Research, Development and Simulation of Quantum Cryptographic Protocols

C. Anghel[1]
[1]*University "Dunărea de Jos" Galati,*
2 Ştiinţei, 800146 Galati, Romania, phone: +40 745 802 834
anghelcata@yahoo.com

***Abstract*—Cryptography is the art of hiding information. Quantum cryptography is the next level in cryptography. This paper presents the development and the software simulation of BB84 without eavesdropper, BB84 with eavesdropper, BB84 with QBTT eavesdropper detection method and BSPA quantum cryptographic communication protocol.**

***Index Terms*—Quantum cryptography, quantum key distribution, access protocols.**

I. INTRODUCTION

A cryptographic algorithm combined with a communication system result in a cryptographic system. Almost any cryptographic system, given enough time and resources could eventually be solved. The only exception to this is a system which uses absolutely random changing keys with every character encrypted and never repeated, named One Time Pad [1], [2].

The other cryptographic algorithms, used in our days, are founded on complexity of the mathematical algorithms, but computers become faster and faster and to break an encrypted message becomes a matter of computational power. Consequently, efforts have been made to establish new foundations for cryptography. One of these efforts has led to the development of quantum cryptography, whose security relies not on assumptions about computer power, but on the laws of quantum physics.

Although many quantum cryptographic schemes have been proposed [3], [4], the one well researched and realized experimentally is the quantum key distribution protocol (QKD).

Also, some QKD commercial products are available [5], [6]. The QKD schemes, in general, utilized photons to transfer classical bit information. Thus, using quantum physics phenomena, we can build a perfectly secure key distribution system – this is known as quantum key distribution (QKD). The keys produced using QKD are guaranteed to be secret – as is proved by BB84 protocol [7], [8] and may be used in conjunction with any classical cryptographic system (CCS).

II. BB84 ALGORITHM OF QUANTUM KEY DISTRIBUTION

BB84 is the first known quantum key distribution scheme, named after the original paper by Bennett and Brassard, published in 1984 [7]. BB84 allows the two parties, Sender and Receiver, to establish a secret, common key sequence using polarized photons – qbits.

To implement the BB84 algorithm we chose for photon polarization the rectilinear (R) and diagonal (D) bases and the convention from Table I to represent the bits from the key.

TABLE I. PHOTON POLARIZATION.

Base	**Rectiliniar**	**Diagonal**	**Rectiliniar**	**Diagonal**
State	0°	45°	90°	135°
Qbit	→	↗	↑	↖
Bit	0	0	1	1

A. Steps of the BB84 key distribution system

The steps of the BB84 quantum key distribution algorithm are:

1) Sender generates a random binary sequence s;
2) Sender chooses which type of photon to use (rectilinearly polarized, "R", or diagonally polarized, "D") in order to represent each bit in *s*. Let *b* denote the sequence of each polarization base;
3) Sender uses specialized equipment, including a light source and a set of polarizers, to create a sequence p of polarized photons - qbits whose polarization directions represent the bits in s;
4) Sender sends the qbits p to Receiver over an optical fiber;
5) For each qbit received, Receiver makes a guess of which base is polarized: rectilinearly or diagonally, and sets up his measurement device accordingly. Let b' denote his choices of basis;
6) Receiver measures each qbit with respect to the basis chosen in step 5, producing a new sequence of bits s';
7) Sender and Receiver communicate over a classical, possibly public channel. Specifically, Sender tells to Receiver the choice of basis for each bit, and Receiver tells to Sender whether he made the same choice. The bits for which Sender and Receiver have used different bases are discarded from s and s'.

B. Detecting eavesdropper's presence

For the i^{th} bit chosen by Sender, *s[i]*, will correspond a choice of polarization basis, *b[i]*, which is used to encode the bit to a photon. If Receiver's chosen measurement basis is *b'[i]* and the outcome of his measurement is *s'[i]*, then if $b'[i] = b[i]$ should imply $s'[i] = s[i]$.

If an *Eavesdropper* tries to obtain any information about *s[i]*, a disturbance will result and, even if Receiver and

Manuscript received May 17, 2012; accepted September 26, 2012.

Sender's bases match, $s'[i] \neq s[i]$. This allows Sender and Receiver to detect the Eavesdropper's presence, and to reschedule their communications accordingly.

III. QBER EAVESDROPPER DETECTION METHOD

Quantum Bit Error Rate – QBER method involves calculating the percentage of errors in the final key [9], obtained at the end of quantum transmission, after Bases reconciliation stage.

Quantum bit error rate is defined as

$$QBER = \frac{Q_I - Q_F}{Q_I} * 100, \quad (1)$$

where Q_I represent the number of qbits from primary key, and Q_F represent the number of qbits from final key.

QBER method relies on the fact that the eavesdropper will create an increase in the QBER value.

IV. QBTT EAVESDROPPER DETECTION METHOD

The Quantum Bit Travel Time – QBTT method [10] can be implemented in every type of quantum key distribution system and has the advantage that the Eavesdropper can be detected by Receiver, during the quantum transmission, after each transmitted qbit and it is not confused with errors caused by noise because noises does not induce time delays.

This method uses the fact that the optical components (polarization filters) induce time delays [11]. Every polarization filter applied to a photon induces a specific time delay.

So, it is reasonable for a particle to experience a time delay ΔT when it passes through the polarization system on Sender's side and detection system on Receiver's side. This delay can be measured and if an eavesdropper tries to read a photon he will induce an additional time delay Δt. Receiver can measure these time delays and use them to detect the Eavesdropper's presence because the final time delay will be

$$\Delta T' = \Delta T + \Delta t, \quad (2)$$

V. BASE SELECTION AND POLARIZATION AGREEMENT PROTOCOL

Founded on Base Selection and Transmission Synchronization quantum cryptographic protocol [12] and Quantum Bit Travel Time eavesdropper detection method [10], we obtain a quantum transmission cryptographic protocol, named Base Selection and Polarization Agreement – BSPA [13].

Based on the bits from the final key, common to Sender and Receiver, targeted parameters in Base Selection and Polarization Agreement quantum cryptographic protocol are:

1) Which pair of bases, between rectilinear (0°, 90°), diagonal (45°, 135°) and circular (left - spinL, right - spinR), will be used for photons polarizations;
2) The polarization base for each photon that has to be transmitted, so the Sender and Receiver will know for each particular photon the polarization base;
3) Eavesdropper detection by monitoring the travel time, from Sender to Receiver, of each photon;
4) Comparison the parity of the blocks received, at the end of quantum transmission and retransmission of the corresponding blocks.

For photon polarization we use the convention from Table II.

TABLE II. PHOTON POLARIZATION.

Base	L	D	C	C	L	D
Polarization	0°	45°	spinL	spinR	90°	135°
Qbit	↔	⤢	↺	↻	↕	⤡
Bit	0	0	0	1	1	1

In Base Selection and Polarization Agreement quantum communication protocol, Sender and Receiver will establish in common, accordingly to the final key, which pair of bases, rectilinear-diagonal, rectilinear-circular or diagonal-circular will be used for photons polarizations.

Also, accordingly to the final key, Sender and Receiver will establish exactly which polarization base to apply for each photon that has to be transmitted or received.

During quantum transmission, after every received qbit, Receiver will verify the time delay ΔT of the photon from the moment of transmission and the moment of reception.

If the delay time ΔT is not in normal limit, limits established by earlier communications, Receiver will stop the transmission.

At the end of quantum transmission, Sender and Receiver divide their bit sequences into blocks. They communicate thru the classical channel, comparing each other's blocks parity and retransmitting blocks that the parity did not match.

VI. SIMULATION OF BB84 WITHOUT EAVESDROPPER'S PRESENCE

For the BB84 without Eavesdropper implementation, the software has been developed using C++ language. Sender and Receiver will communicate through quantum channel and classical channel without the presence of Eavesdropper.

This software consists of 4 objects, which are Sender, Receiver, quantum channel and classical channel. Sender will transmit qbits through the quantum channel and Receiver will acquire those qbits from the quantum channel. At the end of the quantum transmission, Sender and Receiver will communicate through the classical channel and will proceed with Bases reconciliation, Secret key reconciliation and Privacy Amplification stages.

A. Hardware setup

Block diagram of BB84 without Eavesdropper implementation is presented in Fig. 1.

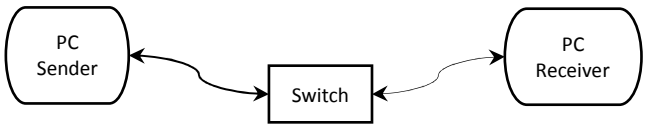

Fig. 1. Implementation of BB84 without Eavesdropper.

Devices used in this implementation are:

1) 2 workstation;
2) 1 switch or router.

Each workstation represents the Sender and the Receiver. Static IP are used so that workstation can communicate via

the switch. Developed software is installed on each workstation to simulate the protocol.

B. Software setup

For this simulation, each of object (Sender and Receiver) play different role. Only the appropriate function is executed on each of workstation, depends on its role, as shown in Fig. 2.

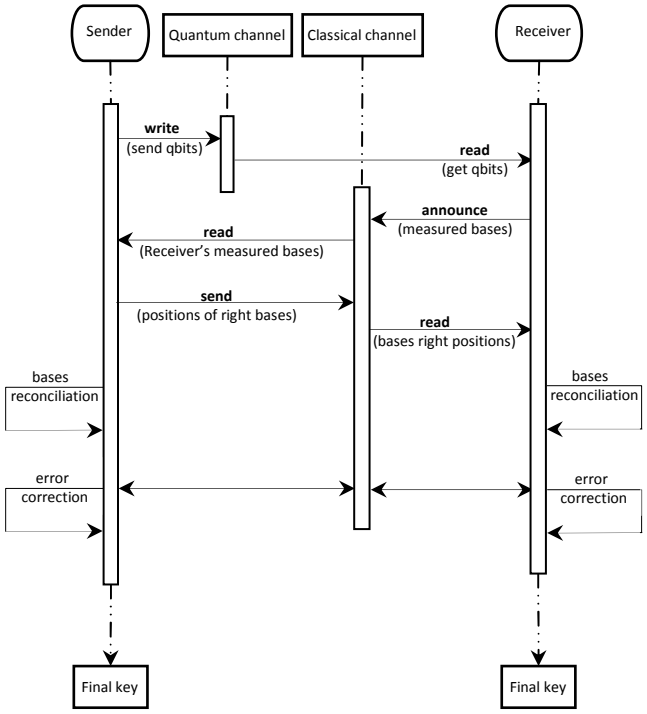

Fig. 2. Software protocol.

C. Experimental Results

After running the BB84 without eavesdropper simulation program 10 times, for a 320 bits primary key, we obtain the results from Table III.

TABLE III. SIMULATION RESULTS OF BB84 WITHOUT EAVESDROPPER.

Primary key	Final key	QBER %
320	162	49.4
320	161	49.7
320	152	52.5
320	172	46.3
320	158	50.6
320	153	52.2
320	165	48.4
320	163	49.1
320	150	53.1
320	160	50.0

Analysing these data we can see that QBER value is approximately 50%, as shown in Fig. 3.

VII. SIMULATION OF BB84 WITH EAVESDROPPER

For the BB84 implementation, Sender and Receiver will communicate through quantum channel and classical channel with or without the presence of Eavesdropper.

This software consists of 5 objects, which are Sender, Receiver, Eavesdropper, quantum channel and classical channel. Sender will transmit qbits through the quantum channel.

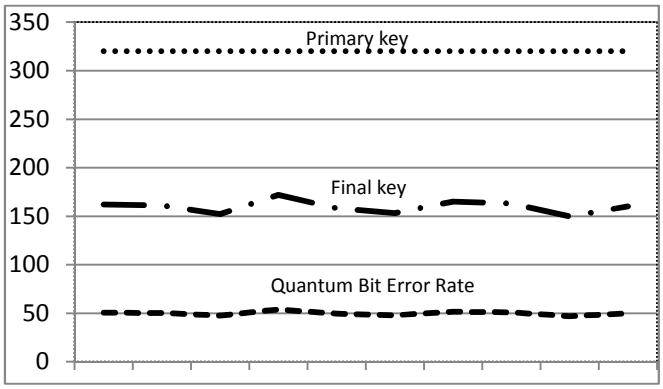

Fig. 3. QBER – Primary key vs. Final key.

Eavesdropper will interrupt the quantum channel, intercept those qbits, read them and send to Receiver other qbits accordingly to his choice of bases. Receiver will acquire those modified qbits from the quantum channel. At the end of the quantum transmission, Sender and Receiver will communicate through the classical channel, which can be tapped but not modified, and will proceed with Bases reconciliation, Secret key reconciliation and Privacy Amplification stages.

A. Hardware setup

Block diagram of BB84 implementation is presented in Fig. 4.

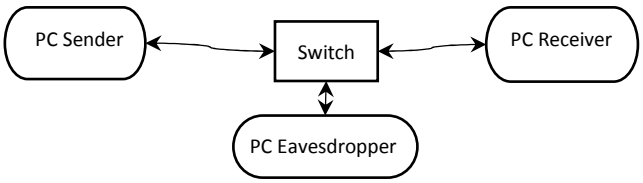

Fig. 4. Implementation of BB84 with eavesdropper.

Devices used in this implementation are:

1) 3 workstation;
2) 1 switch or router.

Each workstation represents the Sender and the Receiver. Static IP are used so that workstation can communicate via the switch. Developed software is installed on each workstation to simulate the protocol.

B. Software setup

For this simulation, each of object (Sender and Receiver) play different role. Only the appropriate function is executed on each of workstation, depends on its role, as shown in Fig. 5.

C. Experimental results

After running the BB84 with eavesdropper simulation program 10 times, for a 320 bits primary key, we obtain the results from Table IV.

TABLE IV. SIMULATION RESULTS OF BB84 WITH EAVESDROPPER.

Primary key	Raw key	Final key	QBER %
320	149	110	65.6
320	156	114	64.4
320	172	129	59.7
320	164	131	59.1
320	167	126	60.6
320	144	105	67.2

Primary key	Raw key	Final key	QBER %
320	159	105	67.2
320	133	108	66.3
320	162	117	63.4
320	171	123	61.6

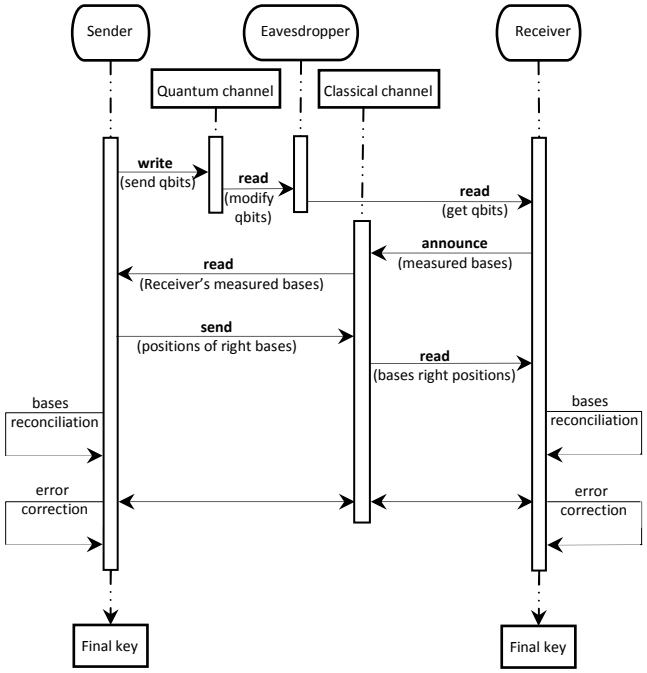

Fig. 5. Software protocol.

Analysing these data we can see that QBER for BB84 with eavesdropper is approximately 64%, Fig. 6, with 14% greater than QBER for BB84 without eavesdropper, because the eavesdropper tapped the quantum channel.

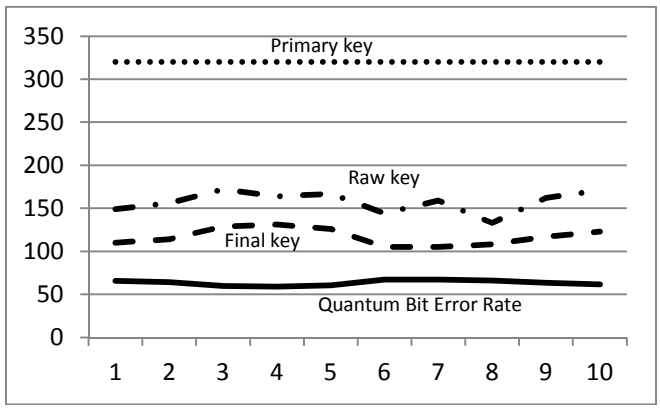

Fig. 6. QBER – Primary key vs. Raw key vs. Final key.

VIII. SIMULATION OF BB84 WITH QBTT

For the simulation of BB84 with QBTT eavesdropper detection method, the software has been developed using C++ language. Sender and Receiver will communicate through quantum channel and classical channel with or without the presence of the Eavesdropper.

A. Hardware setup

Block diagram of BB84 implementation is presented in Fig. 4.

Devices used in this implementation are:

1) 3 workstation;
2) 1 switch or router.

B. Software setup

For this simulation, only the appropriate function is executed on each of workstation, depends on its role, as shown in Fig. 7.

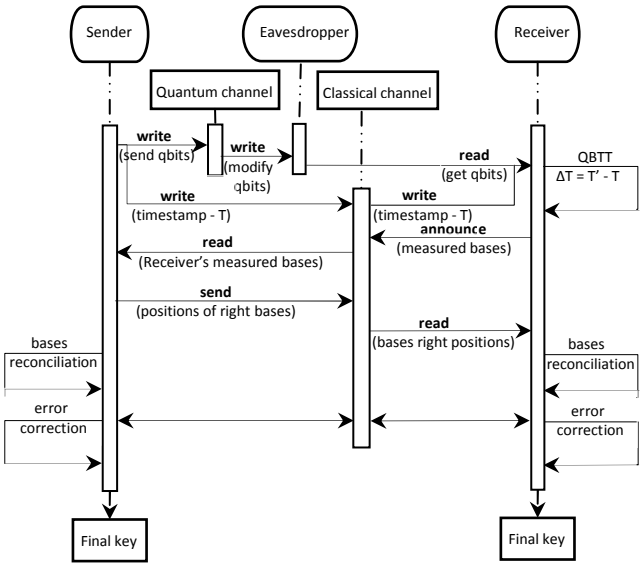

Fig. 7. Software protocol.

C. Experimental results

After running the BB84 with QBTT simulation program 10 times, for a 320 bits primary key, we obtain the results from Table V.

TABLE V. SIMULATION RESULTS OF BB84 WITH QBTT.

Primary key	Raw key	Final key	QBER %
320	148	148	52.2
320	150	150	51.6
320	167	167	46.3
320	157	157	49.4
320	159	159	48.8
320	152	152	50.9
320	168	168	45.9
320	157	157	49.4
320	158	158	49.1
320	162	162	47.8

Analysing these data we can see that QBER value is approximately 50%, Fig. 8, although the eavesdropper was present.

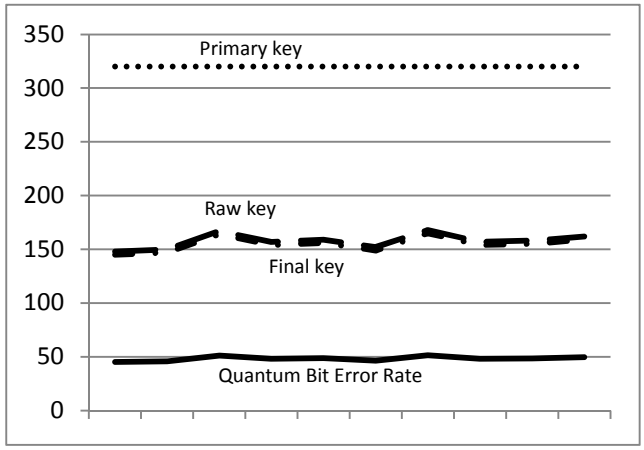

Fig. 8. QBER – Primary key vs. Raw key vs. Final key.

IX. SIMULATION OF BSPA PROTOCOL

For the simulation of the Base Selection and Polarization Agreement protocol, the software has been developed using C++ language. Sender and Receiver will communicate through quantum channel and classical channel with or without the presence of the Eavesdropper.

A. Hardware setup

Block diagram of BB84 implementation is presented in Fig. 4.

Devices used in this implementation are:

1) 3 workstation;
2) 1 switch or router.

All devices are setup in the same room. Switch or router is used to connect all workstation. Each workstation represents the Sender, Receiver and the Eavesdropper. Static IP are used so that workstation can communicate via the switch. Developed software is installed on each workstation to simulate the protocol.

B. Software setup

This software consists of 5 objects, which are Sender, Receiver, Eavesdropper, quantum channel and classical channel.

Sender and Receiver will establish in common, accordingly to the final key, which pair of bases, rectilinear-diagonal, rectilinear-circular or diagonal-circular will be used for photons polarizations.

Also, accordingly to the final key, Sender and Receiver will establish exactly which polarization base to apply for each photon that has to be transmitted or received.

Sender will transmit qbits through the quantum channel and timestamp of each qbit through the classical channel. Eavesdropper will interrupt the quantum channel, intercept those qbits, read them accordingly to his choice of bases and send to Receiver other qbits accordingly to his choice of bases.

Receiver will acquire those qbits from the quantum channel and for each received qbit will verify the time delay ΔT of the photon from the moment of transmission and the moment of reception.

The software setup is presented in Fig. 9.

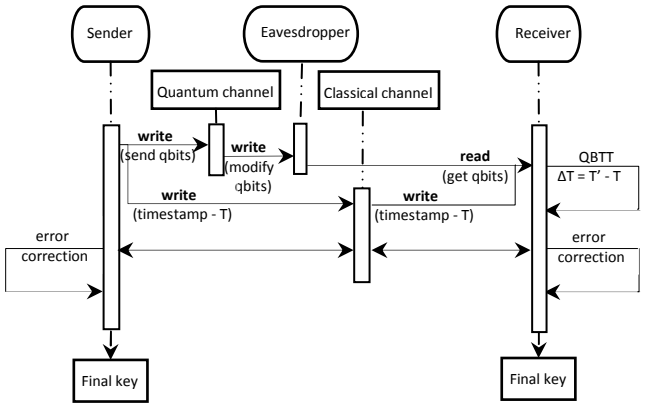

Fig. 9. Software protocol.

C. Experimental results

After running the BSPA simulation program 10 times, for a 320 bits primary key, we obtain the results from Table VI.

TABLE VI. SIMULATION RESULTS OF BSPA.

Primary key	Final key	QBER %
320	320	0.0
320	317	0.9
320	320	0.0
320	319	0.3
320	320	0.0
320	317	0.9
320	320	0.0
320	319	0.3
320	320	0.0
320	319	0.3

Analyzing these data we can see that QBER value is approximately 0.27%, as shown in Fig. 10.

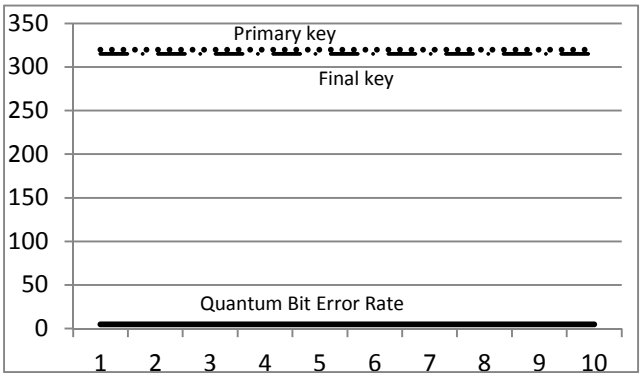

Fig. 10. QBER – Primary key vs. Final key.

X. CONCLUSIONS

The software simulation programs are meant to give an alternative to physical implementation of the quantum devices used in the quantum transmission.

This paper presents a comparison of the Quantum Bit Error Rate – QBTT, between BB84, BB84 with attacks, BB84 with QBTT and BSPA protocols (Fig. 11, Appendix A)

We can observe the advantages of the Quantum Bit Travel Time – QBTT eavesdropper detection method by reducing the percentage of the Quantum Bit Error Rate – QBER from the final key and also the advantages of the Base Selection and Polarization Agreement – BSPA quantum communication protocol by reducing near 0,3 % the percentage of QBER.

APPENDIX A

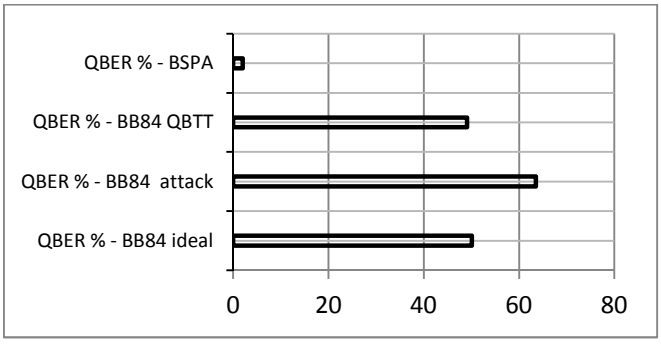

Fig. 11. QBER comparison.

REFERENCES

[1] G. S. Vernam, "Cipher printing telegraph systems for secret wire and radio telegraph communications", *Journal of the IEEE,* vol. 45, pp. 109–115, 1926.

[2] W. Yong, "Unconditional Security of Cryptosystem: A Review and Outlook", *Trends in Applied Sciences Research,* vol. 6, no. 6, pp. 554–562, 2011. [Online]. Available: http://dx.doi.org/10.3923/tasr.2011.554.562

[3] L. Bin, G. Fei, W. Qiao-Yan, "Single-Photon Multiparty Quantum Cryptographic Protocols with Collective Detection", *IEEE Journal of Quantum Electronics,* vol. 47, no. 11, pp. 1383–1390, 2011. [Online]. Available: http://dx.doi.org/10.1109/JQE.2011.2167743

[4] B. Harry, C. Nishanth, et al, "Position-Based Quantum Cryptography: Impossibility and Constructions", *Advances in Cryptology – Lecture Notes in Computer Science,* vol. 6841, pp. 429–446, 2011.

[5] *Quantum Key Distribution System (Q-Box) – hardware equipment,* MagiQ Technologies Inc. [Online]. Available: http://www.magiqtech.com/MagiQ/Products.html

[6] *IDQ's Cerberis solution – hardware equipment,* Id Quantique SA. [Online]. Available: http://www.idquantique.com/network-encryption/cerberis-layer2-encryption-and-qkd.html

[7] C. H. Bennett, G. Brassard, "Quantum cryptography: Public key distribution and coin tossing", in *Proc. of IEEE International Conference on Computers Systems and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[8] M. K. Muhammad, X. Jie, "Generalization of Quantum Key Distribution Protocol", *International Journal of Computer Science and Network Security,* vol. 12, no. 8, pp. 98–101, 2012.

[9] A. Treiber, "A fully automated quantum cryptography system based on entanglement for optical fiber networks", *New Journal of Physics,* vol. 11, no. 4, pp. 1–19, 2009. [Online]. Available: http://dx.doi.org/10.1088/1367-2630/11/4/045013

[10] C. Anghel, "New eavesdropper detection method in quantum cryptography", *The annals of "Dunarea de Jos" University of Galati,* vol. 34, no. 1, pp. 1–8, 2011.

[11] S. Zhao, H. De Raedt, "Event-by-event Simulation of Quantum Cryptography Protocols", *Journal of Computational and Theoretical Nanoscience,* vol. 5, no. 4, pp. 490–504, 2008.

[12] C. Anghel, G. Coman, "Base selection and transmission synchronization algorithm in quantum cryptography", in *Proc. of the 17th International Conference on Control Systems and Computer Science (CSCS17)*, Bucharest, Romania, 2009, vol. 1, pp. 281–284.

[13] C. Anghel, "New quantum cryptographic protocol", *The annals of "Dunarea de Jos" University of Galati,* vol. 34, no. 2, pp. 7–13, 2011.