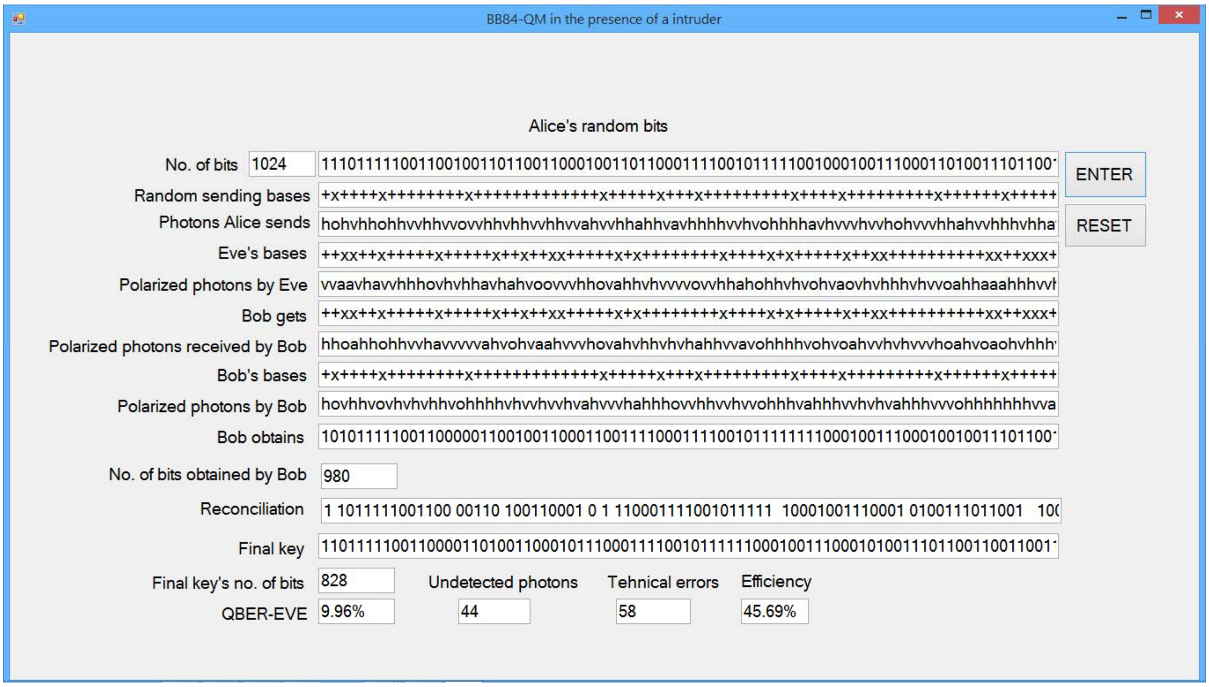
Simulating the algorithm assuming ideal conditions is necessary for understanding the complexity of the algorithms, representing a benchmark that tells us how much we need to improve the devices for optimal operation.

For the generation of numbers, a true number generator was created using the *RNGCryptoServiceProvider* class that uses a series of entropy sources in the operating system to provide random numbers. It is not based on a single generation key and its call combines the values of mouse movements, keystrokes or different system or user data, the computer clock, memory status, and other processes.

The error in simulators does not exceed 10%.

The intruder's attack is intercept-resend. In the quantum communication process between Alice and Bob, Eve intervenes, cuts the optical fiber, and places her own photon detector, having a transmitter identical to Alice's. Eve intercepts the photons sent by Alice, memorizes them, then generates other photons that she polarizes, and sends them to Bob. Eve does not know which bases were used and the only thing she can do is polarize at random. The created application starts from this aspect and analyzes the degree of disturbance of the quantum communication process produced by Eve's action.

The graphical interface of the simulator when the photons are transmitted in the real environment and under the action of an intruder is presented in Fig. 2.



BB84-QM in the presence of a intruder

Alice's random bits

No. of bits 1024 11101111100110010011011001100010011011000111100101111100100010011100011010011101100

Random sending bases +x++++x++++++++x++++++++++++x+++++x+++x+++++++++x++++x+++++++++x++++++x+++++

Photons Alice sends hohvhhohhvvhhvvovvhhvhhvvhhvvahvvhhahhvavhhhhvvhvohhhhavhvvvhvvhohvvvhhahvvhhhvhha

Eve's bases ++xx++x+++++x+++++x++x++xx+++++x+x++++++++x++++x+x+++++x++xx++++++++++xx++xxx+

Polarized photons by Eve vvaavhavvhhhovhvhhavhahvoovvvhhovahhvhvvvvovvhhahohhvhvohvaovhvhhhvhvvoahhaaahhhvvh

Bob gets ++xx++x+++++x+++++x++x++xx+++++x+x++++++++x++++x+x+++++x++xx++++++++++xx++xxx+

Polarized photons received by Bob hhoahhohhvvhavvvvvahvohvaahvvvhovahvhhvhvhahhvvavohhhhvohvoahvvhvhvvvhoahvoaohvhhh

Bob's bases +x++++x++++++++x++++++++++++x+++++x+++x+++++++++x++++x+++++++++x++++++x+++++

Polarized photons by Bob hovhhvovhvhvhhvohhhhvhvvhvvhvahvvvhahhhovvhhvvhvvohhhvahhhvvhvhvahhhvvvohhhhhhhvva

Bob obtains 10101111100110000011001001100011001111000111100101111111100010011100010010011101100

No. of bits obtained by Bob 980

Reconciliation 1 1011111001100 00110 100110001 0 1 110001111001011111 10001001110001 0100111011001 10

Final key 11011111001100001101001100010111000111100101111110001001110001010011101100110011001

Final key's no. of bits 828

QBER-EVE 9.96%

Undetected photons 44

Tehnical errors 58

Efficiency 45.69%

Fig. 2 – Graphical simulator interface.

Remark. The simulators have been designed to meet the conditions for each protocol, even they have the same graphical interface.

3.2. Simulation Results

The efficiency, one of the important parameters of a quantum key distribution protocols, is defined as $\eta = \frac{q_u}{q_t}$, where q_u is the useful qubits and q_t is the total qubits transmitted.

In BB84 and EBB84-QM protocols each of the two users, Alice and Bob, chooses for each photon between two polarization bases randomly, uniformly (equal probability) and independently. A single quantum bit error rate (QBER) is estimated. In contrast, in EBB84-WQM scheme Alice and Bob choose between the two bases randomly, independently but not uniformly (the two bases are chosen with substantially different probabilities), rectilinear basis is chosen with probability p and diagonal basis with probability $1-p$, $0 \le p \le 1/2$. The probabilities used are announced publicly. To defeat the eavesdropper's attack to the predominant basis, two error rates e_1 and e_2 are estimated in the refined protocol: e_1 when Eve uses diagonal basis while Alice and Bob use rectilinear basis and e_2 when Eve uses rectilinear basis while Alice and Bob use diagonal basis.

The simulation results are shown in Table 1 and display that the best efficiency is achieved for EBB84-QM and EBB84-WQM doubles the efficiency of the BB84 protocol. The average values obtained for efficiency in the absence of an intruder are: 70%, 40% and 23% for EBB84-QM, EBB84-WQM and BB84 respectively. A simple graphical representation of the efficiency in Fig. 3 shows the economy is maximized for EBB84-QM protocol.

Table 1

Efficiency (%)

BB84			EBB84-QM			EBB84-WQM		
Under ideal conditions	In the absence of an intruder	In the presence of an intruder	Under ideal conditions	In the absence of an intruder	In the presence of an intruder	Under ideal conditions	In the absence of an intruder	In the presence of an intruder
51.60	22.46	11.48	100.00	72.95	42.26	71.19	38.13	19.31
49.02	23.59	11.09	100.00	66.50	43.80	71.73	37.91	19.48
49.32	23.68	12.01	100.00	68.27	43.58	73.00	40.41	19.94
51.08	22.85	12.50	100.00	72.51	47.68	71.04	39.09	20.00
51.46	23.39	11.43	100.00	67.82	44.68	71.63	39.37	19.87
50.00	24.32	10.79	100.00	71.41	45.48	73.49	38.54	19.53
51.56	23.73	11.87	100.00	69.22	46.14	72.02	40.14	20.91
51.66	22.81	11.43	100.00	69.36	46.80	73.29	43.46	19.75
51.86	24.12	12.99	100.00	72.22	48.41	70.75	40.61	20.58
50.50	23.73	11.82	100.00	74.12	46.51	71.63	39.81	20.61

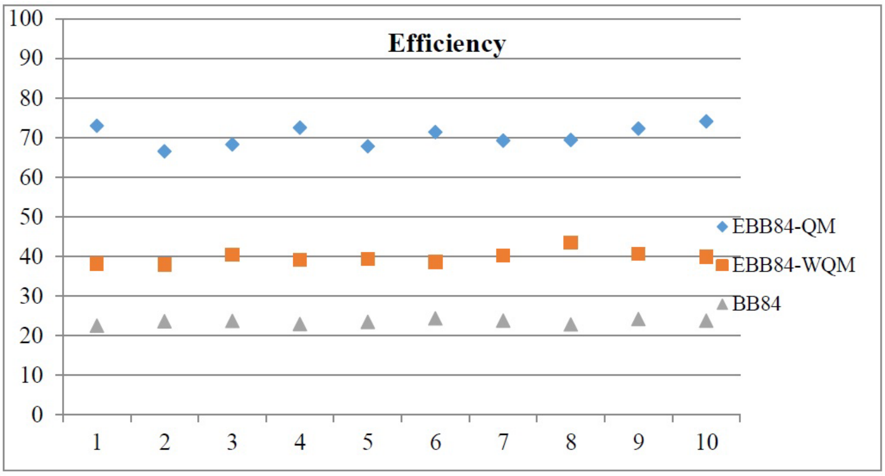


Fig. 3 – In the presence of an intruder.

For a complex analysis of the EBB84-WQM protocol, three different values of probabilities were chosen for efficiency comparison: 0.75, 0.80 and 0.85. Fig. 4 highlights the proportional ratio between efficiency and probability.

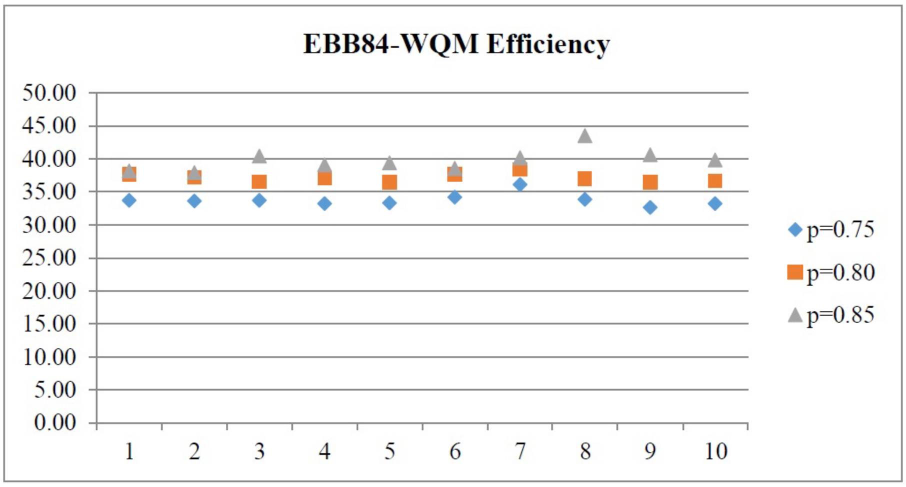


Fig. 4 – In the absence of an intruder.

The simulation allows the evaluation of the security level of the protocols. There are two criteria to measure the security of the protocol. One is the information gathered by the eavesdropper and the other is disturbance caused by the attack to each qubit. The paper analyses the degree of disturbance determined by Eve's action. The maximal tolerable error rate is 11%. The two error rates are computed separately for the cases when both Alice and Bob use the rectilinear basis and when both Alice and Bob use the diagonal basis. The results obtained as shown in Table 2 indicate small values for both error rates in the absence of an intruder and great values in the presence of an intruder. The value of e_1 decreases (the lowest value is for $p=0.85$) and value of e_2 increases (the greatest value is for $p=0.85$), so the presence of an intruder can be detected by e_1 or by e_2.

Table 2

Error Rates

In the absence of an intruder								In the presence of an intruder							
$p=0.5$		$p=0.75$		$p=0.80$		$p=0.85$		$p=0.5$		$p=0.75$		$p=0.80$		$p=0.85$	
e_1	e_2	e_1	e_2	e_1	e_2	e_1	e_2	e_1	e_2	e_1	e_2	e_1	e_2	e_1	e_2
0.33	0.83	0.64	0.65	1.51	1.14	0.67	1.82	23.13	25.9	12.09	47.76	9.7	44.94	8.12	44.00
1.28	0.96	0.51	0.68	0.76	0.00	1.05	2.04	24.01	24.8	14.24	43.87	10.27	46.00	7.85	41.67
0.85	1.31	1.19	0.00	1.36	1.19	0.57	1.96	25.12	23.99	12.74	34.64	9.47	37.37	7.30	34.04
0.32	0.63	0.58	1.26	0.68	1.12	0.55	0.00	24.43	27.34	13.05	35.46	10.18	43.48	8.47	46.81
1.76	0.98	1.46	0.75	0.63	0.00	0.89	3.28	23.49	27.65	11.17	43.21	9.82	43.37	7.84	38.89
0.63	0.67	0.21	0.00	0.32	1.00	0.77	2.22	23.55	27.72	12.99	35.29	10.84	45.13	7.13	37.50
0.16	0.62	1.09	1.90	0.19	0.00	1.44	0.00	25.75	27.27	15.77	37.82	9.68	40.00	6.96	42.86
0.85	1.15	1.53	1.49	1.13	0.96	0.22	0.00	24.2	26.97	12.36	25.74	11.39	33.91	7.58	44.00
1.42	1.39	1.09	0.00	1.07	2.89	0.49	2.27	24.88	22.82	12.68	43.59	9.17	42.31	8.30	41.67
0.98	1.00	1.36	0.69	0.7	1.82	1.27	1.85	25.12	27.24	13.15	35.62	12.21	38.95	8.42	56.92

4. CONCLUSION

We have simulated two methods improving the efficiency of the BB84 protocol. The first method provides a maximum efficiency but requires the existence of a quantum memory. The second method indeed doubles protocol efficiency, but it involves working with a large number of photons. Although access to a quantum memory is not easy at the moment and it would appear also in the near future, still, a group of researchers have registered remarkable success, building a network of quantum devices which allows quantum cryptographic communication with low quantum bit error rate [8]. The paper added a computational proof to the extant mathematical ones.

REFERENCES

1. S. WIESNER, *Conjugate coding*, ACM SIGACT News, 15, 1, pp. 78-88, 1983.
2. C.H. BENNETT, G. BRASSARD, *Quantum cryptography: public key distribution, and coin-tossing*, Proc. 1984 IEEE International Conference on Computers, Systems, and Signal Processing, **560**, pp. 175-179, 1984.
3. A.K. EKERT, *Quantum cryptography based on Bell's theorem*, Phys. Rev. Lett., **67**, *6*, pp. 661-663, 1991.
4. H. BECHMANN-PASQUINUCCI, N. GISIN, *Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography*, Physical Review A, **59**, *6*, pp. 4238-4248, 1999.
5. D. MAYERS, *Unconditional security in quantum cryptography*, Journal of the ACM, **48**, *3*, pp. 351-406, 2001.
6. W. XIANGBIN, *A fully efficient secure quantum cryptography protocol*, Imai Quantum Computation and Information Project, ERATO, Japan Sci. and Tech. Corp., 2001.
7. Hoi-Kwong LO, H.F. CHAU, M. ARDEHALI, *Efficient quantum key distribution scheme and proof of its unconditional security*, Journal of Cryptology, **18**, *2*, pp. 133-165, 2005.
8. M. NAMAZI, G. VALLONE, B. JORDAAN, C. GOHAM, R. SHAHROKHSHAHI, P. VILLORESI, E. FIGUEROA, *Free space quantum communication with a portable quantum memory*, Phys. Rev. Applied, **8**, *6*, p. 064013, 2017.

Received July 1, 2019