Volume XXII 2019
ISSUE no.1
MBNA Publishing House Constanta 2019

Scientific Bulletin of Naval Academy

SBNA PAPER • OPEN ACCESS

A method to improve the BB84 protocol

To cite this article: L. Zisu, C. Răcuciu, D. Glăvan, N. F. Antonie, S. Eftimie, Scientific Bulletin of Naval Academy, Vol. XXII 2019, pg. 171-176.

Available online at www.anmb.ro

ISSN: 2392-8956; ISSN-L: 1454-864X

doi: 10.21279/1454-864X-19-I1-023

A Method to Improve the BB84 Protocol

Liliana Zisu

Doctoral School, "Ferdinand I" Military Technical Academy, Bucharest, Romania
E-mail: liliana_zisu@yahoo.com

Abstract. Quantum cryptography, the principles of which are based on classical mechanics laws, solves exceptionally the issue of key distribution in classical cryptography. BB84, the first quantum key distribution created by Charles Bennett and Gilles Brassard in 1984 offers unconditional security and allows the transmission of a key with the length equal to the length of the message. According to Vernom, using the key with the above feature once together with an encryption algorithm leads to the formation of a most secure cryptographic system. The paper presents a method for improving the BB84 quantum protocol, using ten states of polarization, quantum memory and direct communication in both directions. The implementation of both the proposed method and the BB84 protocol was done through a C# application.

1. Introduction

The idea of quantum key distribution was first proposed by Wiesner [1] and the first protocol was created in 1984 by Charles Bennett and Gilles Brassard [2]. The second remarkable protocol was proposed in 1991 by Ekert [3], but unlike BB84 that uses single photons and it is based on Heisenberg's Uncertainty Principle E91uses entangled photons and it is based on Bell's theorem. A whole series of protocols followed which built on the ideas of BB84 or E91. Some of the most notable of these are B92 [4], SSP [5], Sarg04 [6], BBM92 [7], Enzer02 [8] and Fung06 [8].

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. BB84 – Brief Description

The main steps of the BB84 protocol are as follows:

- Alice, using a random number generator, creates a random sequence of classical bits and then sends Bob a series of photons that she polarizes properly according to the generated bit sequence. Alice sends single polarized photons according to four possible directions, ↑ →, ↗,

and ↖. The first two are orthogonal in the rectilinear basis and the other two are orthogonal in the diagonal basis. States ↑ and ↗ represent bit 0, and states →, ↖ represent bit 1.

- Bob, randomly using one of the two bases will measure each photon. In the absence of noise or an intruder, the transmitter and receiver will obtain the same measurement result if they choose the same base. Using a public channel, the receiver (Bob) passes to the transmitter (Alice) to the measurement base it used without revealing the result. If the measurement bases are not well chosen, the results obtained in this case will not be taken into account. The bit sequence thus obtained is called the raw key.
- Alice and Bob estimate the error rate and if it does not exceed a certain threshold, generally around 7-8%, then error correction and key creation occur. Otherwise, the protocol is dropped or resumed. At this phase known as the Secret Key Reconciliation, a binary, interactive error search is performed. The transmitter and receiver divide the remaining bit sequence into bit blocks and compare the parity of each block. If the parity of a bit block differs, they will divide that block into smaller blocks and compare their parity. This process will be repeated until the bit that is different will be discovered and removed. Communications to eradicate errors will be made on an unsecured public channel. The key obtained is called the sifted key.
- Transforming the original key into a different one that reduces Eve's information is called privacy amplification. This phase is accomplished by applying mathematical algorithms of great complexity.

3. Ten State BB84 with Quantum Memory

Unlike the BB84 protocol, Alice and Bob have quantum memories and use the following ten states of polarization that form five orthogonal bases + (0^0-90^0), x (45^0-135^0), y (30^0-120^0), z (20^0 - 110^0) and w (60^0 - 150^0) and for each polarization state they associate a classical bit, as seen in Figure 1.

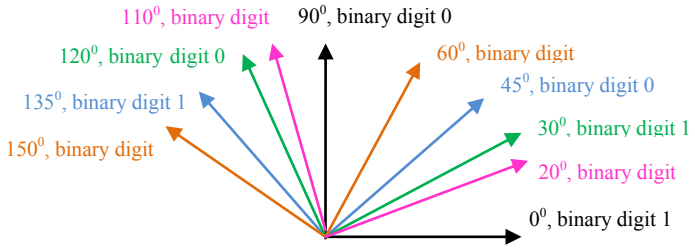


Figure 1. Polarized states

The main steps of the improved protocol are as follows:

• Alice, using a random number generator, creates a random sequence of classical bits and then sends Bob a string s_1 of polarized singular photons based on the ten directions and according to the bit sequence generated.

• Bob does not measure the received photons, as it happens in the BB84 protocol, but he memorizes them and waits for Alice to transmit the bases used on a classic channel.

• When Bob and Alice are in the possession of the photons and bases, Bob and Alice change the roles, Bob becoming now the transmitter and Alice the receiver, and so Bob sends in turn a string s_2 of polarized photons that Alice needs to memorize and then wait for the bases used to be transmitted on the classic channel.

• Alice and Bob extract raw keys by removing polarized photons with the penultimate base.

• Estimating errors and continuing the protocol or dropping it according to the error rate

• Reconciliation for both keys and final key formation by adding Alice's key to Bob's key.

• Privacy amplification to minimize information obtained by Eve.

4. Results and Discussions

The BB84 protocol simulation as well as the proposed method was done through a C# application. The simulator was built on three aspects: ideal conditions, real environment and in the absence of an intruder, real environment and in presence of an intruder. The intruder's attack is represented by intercept - resend. In the quantum communication process between Alice and Bob, Eve intervenes, cuts the optical fibre, and places its own photon detector, having a transmitter identical to Alice's. Eve intercepts the photons sent by Alice, memorizes them, then generates other photons that are going to be polarized, and sends them to Bob. Eve does not know what bases have been used to polarize the bases, and the only thing it can do is to polarize randomly. The created application starts from this aspect and analyses the degree of disturbance of the quantum communication process produced by Eve's action.

The symbols used in the simulator for photon polarization are shown in Table 1.

Table 1. Bases & Symbols

Basis	Symbol	Bit Value Associated
Rectilinear (+)	h	1
	v	0
45^0- 135^0 Diagonal (x)	a	0
	o	1
30^0- 120^0 Diagonal (y)	f	1
	t	0
20^0- 110^0 Diagonal (z)	e	0
	u	1
60^0- 150^0 Diagonal (w)	b	1
	s	0

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 Figure 2.

Figure 2. Graphical simulator interface

The simulation of the BB84 algorithm, whose results are presented in Table 2, displays an efficiency of the protocol, under ideal photon transmission conditions of approximately 50%, the result depending entirely on the bases selection by the receiver according to those chosen by the transmitter. A value close to 50% of the efficiency is obtained also in the absence of an intruder, when the transmission of photons is made with errors. The situation changes when an intruder is present, the efficiency of the BB84 algorithm being of approximately 23%, in which case the quantum communication interruption is recommended.

Table 2. BB84 Efficiency

Under ideal conditions	**In the absence of an intruder**	**In the presence an intruder**
52.83	51.59	22.17
49.51	46.48	25.39
51.59	49.32	23.24
50.39	46.00	25.00
49.71	47.95	22.56
50.59	46.97	22.75
50.88	48.24	23.44
45.61	46.78	23.05
52.73	48.73	25.88
49.23	49.71	24.22

The graphical representation of the BB84 protocol efficiency is shown in Figure 3.

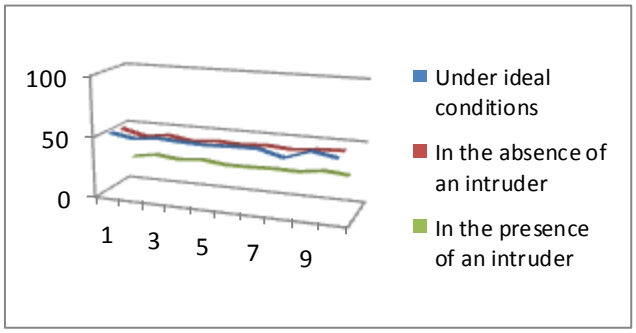


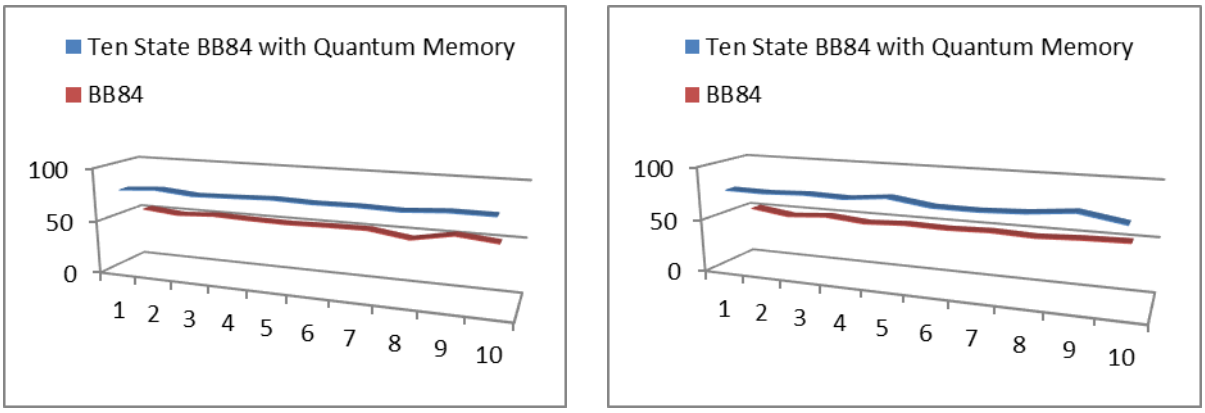
Figure 3. BB84 Efficiency

Analysing the results of Table 3, obtained for the proposed method, we notice that the efficiency values increase by about 30%. Using a false base and removing the photons polarized with it from the key creation leads to a higher security level, the intruder overwhelmingly interfering with the communication process.

Table 3. Ten State BB84 with Quantum Memory Efficiency

Under ideal conditions	In the absence of an intruder	In the presence of an intruder
79.10	77.54	41.41
81.45	76.95	43.36
78.32	78.61	41.60
79.30	77.54	41.99
80.57	81.35	39.36
79.39	75.98	43.44
79.79	75.59	44.73
78.81	77.34	43.07
81.25	81.15	44.92
81.05	74.61	43.95

From the graphical representation of the efficiency of the two protocols in Figure 4, the superiority of the Ten State BB84 protocol with Quantum Memory over the BB84 protocol is observed.



a) b)

Figure 4. Efficiency of the protocols a) Under ideal conditions b) In the absence of an intruder

5. Conclusions

The use of ten polarization bases and the random use of one of them as false as well as of quantum memory significantly improve the BB84 security level protocol. Also, communication on the classical channel is reduced and greater protocol efficiency is achieved.

References

[1] S. Wiesner, "Conjugate coding ", ACM SIGACT News, 15, 1983, pp. 78–88.

[2] Bennett, C. H. and Brassard, G., "Quantum Cryptography: Public key distribution and coin tossing.", International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10-12 December 1984, pp. 175-179.

[3] Ekert, A. K., "Quantum cryptography based on Bell's theorem", Physical Review Letters, vol. 67, no. 6, 5 August 1991, pp. 661 – 663.

[4] Bennett, C., "Quantum cryptography using any two nonorthoganol states.", Phys. Rev. Lett. 68, 1992, pp. 3121-3124

[5] Bechmann-Pasquinucci, H., and Gisin, N., "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography." Phys. Rev. A 59, 4238-4248, 1999

[6] Scarani, A., Acin, A., Ribordy, G., Gisin, N., "Quantum cryptography protocols robust against photon number splitting attacks.", Physical Review Letters, vol. 92, 2004.
[7] Bennet, C. H., Brassard, G., and Mermin, N., D., "Quantum cryptography without Bell's theorem.", Phys. Rev. Lett. 68, 1992, pp. 557-559
[8] Enzer, D., Hadley, P., Gughes, R., Peterson, C., Kwiat, P., "Entangled-photon six-state quantum cryptography.", New Journal of Physics, 2002, pp 45.1-45.8.
[9] Fung, C., Tamaki, K., Lo, H., "On the performance of two protocols: SARG04 and BB84.", Phys. Rev., A 73, 012337, 2006.