THE ANNALS OF "DUNAREA DE JOS" UNIVERSITY OF GALATI
FASCICLE III, VOL.34, NO.1, 2011, ISSN 1221-454X
ELECTROTECHNICS, ELECTRONICS, AUTOMATIC CONTROL, INFORMATICS

NEW EAVESDROPPER DETECTION METHOD IN QUANTUM CRYPTOGRAPHY

Cătălin Anghel – PhD Student in Systems Engineering

Faculty of Computer Science, University "Dunărea de Jos" of Galati
Galati, Romania (e-mail: catalin.anghel@ugal.ro

Abstract: Security of quantum cryptographic algorithms is one of the main research directions in quantum cryptography. Security growth of the quantum key distribution systems can be realized by detecting the eavesdropper quickly, precisely and without letting any secret information in the hands of the enemy. This paper proposes a new method, named QBTT, to detect the enemy who try to tap the communication channel. The QBTT method can be implemented in every type of quantum key distribution scheme.

Keywords: quantum cryptography, quantum physics, quantum key distribution, qkd, cryptography, quantum algorithm.

INTRODUCTION

A cryptographic algorithm combined with a communication system result in a cryptographic system. Almost any cryptographic system, given enough time and resources can 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. In 1917, Vernam proposed One Time Pad (OTP) encryption scheme (Vernam, 1926) also known as Vernam Cipher and in 1949, Shannon proved that the one-time pad is information-theoretically secure, no matter how much computing power is available to the eavesdropper (Shannon, 1949).

So, the One Time Pad is the only cryptosystem that have been proved to be perfectly secure if the key is truly random, never reused and kept secret. Despite Shannon's proof of its security, the one-time pad has serious drawbacks in practice:

- it requires a perfectly random key;
- a secure key generation and exchange;
- the key must be at least as long as the message.

These implementation problems have lead to one-time pad systems being unpractical and are so serious that they have prevented the one-time pad from being adopted as a widespread tool in information security.

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 lead 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 (Waseda, *et al.*, 2008; Li, and Chen, 2007), the one well researched and realized experimentally is the quantum key distribution protocol (QKD). Also, some QKD commercial products are available (MagiQ Technologies; id Quantique). 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 (Bennett, and Brassard, 1984; Bennett, *et al.*, 1992), and may be used in conjunction with any classical cryptographic system (CCS) (Shannon, 1949).

In conclusion, a perfectly secure cryptographic communication system can be obtained if we use a quantum key distribution system in conjunction with one-time pad cryptographic algorithm.

QUANTUM KEY DISTRIBUTION - PRELIMINARIES

Electromagnetic waves such as light waves can exhibit the phenomenon of polarization, in which the direction of the electric field vibrations is constant or varies in some definite way. A polarization filter is a material that allows only light of a specified polarization direction to pass. Information about the polarization of the photon can be determined by using a photon detector to determine whether it passed through a filter. In quantum key distribution, any attempt of an enemy to obtain the bits in a key not only fails, but is detected as well. Specifically, each bit in a key corresponds to the state of a certain particle, such as the polarization of a photon – named quantum bit – qbit (Nielsen, and Chuang, 2000).

The sender of a key has to prepare a sequence of polarized photons - qbits, which are sent to the receiver through an optical fiber. In order to obtain the key represented by a given sequence of photons, the receiver must make a series of measurements using a set of polarization filters.

A photon can be polarized rectilinear (R) in one of the states (0^o, 90^o), diagonal (D) in one of the states (45^o, 135^o) and circular (left – spin L, right – spin R). The process of mapping a sequence of bits to a sequence of rectilinearly, diagonally or circularly polarized photons is referred to as conjugate coding, while the rectilinear, diagonal and circular polarization are known as conjugate variables. Quantum theory stipulates that it is impossible to measure the values of any pair of conjugate variables simultaneously. The same impossibility applies to rectilinear, diagonal and circular polarization for photons. For example, if someone tries to measure a rectilinearly polarized photon with respect to the diagonal one, all information about the rectilinear polarization is lost.

BB84 ALGORITHM OF QKD

BB84 is the first known quantum key distribution scheme, named after the original paper by Bennett and Brassard, published in 1984. 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 following convention to represent the bits from the key.

Table 1. Photon polarization

Base	R	D	R	D
State	0^o	45^o	90^o	135^o
Qbit	→	↗	↑	↖
Bit	0	0	1	1

1.1. Steps of the BB84 key distribution system

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 polarisers, 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'.

1.2. 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:

$$b'[i] = b[i] \text{ should imply } s'[i] = s[i]$$

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

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

1.3. Pseudo code of the BB84 key distribution system

Step 1 – communication over quantum channel

Sender:
generate string **s** randomly from (0,1)
FOR each bit from **s**
pick randomly from ("R", "D") resulting base **b**[i]
ENDFOR
FOR each bit from **s**
generate a photon
IF **s**[i] = 1 and **b**[i] = R THEN *polarize* the photon in state (90°) result qbit **p**[i] = ↑
IF **s**[i] = 0 and **b**[i] = R THEN *polarize* the photon in state (0°) result qbit **p**[i] = →
IF **s**[i] = 1 and **b**[i] = D THEN *polarize* the photon in state (135°) result qbit **p**[i] = ↖
IF **s**[i] = 0 and **b**[i] = D THEN *polarize* the photon in state (45°) result qbit **p**[i] = ↗
send qbit **p**[i] to ***Receiver***
ENDFOR

Receiver:
FOR each qbit **p′**[i] received
generate RANDOM ("R", "D") result **b′**[i]
measure qbit **p′**[i] in respect to base **b′**[i] result bit ***s′***[i]
ENDFOR

Step 2 – communication over classical channel
Receiver:
FOR each bit ***s′***[i]
send base **b′**[i] to ***Sender***
ENDFOR
Sender:
FOR each bit ***s′***[i]
send base **b**[i] to ***Receiver***
ENDFOR
Step 3 – Bases reconciliation
Receiver:
FOR each bit ***s′***[i]
IF base **b′**[i] ≠ **b**[i]
eliminate bit ***s′***[i] from string ***s′***
ENDIF
ENDFOR
Sender:
FOR each bit **s**[i]
IF base **b**[i] ≠ **b′**[i]
eliminate bit **s**[i] from string **s**
ENDIF
ENDFOR

Step 4 – Detecting Eavesdropper presence
Sender and Receiver:
FOR a subset of bites randomly chosen from string ***s***
IF ***s'****[i] ≠* ***s****[i] and* ***b'****[i] =* ***b****[i]*
Eavesdropper *was present*
ENDIF
eliminate ***s'****[i] and* ***s****[i]*
ENDFOR

B92 ALGORITHM OF QKD

Quantum key distribution protocol B92 (Bennett, 1992), proposed by Charles Bennet in 1992, is similar to the BB84 coding scheme with the difference that *Sender* uses to encode classical bits two non-orthogonal states, fig.1 and *Receiver* uses to measure the qbits all four states used in BB84, fig. 2 and fig. 3.

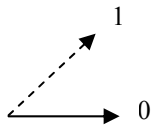

Fig.1. *Sender's* non-orthogonal polarization states

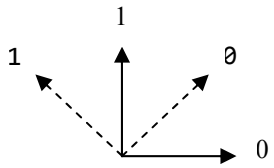

Fig.2. *Receiver's* measurement states

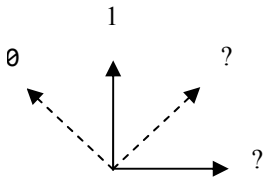

Fig.3. *Receiver's* states interpretation

Since no measurement can distinguish two non-orthogonal quantum states, it is impossible to identify the bit with certainty. Moreover, any attempt to learn the bit will modify the state in a noticeable way. This is the basic idea behind the quantum key distribution protocol B92.

To implement the B92 algorithm we use for photon polarization on *Sender's* side, convention from table

2 and photon measurement on *Receiver's* side, convention from table 3.

Table 2. Photons polarization for *Sender*

Sender		
State	0^o	45^o
Qbit	→	↗
Bit	0	1

Table 3. Photons polarization for *Receiver*

Receiver				
State	0^o	45^o	90^o	135^o
Qbit	→	↗	↑	↖
Result	0	0	1	1
Bit	?	?	1	0

1.4. Steps of the B92 key distribution system

1. *Sender* generates a random binary sequence s.
2. *Sender* uses specialized equipment, including a light source and a set of polarisers, to create a sequence p of polarized photons - qbits whose polarization directions represent the bits in s accordingly to table 2.
3. *Sender* sends the qbits p to *Receiver* over an optical fiber.
4. For each qbit received, *Receiver* chooses randomly between rectilinearly "R" and diagonally "D". Let b' denote his choices of basis.
5. *Receiver* measures each qbit with respect to the basis chosen in step 5 and communicates to *Sender* over the classical channel where he detects a '0'.
   If Receiver detects '0' then ***s′ = ?*** and the corresponding bit will be eliminated form ***s′***
   If Receiver detects '1' then ***s′ = 0*** if **b′ = *D*** or ***s′ = 1*** if **b′ = *R***
6. Sender, eliminate from **s** the corresponding bit where he received a '0' from Receiver.

1.5. Detecting Eavesdropper's presence

Eavesdropper's presence is detected by an unusual error rate on *Receiver's* row key. This means that Receiver detects much more '0' than usual. In the absence of the *Eavesdropper*, for the i^{th} bit, if s′[i] ≠ ? then s′[i] = s[i].

If the *Eavesdropper* try to intercept qbit s[i] this will increase the probability Pr{s′[i] = ?} and thus will be detected by *Sender* and *Receiver*.

1.6. Pseudo code of the B92 key distribution system

Step 1 – communication over quantum channel

Sender:
generate string ***s*** randomly from (0,1)
FOR each bit from **s**
generate a photon
IF **s**[i] = 0 THEN *polarize* the photon in state (0^o) resulting qbit **p**[i] = →
IF **s**[i] = 1 THEN *polarize* the photon in state (45^o) resulting qbit **p**[i] = ↗
send qbit **p**[i] to ***Receiver***
ENDFOR

Receiver:
FOR each qbit **p′**[i] received
generate randomly from ("R", "D")
resulting base **b′**[i]
measure qbit **p′**[i] in respect to base **b′**[i]
resulting a value **v** // *where* $v \in \{0, 1\}$
IF **v** = 0
s′[i] = ? *and the corresponding bit will be eliminated from* ***s′***
send value '0' to ***Sender***
ELSE // ***v*** *= 1*
IF **b′**[i] = D
THEN ***s′[i] = 0***
ELSE // ***b′****[i] = R*
THEN ***s′[i] = 1***
ENDIF
ENDIF
ENDFOR
Step 2 – communication over classical channel

Sender:
FOR each value '0' received from ***Receiver***
eliminate the corresponding bit from ***s***
ENDFOR
Step 3 – Detecting Eavesdropper presence

Sender and Receiver:
IF Pr{**s′**[i] = ?} is higher than usual // Pr = probability
Eavesdropper *was present*
ENDIF

CLASSICAL EAVESDROPPER DETECTION METHODS

Detection of the *Eavesdropper* is one of the most important objectives of a quantum cryptographic system. Security of quantum cryptographic systems resides in the effectiveness of detection method of the *Eavesdropper*.

When the *Eavesdropper* is present, he will introduce additional errors in the raw key, as a consequence of not knowing which basis to use for decoding the qbit. There are several methods for detecting the *Eavesdropper* and these methods are used depending on the type of quantum key distribution system.

1. Bits Comparing Method
2. Quantum Bit Error Rate Estimation Method
3. Bell's Inequality Method

1.7. Bits Comparing Method

In the Bits Comparing method, detection of the *Eavesdropper* is realized at the end of quantum transmission after basis announcement over the classical communication channel at the end of the basis reconciliation stage.

Eavesdropper's presence is detected by comparing some of the bits from raw key, obtained after the bases reconciliation stage, and if those bits differ implies that the *Eavesdropper* was present, because any discrepancy between *Sender's* and *Receiver's* raw keys is proof of *Eavesdropper's* intrusion.

So, to detect the *Eavesdropper*, *Sender* and *Receiver* select a random subset of bit locations in the raw key, and publicly compare corresponding bits, making sure to discard from raw key each bit as it is revealed. If at least one comparison reveals an inconsistency, then *Eavesdropper* has been detected, in which case *Sender* and *Receiver* reschedule their transmission.

1.8. Quantum Bit Error Rate Estimation Method

In the Quantum Bit Error Rate Estimation method, detection of the *Eavesdropper* is realized at the end of quantum transmission after basis announcement over the classical communication channel at the end of the basis reconciliation stage (Treiber, 2009).

Eavesdropper's presence is detected by an unusual error rate, named quantum bit error rate, in the raw key, obtained after the bases reconciliation stage. If quantum bit error rate – QBER is higher than usual that means the *Eavesdropper* was present and *Sender* and *Receiver* have to reschedule their transmission.

1.9. Bell's Inequality Method

In this method, detection of the *Eavesdropper*, it is realized at the end of quantum transmission after basis announcement over the classical communication channel at the end of the basis reconciliation stage.

Sender and *Receiver*, on a discussion over a public channel, determine whether or not Bell's inequality (Bell, 1964), applied on rejected bits, is satisfied. If it is, *Eavesdropper's* presence is detected. If not, then *Eavesdropper* is absent.

QBTT EAVESDROPPER DETECTION METHOD

Increasing security of quantum key distribution systems is one of the main research directions in quantum cryptography. Security growth of the quantum key distribution systems can be accomplished by detecting the *Eavesdropper* instantly, precisely and without letting any secret information in the hands of the enemy.

Instantly detection of an eavesdropper – the *Eavesdropper* must be detected in the moment he intervened to read a qbit.

Precisely detection of an eavesdropper – the *Eavesdropper* must not be confused with errors caused by noise of the quantum channel.

Classical detection methods of quantum key distribution systems can detect the *Eavesdropper* after basis announcement over the classical communication channel at the end of the basis reconciliation stage, which means the *Eavesdropper* can learn some secret information about the key.

This paper proposes a new method to detect the enemy who try to tap the quantum communication channel between *Sender* and *Receiver*, named Quantum Bit Travel Time – QBTT. The Quantum Bit Travel Time – QBTT method can be implemented in every type of quantum key distribution system to replace the classical eavesdropper detection method and to increase the security of the system.

1.10. QBTT principle

The Quantum Bit Travel Time – QBTT method 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 – that means instantly – and it is not confused with errors caused by noise because noises does not induce time delays – that means precisely.

The proposed method uses the fact that the optical components (polarization filters) induce time delays. 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 try 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 $\Delta T' = \Delta T + \Delta t$.

MODIFIED BB84 ALGORITHM WITH QBTT METHOD

The Quantum Bit Travel Time – QBTT method can easily be implemented in BB84 quantum key distribution scheme to detect the *Eavesdropper*. Classical detection method of BB84 system can detect the *Eavesdropper* at the end of quantum transmission after the basis announcement over the classical communication channel. The QBTT detection method allows detection of the *Eavesdropper* during the quantum transmission, after each transmitted qbit from *Sender* to *Receiver*.

1.11. Steps of the BB84 key distribution system with QBTT method

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 polarisers, 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. For each qbit from *p*, *Sender* sends to *Receiver* over the classical channel the timestamp of the moment of transmission.
5. For each received qbit, *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. For each received qbit, *Receiver* calculates the delay time ΔT. If *Receiver* finds that the delay time ΔT, for a particular qbit, is much higher than usual that means *Eavesdropper* was present and he stops the communication.
7. *Receiver* measures each qbit with respect to the basis chosen in step 5, producing a new sequence of bits s'.
8. *Sender* and *Receiver* communicate over the classical channel. Specifically, *Sender* tells *Receiver* the choice of basis for each bit, and *Receiver* tells *Sender* whether he made the same choice. The bits for which *Sender* and *Receiver* have used different bases are discarded from s and s'.

1.12. Detecting Eavesdropper's presence

For each qbit received there is a time delay ΔT, between the moment of transmission and the moment of reception. If an *Eavesdropper* tries to tap the quantum channel that imply he have to read the qbits with a polarization filter and thus to induce a new time delay Δt. The final time delay for each tapped qbit will be $\Delta T' = \Delta T + \Delta t$. This allows *Sender* and *Receiver* to detect the *Eavesdropper's* presence, and to reschedule their communications accordingly.

1.13. Pseudo code of the modified BB84 algorithm with QBTT method

Step 1
Sender :
generate RANDOM(0,1) string **s**
FOR each bit from **s**
generate RANDOM("R", "D") result **b**[i]
ENDFOR
FOR each bit from **s**
generate a photon
IF **s**[i] = 1 and **b**[i] = R THEN *polarize* the photon in state (90^o) result qbit **p**[i] = ↑
IF **s**[i] = 0 and **b**[i] = R THEN *polarize* the photon in state (0^o) result qbit **p**[i] = →
IF **s**[i] = 1 and **b**[i] = D THEN *polarize* the photon in state (135^o) result qbit **p**[i] = ↖
IF **s**[i] = 0 and **b**[i] = D THEN *polarize* the photon in state (45^o) result qbit **p**[i] = ↗
send qbit **p**[i] to ***Receiver***
generate timestamp *T*
send the timestamp *T*
ENDFOR
Receiver :
FOR each qbit **p′**[i] received
generate RANDOM("R", "D") result **b′**[i]
measure qbit **p′**[i] in respect to base **b′**[i] result bit ***s′***[i]
generate timestamp *T'*
calculate $\Delta T = T' - T$
IF ΔT is NOT in normal range
Eavesdropper *was present*
stop *transmission*
ENDIF
ENDFOR
Step 2
Receiver :
FOR each bit ***s′***[i]
send base **b′**[i] to ***Sender***
ENDFOR
Sender :
FOR each bit ***s′***[i]
send base **b**[i] to ***Receiver***
ENDFOR
Step 3 – Bases reconciliation
Receiver :
FOR each bit ***s′***[i]

IF base **b′**[i] ≠ **b**[i]
eliminate bit ***s′***[i] from string ***s′***
ENDIF
ENDFOR
Sender :
FOR each bit **s**[i]
IF base **b**[i] ≠ **b′**[i]
eliminate bit **s**[i] from string **s**
ENDIF
ENDFOR

MODIFIED B92 ALGORITHM WITH QBTT METHOD

The Quantum Bit Travel Time – QBTT method can be implemented in B92 quantum key distribution scheme as an alternative method to detect the *Eavesdropper*. QBTT detection method allows the detection of the *Eavesdropper* during the quantum transmission, after each transmitted qbit from *Sender* to *Receiver*.

1.14. Steps of the B92 key distribution system with QBTT method

1. *Sender* generates a random binary sequence **s**.
2. *Sender* uses specialized equipment, including a light source and a set of polarisers, to create a sequence **p** of polarized photons - qbits whose polarization directions represent the bits in s accordingly to table 2.
3. *Sender* sends the qbits **p** to *Receiver* over an optical fiber. For each qbit from **p**, *Sender* sends to *Receiver* over the classical channel the timestamp of the moment of transmission.
4. For each qbit received, *Receiver* chooses randomly between rectilinearly "R" and diagonally "D". Let **b′** denote his choices of basis.
5. For each received qbit, *Receiver* calculates the delay time ΔT. If *Receiver* finds that the delay time ΔT, for a particular qbit, is much higher than usual that means *Eavesdropper* was present and he stops the communication.
6. *Receiver* measures each qbit with respect to the basis chosen in step 5 and communicates to *Sender* over the classical channel where he detects a '0'.
   If Receiver detects '0' then ***s′ = ?*** and the corresponding bit will be eliminated form ***s′***
   If Receiver detects '1' then ***s′ = 0*** if **b′ = *D*** or ***s′ = 1*** if **b′ = *R***
7. *Sender,* eliminate from **s** the corresponding bit where he received a '0' from *Receiver.*

1.15. Detecting Eavesdropper's presence

For each qbit received there is a time delay ΔT, between the moment of transmission and the moment of reception. If an *Eavesdropper* tries to tap the quantum channel that imply he have to read the qbits with a polarization filter and thus to induce a new time delay Δt. The final time delay for each tapped qbit will be $\Delta T' = \Delta T + \Delta t$. This allows *Sender* and *Receiver* to detect the *Eavesdropper's* presence, and to reschedule their communications accordingly.

1.16. Pseudo code of the modified B92 algorithm with QBTT method

Step 1
Sender:
generate string ***s*** randomly from (0,1)
FOR each bit from **s**
generate a photon
IF **s**[i] = 0 THEN *polarize* the photon in state (0^o) resulting qbit **p**[i] = →
IF **s**[i] = 1 THEN *polarize* the photon in state (45^o) resulting qbit **p**[i] = ↗
send qbit **p**[i] to ***Receiver***
generate timestamp *T*
send the timestamp *T*
ENDFOR
Receiver:
FOR each qbit **p′**[i] received
generate randomly from ("R", "D")
resulting base **b′**[i]
measure qbit **p′**[i] in respect to base **b′**[i]
resulting a value **v**
generate timestamp *T'*
calculate $\Delta T = T' - T$
IF ΔT is NOT in normal range
Eavesdropper *was present*
stop *transmission*
ENDIF
IF **v** = 0
s′[i] = ? *and the corresponding bit will be eliminated from* ***s′***
send value '0' to ***Sender***
ELSE // ***v*** *= 1*
IF **b′**[i] = D
THEN ***s′[i] = 0***
ELSE // ***b′****[i] = R*
THEN ***s′[i] = 1***
ENDIF
ENDIF
ENDFOR
Step 2
Sender:
FOR each value '0' received from ***Receiver***

eliminate the corresponding bit from ***s***
ENDFOR

CONCLUSION

This paper, proposes a new method to detect the *Eavesdropper's* presence, named Quantum Bit Travel Time – QBTT, by measuring the time between the moment of transmission and the moment of reception of every qbit. If an *Eavesdropper* is tapping the quantum channel, the delay time for that qbit will grow due to the polarization filter applied by him and thus *Receiver* will notice the difference and will stop the transmission.

The main advantage of this method is that the *Eavesdropper* can be detected instantly and precisely. Instantly – *Eavesdropper* can be detected during the quantum transmission. Precisely – *Eavesdropper* cannot be confused with noise errors because noises do not induce time delays.

QBTT detection method allows *Receiver* to detect the *Eavesdropper's* presence at any time during quantum transmission, after each received qbit, not only at the end of it. The classical detection method of BB84 algorithm and QBER detection method of B92 algorithm can detect the *Eavesdropper* at the end of quantum transmission after the communication over the classical channel of the polarization basis.

REFERENCES

Bell, J.S. (1964). On Einstein-Podolsky-Rosen paradox. *Physics 1*, pp. 195.

Bennett, C. H. and Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, pp. 175-179, Bangalore, India.

Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., and Smolin, J. (1992). Experimental quantum cryptography. *Journal of Cryptology*, vol. 5, pp. 3 – 28.

Bennett, C.H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, vol. 68, pag. 3121-3124.

id Quantique SA, *http://www.idquantique.com/products/network.htm*.

Li, X. and Chen, L. (2007). Quantum Authentication Protocol Using Bell State. *Proceedings the First International Symposium on Data, Privacy, and E-Commerce*, pp. 128-132.

MagiQ Technologies Inc., *http://www.magiqtech.com*.

Nielsen, M.A. and Chuang, I.L. (2000). Quantum Computation and Quantum Information, *Cambridge University Press*.

Shannon, C. (1949). Communication theory of secrecy systems, *Bell System Technical Journal*, vol. 28, pp. 656-715.

Treiber, A. (2009). A fully automated quantum cryptography system based on entanglement for optical fibre networks. *New Journal of Physics*, vol. 11.

Vernam, G.S. (1926). Cipher printing telegraph systems for secret wire and racho telegraphm communications. *Journal of the American Institute of Electrical Engineers*, pp. 109.

Waseda, A., Takagi, T., Soshi, M. and Miyaji, A. (2008). Quantum Secret Sharing between Multiparty and Multiparty against the Attack with Single Photons or EPR-pair. *Proc. of 2008 International Symposium on Information Theory and its Applications*, pp. 304-307, Auckland, New Zealand.