International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:13, No:4, 2019

# Eight-State BB84: A C# Simulation

Liliana Zisu

***Abstract*—**The first and best known quantum protocol BB84, whose security is unconditional allows the transmission of a key with a length equal to that of the message. This key used with an encryption algorithm leads to an unbreakable cryptographic scheme. Despite advantages the protocol still can be improved in at least two aspects: its efficiency which is of about 50%, only half of the photons transmitted are used to create the encryption key and the second aspect refers to the communication that takes place on the classic channel, as it must be reduced or even eliminated. The paper presents a method that improves the two aspects of the BB84 protocol by using quantum memory and eight states of polarization. The implementation of both the proposed method and the BB84 protocol was done through a C# application.

***Keywords*—**BB84, protocol, quantum cryptography, quantum key distribution.

## I. Introduction

QUANTUM cryptography, whose principles are based on the quantum mechanics laws, solves the key distribution problem, existing in classical cryptography. Although the first quantum distribution system was created by Bennet and Brassard [1] in 1984, quantum cryptography awoke the interest of researchers a decade later when Shor [2] proposed a polynomial-time quantum algorithm for the factoring problem. In 1994 he showed that quantum computers could efficiently factor large numbers, thereby rendering any encrypted information vulnerable to decryption.

The basic idea of the BB84 protocol is to encode bits using photon polarization. The transmitter sends the receiver a series of polarized photons by four polarization directions ↑ →, ↗ and ↖. The first two directions are orthogonal in the rectilinear basis and the other two are orthogonal in the diagonal basis. Each direction is associated with a bit; the polarization states ↑ and ↗ are assigned the value of bit 0 and to states →, ↖ the value of bit 1.

The security of the protocol is based on a fundamental property of quantum mechanics that states that the process of measuring a quantum system disrupts the system. Therefore, two communicating users can detect the presence of a third person trying to obtain information about the transmitted key by measuring it and thus detecting detectable errors.

The second remarkable protocol is proposed in 1991 by Ekert [3], but unlike BB84, which uses single photons and is based on the Heisenberg principle, the E91 protocol uses entangled photons and is based on Bell's theorem.

In the E91 protocol a single source emits pairs of entangled polarized photons, one photon is sent to Alice and the other one to Bob. Alice measures polarisation along three different angles $0^0$, $45^0$ and $90^0$ while Bob measures along $45^0$, $90^0$ and $135^0$. Bob and Alice measure their received photons using a random sequence of bases. After the measurements are completed Alice and Bob publicly reveal the polarization basis they used. The photons measured with the same basis must be anti-correlated and are used as bits to generate the key and all the other photons are used to test the Bell's inequality which should not hold for entangled particles. If the Bell's inequality does hold, it indicates the presence of an eavesdropper.

A simplified version of BB84 is proposed by Charles Bennett in 1992 [4]. The essential difference in B92 is that only two states are necessary rather than the possible four polarization states in BB84. The transmitter sends a random series of encoded bits in the two polarization states and the receiver without disclosing the polarization states uses publicly announces in which cases a positive result has occurred, and the other cases are not taken into account. There followed a series of protocols, more or less improved versions of the first two. Among these, we mention the protocol with six polarization states SSP [5] proposed by Pasquinucci and Gisin in 1999 which is identical to the BB84 protocol, except that it uses six polarization states. Adding another base increases the security level of the protocol because it causes the intruder to produce more errors making it easier to be detected.

A variant of the SSP protocol with entangled photons but with added security is described by Enzer et al. [6] in 2002.

In 2004, Scarani et al. propose another protocol SARG04 [7], the transmitter does not disclose the bases used but announces a pair of non-orthogonal states in which it coded the bit. If the receiver uses the correct base, it will measure the correct status; otherwise it will not be able to determine the transmitted bit.

## II. BB84 – Brief Description

The BB84 protocol enables two parties: Alice (the transmitter) and Bob (the receiver) to share a random secret key. The users are connected through two communication channels: a quantum one and a classical one. The quantum channel is used to transmit the photons 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 main stages of BB84 protocol are as follows:

1) Alice, using a random number generator, creates a random sequence of classical bits, and then she sends to Bob a string of polarized photons according to the bit sequence generated.
2) Bob receives Alice's photons and measures them using a

Liliana Zisu is with "Ferdinand I" Military Technical Academy, Bucharest, Romania (e-mail: liliana_zisu@yahoo.com).

random sequence of bases.

3) Bob publicly announces the bases used. If Alice and Bob measured in the same base, that bit is added to the key, otherwise it is dropped. The key thus obtained is called raw key.
4) Bob estimates 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 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.
5) Transforming the original key into a different one that reduces Eve's information is called privacy amplification.

## III. Eight-State BB84 with Photon Storage

The method proposed involves the use of quantum memory by the receiver. Bob does not measure the received photons, as it happens in the BB84 protocol, but memorizes them and then waits for Alice to transmit, over a classic channel, the four bases she used to polarize the photons: rectilinear basis (+), $45^0$ - $135^0$ diagonal basis (x), $20^0$ - $110^0$ diagonal basis (y) or $60^0$ - $150^0$ diagonal basis (z). For each basis, Alice designates a direction as 0 and the other as 1as shown in Fig. 1. She sends these options to Bob through unencrypted text.

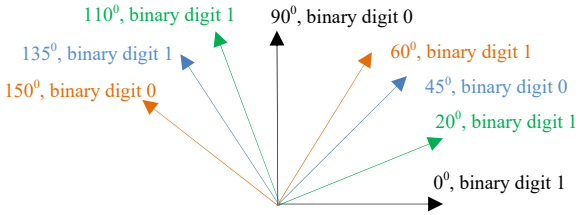


Fig. 1 Polarization states

The main stages of Eight-State BB84 protocol are as follows:

1) Alice, using a random number generator, creates a random sequence of classical bits, and then she sends Bob a string of polarized photons according to the bit sequence generated.
2) Bob does not measure the received photons, as it happens in the BB84 protocol, but memorizes them and then waits for Alice to transmit, over a classic channel, the four bases she used to polarize the photons: rectilinear basis (+), $45^0$ - $135^0$ diagonal basis (x), $30^0$ - $120^0$ diagonal basis (y) or $20^0$ - $110^0$ diagonal basis (z).
3) Bob estimates the error rate and if its value exceeds 8% the protocol is resumed or abandoned. Otherwise, the reconciled key is extracted.
4) Alice and Bob perform the privacy amplification stage to reduce the information gained by Eve.

## IV. Simulation and Results

The implementation of both the proposed method and the BB84 protocol was done through a C# application.

The simulators were built on three aspects: ideal conditions, real environment and absence of an intruder, real environment and presence of an intruder.

Achieving the implementation of simulation of protocol assuming ideal conditions (in the absence of errors, whether caused by noise, imperfection of the photon detector or the presence of an intruder) is required to understand the complexity of protocol, representing a milestone that tells us how we must improve devices for optimal operation.

The intruder's attack is 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 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 photons, 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 I.

TABLE I
Symbols & Bases

| Basis | Symbol | Bit Value Associated |
|---|---|---|
| *Rectilinear (+)* | h | 1 |
| | v | 0 |
| *$45^0$- $135^0$ Diagonal (x)* | a | 0 |
| | o | 1 |
| *$60^0$ - $150^0$ Diagonal (y)* | f | 1 |
| | t | 0 |
| *$20^0$ – $110^0$ Diagonal (z)* | e | 0 |
| | u | 1 |

The error in simulators does not exceed 10%.

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, computer clock, memory status, and other processes.

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.

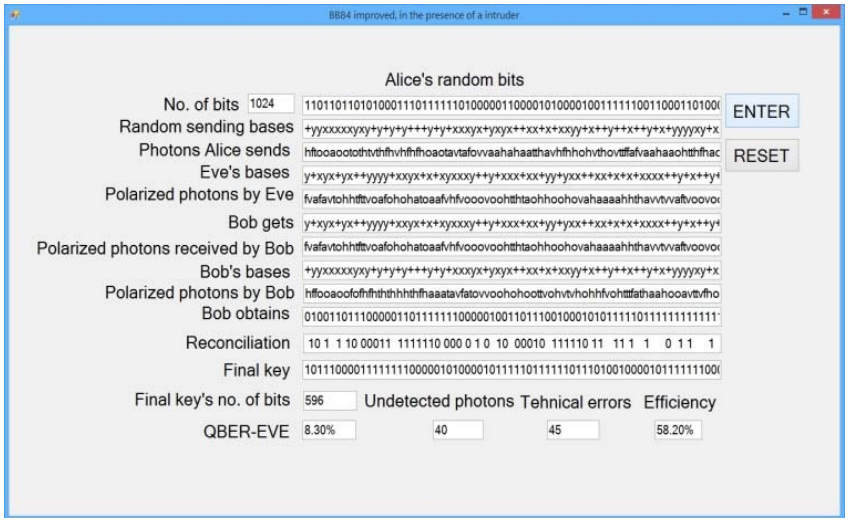


Fig. 2 Graphical simulator interface

### A. BB84 Simulation

The simulation of the BB84 algorithm, whose results are presented in Table II, 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 II
EFFICIENCY OF THE BB84 PROTOCOL (%)

| Under ideal conditions | In the absence of an intruder | In the presence of an intruder |
|---|---|---|
| 51.59 | 44.92 | 22.95 |
| 49.02 | 47.17 | 22.17 |
| 49.32 | 47.36 | 24.02 |
| 51.07 | 45.70 | 25.00 |
| 51.46 | 46.78 | 22.85 |
| 50.00 | 48.63 | 21.58 |
| 51.56 | 47.46 | 23.73 |
| 51.66 | 45.61 | 22.85 |
| 51.86 | 48.24 | 25.98 |
| 51.59 | 47.46 | 23.63 |
| 49.06 | 45.81 | 22.78 |
| 52.35 | 47.88 | 23.01 |
| 50.39 | 48.83 | 24.51 |
| 49.71 | 43.55 | 26.27 |
| 48.14 | 46.68 | 24.90 |

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

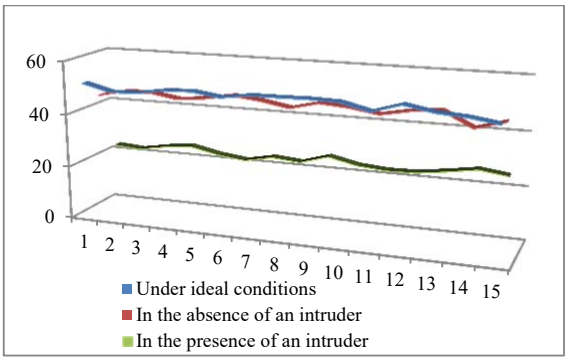


Fig. 3 BB84 Efficiency

The security of BB84 protocol is unconditional, relies only on the laws of quantum mechanics and was theoretically first proved by Mayers [8].

### B. Eight-State BB84 with Photon Storage Simulation

The obtained results as shown in Table III indicate the maximum efficiency of the algorithm under ideal conditions. In the absence of an intruder, photons are transmitted with an average efficiency greater than 90% and decreases to 55% under the action of an intruder.

The simulation results do not differ from expected values, as the receiver knows the polarization bases used by the transmitter. Compared to BB84 protocol, the values obtained for the proposed protocol show a high efficiency, almost double. As the intruder's action is aggressive and massive, the degree of disturbance of quantum communication is also great.

The graphical representation of the efficiency of the Eight-State BB84 protocol is shown in Fig. 4. Even if the efficiency of the protocol, in the presence of an intruder, is represented graphically, it has no relevance to the key, the process of quantum communication being aborted or resumed.

To determine the security level of the proposed protocol, we analysed the cases with four, six and eight states of polarization, the protocol remaining unchanged, except the

number of polarization bases.

TABLE III
EFFICIENCY OF THE EIGHT-STATE BB84 PROTOCOL WITH PHOTON STORAGE (%)

| Under ideal conditions | In the absence of an intruder | In the presence of an intruder |
|---|---|---|
| 100 | 98.24 | 54.98 |
| 100 | 95.80 | 53.71 |
| 100 | 96.88 | 55.57 |
| 100 | 95.51 | 53.32 |
| 100 | 97.95 | 54.69 |
| 100 | 94.34 | 55.18 |
| 100 | 98.63 | 52.54 |
| 100 | 94.53 | 54.49 |
| 100 | 97.56 | 53.81 |
| 100 | 94.43 | 56.45 |
| 100 | 93.97 | 55.04 |
| 100 | 95.05 | 54.30 |
| 100 | 93.16 | 54.10 |
| 100 | 94.92 | 54.59 |
| 100 | 93.55 | 54.98 |

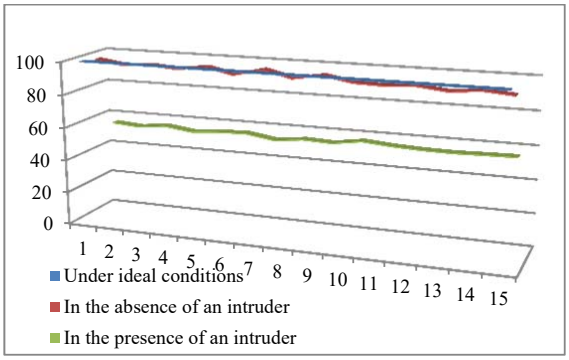


Fig. 3 Eight-State BB84 with Photon Storage Efficiency

A simple graphical representation of the obtained results of the quantum bit error rate (QBER) based on efficiency in the two cases in the absence or presence of an intruder, evidenced in Fig. 4 clearly shows the natural situation when an intruder does not intervene, the efficiency being inversely proportional to the errors. The intruder's action destroys this ratio, as outlined in Fig. 5. Moreover, Eve makes errors even when choosing the right base. If she polarizes with rectilinear basis, for example vertically, and Alice chooses horizontally, and Bob chooses vertically as well, he will think that the corresponding bit is 0 when in fact the bit chosen by Alice was actually 1. Also, from the analysis of the results graphically represented in Fig. 5, the security level of the Eight-State protocol is greater than that of the other two, as the higher number of polarization states causes the intruder to produce more errors and to be more easily detected.

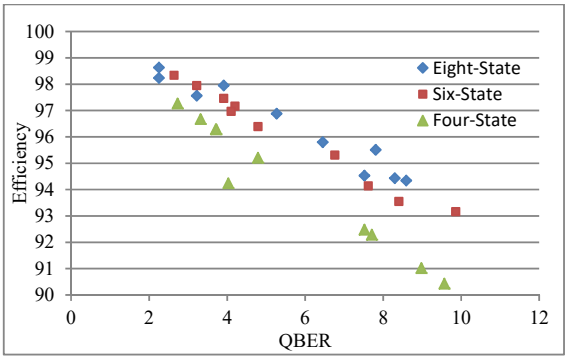


Fig. 4 In the absence of an intruder

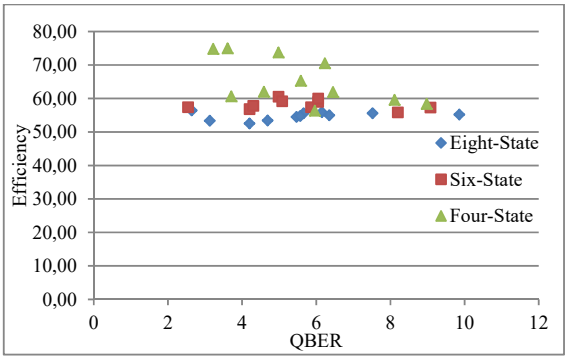


Fig. 5 In the presence of an intruder

## REFERENCES

[1] C. H. Bennett, G. Brassard, "Quantum Cryptography: Public key distribution and coin tossing", International Conference on Computers, Systems & Signal Processing, Bangalore, India, 10-12 December 1984, pp. 175-179.
[2] P. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer", SIAM Journal of Computing, 26, 1997, pp. 1484-1509.
[3] A. K. Ekert, "Quantum cryptography based on Bell's theorem", Physical Review Letters, vol. 67, no. 6, 5 August 1991, pp. 661 - 663.
[4] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states ", Phys. Rev. Lett. 68, 1992, pp. 3121-3124.
[5] H. Bechmann-Pasquinucci, N. Gisin, "Incoherent and coherent eavesdropping in the six-state protocol of quantum cryptography" Phys. Rev. A 59, 4238-4248, 1999.
[6] D. Enzer, P. Hadley, R. Gughes, C. Peterson, P. Kwiat, "Entangled-photon six-state quantum cryptography", New Journal of Physics, 2002, pp 45.1-45.8.
[7] A. Scarani, A. Acin, G. Ribordy, N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks.", Physical Review Letters, vol. 92, 2004.
[8] D. Mayers, "Unconditional security in quantum cryptography," Journal of the ACM, vol. 48, no. 3, pp. 351–406, May 2001.