

A NOVEL ANALYSIS APPROACH OF QUANTUM TRANSMISSION ALGORITHM WITH BLIND DETECTION METHOD

SKANDER ARIS¹, ABDERRAOUF MESSAI¹, NADJIM MERABTINE²
MALEK BENSLAMA¹ AND AL-ANI KINAN¹

¹Electromagnetism and Telecommunication Laboratory
Faculty of Science Technology
University of Brothers Mentouri

Route Ain El bey, BP 25000, Constantine, Algeria
{ arisskander; r_messai; benslamamalek }@yahoo.fr; kinanaani@hotmail.com

²Department of Electrical Engineering
Faculty of Engineering
University of Taif

Airport Road, Al Hawiyah Area, P. O. Box 888, Taif, Saudi Arabia
na_merabtine@hotmail.com

Received June 2015; revised November 2015

ABSTRACT. *Based on Quantum Coding and Blind Detection Method a novel quantum algorithm strategy that can be used to encrypt secret keys is proposed. The security and the future implementation of this algorithm are analyzed in detail. It is shown that the algorithm can prevent quantum as well as classical attack strategy. There are numerous advantages in using the proposed algorithm, mostly important in satellite transmission networks. Our study presents a blind detection algorithm for linear mixtures of sources and matrix transmission methods, which can be applied to mobile MIMO systems as well. Moreover, it can be used for coding and decoding optical fiber transmissions. In addition, quantum communications offer many advantages for securing data transmission. An application of the implementation of our method is presented in this investigation addressing single secure optical communications based upon quantum cryptography BB84 protocol.*

Keywords: Quantum theory, Algorithm, Transform coding, BB84 protocol, Blind detection

1. Introduction. With the emerging high speed data technologies there is an incentive in innovating in the bandwidth usage savings from one hand and the need for a reliable detection of sources from the other hand, without spoiling part of the bandwidth for learning [1]. The latter is commonly known as blind source detection. Compared to this problem, we propose a new blind identification algorithm that is very simple, which makes it easier to build a more robust technique, especially addressing the new generation of transmission “quantum communication”. Quantum cryptography is of particular interest since the initial proposal of quantum key distribution in 1984 proposed by Bennett and Brassard [2] and its experimental demonstration in 1992 [3]. Current investigations of quantum cryptography are mainly concentrated on the following aspects: quantum key distribution [4], quantum secret sharing [5] and quantum cryptographic algorithm [6]. The goal of quantum protocol is consistent with more data protection carrying secret information or, in general, with keeping communication private in a large scale.

In quantum theory, the acts of measuring a quantum state can destroy this state (not only destroy it but also change it in the case of a spy for practical considerations). This is

a phenomenon that is difficult to correct and does not appear in the classical model (the act of taking a measure does not affect the measured object). In particular, in the theory of vector codes, it is quite common to measure the transmitted information to determine if there were errors and in this case, how to correct them. The fact that the measures are destructive to the quantum states makes the task of developing a quantum code very difficult to destroy with conventional correcting code.

From this point of view, in our paper we propose a novel and practical quantum cryptographic algorithm.

2. Source Detection. The mixing process between source and sensors is modeled by:

$$X(t) = A(S(t)) * B(t) \quad (1)$$

where, $X(t)$ is the observation vector measured by the receivers, A is the mixture operator, $S(t)$ is the unknown source vector signals that we seek to estimate, and $B(t)$ is the noise vector that models the measurement errors.

We can classify the problems of Blind Source Separation based on the nature of the operator A . If this operator is linear, we are then dealing with a formula with linear mixing. Equation (1) becomes:

$$X(t) = A(t) * S(t) + B(t) \quad (2)$$

$A(t)$ is a matrix of impulse responses of filters. $*$ is the continuous convolution operator.

If the measured signals are discrete in the time domain, which is necessary in the case of stored digital signals, the time variable (t) is replaced by a time index (n) and the integer continuous convolution operator is replaced by a discrete convolution. Equation (2) can be recast in the following form:

$$X(n) = A(n) * S(n) + B(n) \quad (3)$$

Among the linear mixtures, we can isolate two particular cases: The mixtures are instantaneous linear when the matrix of the filters impulse responses $A(n)$ is made of unit samples δ centered at 0. The matrix $A(n)$ is then written as:

$$A(n) = A\delta(n) \quad (4)$$

where A is a matrix. The convolution operator then becomes a simple matrix multiplication.

$$X(n) = AS(n) + B(n) \quad (5)$$

The mixtures are linear with respect to attenuation and delay when the function $A(n)$ is built from unity samples of different magnitudes and centered at different times, depending on the considered source-sensor [1].

3. Presentation of Algorithm. The detection is based on the principle of block diagram for an LR-aided detector [7] thus; our algorithm is to identify separately the rows of the mixing matrix. The response filter identifies the row containing useful information and thus generates the A matrix [8]. Our algorithm is based upon the following conditions.

The mixing matrix is a square matrix ' S '. The number of (columns) $l = i$.

(i) being the number of rows in the matrix

$$S = \begin{bmatrix} S_{11} & S_{12} & \cdot & \cdot & S_{1i} \\ S_{21} & S_{22} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ S_{i1} & \cdot & \cdot & \cdot & S_{ii} \end{bmatrix}$$

In the initial state, we must give the benefit of the matrix A_0 as the unit diagonal matrix of same rows and columns ‘ S ’, in the case of a determination and detection.

$$A_0 = \begin{bmatrix} 1 & 0 & 0 & \cdot & \cdot & 0 \\ 0 & 1 & 0 & \cdot & \cdot & 0 \\ 0 & 0 & 1 & \cdot & \cdot & 0 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & \cdot & \cdot & 1 \end{bmatrix}$$

Our algorithm is based on the response of the filter that changes the rows of the matrix A_0 up to the central row, with consideration that the strong points in the diagonal. Subsequently, the first change will be the matrix A_1 . It is important to point out that we must put in evidence that the algorithm works well as it should choose odd square matrix.

Continue with the process of mixing equation:

$$X_1 = A_1 S_0 \tag{6}$$

The second step is to reinjection of the X_1 matrix transposed obtained in the filter that will generate once again the matrix A_2 , and then recalculate the product to obtain X_2 :

$$X_2 = A_2 S_1 \quad \text{with: } (S_1 = X_1^T) \tag{7}$$

X_1^T is the transpose of X_1 matrix.

The process is reiterated and the loop is performed again. The source to be identified is centrifuged at the heart of the matrix X_3 (the $i + 1$ element of the $i + 1$ row) to provide more strength to our algorithm, we continue the calculations for X_5 and ensure that the result is identical to X_3, X_4 et X_5 .

4. Blind Detection Method Demonstration. For a simple proof, we present a simple example using a 3×3 matrix.

$$A_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$S_0 = \begin{bmatrix} A & B & C \\ D & E & F \\ G & H & I \end{bmatrix}$$

To show the robustness of our method we need to choose an element in the matrix that needs to be detected. In our example the symbol that we need to detect is denoted as C . The response filter gives the matrix A_1 as follows:


$$A_1 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

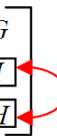
$$X_1 = A_1 \cdot S_0 = \begin{bmatrix} D & E & F \\ A & B & C \\ G & H & I \end{bmatrix}$$

The response of the filter on the transposed X_1 is:

$$X_1^T = \begin{bmatrix} D & A & G \\ E & B & H \\ F & C & I \end{bmatrix} = S_1$$

The matrix A_2 is:

$$A_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$$


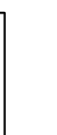
$$X_2 = A_2.S_1 = \begin{bmatrix} D & A & G \\ F & C & I \\ E & B & H \end{bmatrix}$$


The response of the filter on the transposed X_2 is:

$$X_2^T = \begin{bmatrix} D & F & E \\ A & C & B \\ G & I & H \end{bmatrix} = S_2$$

The matrix A_3 is:

$$A_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

$$X_3 = A_3.S_2 = \begin{bmatrix} D & F & E \\ A & C & B \\ G & I & H \end{bmatrix}$$


After the third step, the symbol C will always be the central element of the matrix and is the strongest in the diagonal as it is protected by other elements of Matrix. This technique has helped us give the couple of the algorithm proposed in quantum cryptography as a method of detecting or coding.

5. Quantum Cryptography Algorithm. Quantum cryptography for optical communications is to say the communications by conveying photons. It applies primarily to the distribution of encryption keys by optical fiber but also by the atmosphere. The general principle of quantum encryption is based on the quantum properties of photons identified by the Heisenberg uncertainty principle [9]. Indeed, according to this principle, any measure or observation of a quantum system disturbs immediately and permanently alter their condition. Thus, quantum communications guarantee total security since an intruder trying to intercept the transmission to irreparably disrupt the quantum state of the photon, which carries the information, which triggers an error message to the recipient of the message.

In order to perform quantum encryption, the sender will be associated with each bit of information a photon in a particular quantum state (polarization or frequency) and will send the string of photons (the message) to the recipient.

Any time the speed of quantum secure transmissions is still limited due to physical devices. At present, the speed is 1000bits. This speed is too low to allow the application of quantum encryption at all optical communications used at the moment. By cons, it is suitable for key distribution.

The properties outlined above, show that this distribution is totally secure since any intrusion permanently alters the encryption key. Thus, quantum encryption is generally used only for distribution of secret keys.

The protocol of quantum key distribution, developed in 1984 by Bennett and Brassard, allows two callers to exchange an encryption key [2]. Many experimental realizations using physical variables to discrete values, encoded on single photons, based on the use of this protocol [10]. Alice and Bob have a quantum transmission channel (optical fiber, free space) and a public channel (radio, Internet) [11]. The BB84 requires four states of coding in such a way to form two conjugate bases as shown in Figure 1. Each state is encoded by a linear polarization. BB84 protocol is non-deterministic. This means that it distributes a random sequence of bits. BB84 cannot be used for the transmission of a selected message. Communication between Alice and Bob is simply being successful based on the randomness of each step of the protocol.

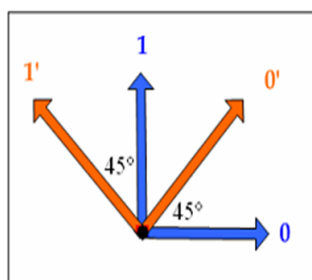


FIGURE 1. The coding polarization scheme of BB84 protocol

The coding scheme BB84 quantum protocol is the first proposal for encoding, or the receiver (legitimate or illegitimate) cannot recover with 100% reliability. It provides a basis for most other quantum. According to this protocol, the bit is encoded by classical quantum states, or qubits. Each state can represent the two classical bits, 1 and 0, and conversely, each 0 or 1 corresponds to an equal mixture of two quantum states that may not be orthogonal [2]. An illustration of the four states $|0\rangle$, $|1\rangle$, $|1'\rangle$, $|0'\rangle$ is given in the preceding figure. The information provided in the quantum channel is often in the form of polarized photons. The encoding of classical bits is done by using the direction of polarization. In the BB84 coding scheme the classical bit 0 is represented by a photon polarized at 0 and 45 degrees from the horizontal axis, and the two orthogonal directions corresponding, 90 and 135 degrees, are used for a bit 1 (see Figure 1).

6. Quantum Key Distribution. A solution to ensure the confidentiality of information passing through an optical fiber is to hide (encrypt) the information before transmitting. The information security is achieved by blurring the original message with a signal that looks like a noise, the key. To decrypt the message that is then to use the same key [12].

If the use of secret keys to encrypt data transmitted is a widely used method, it requires the distribution between the corresponding secret keys used for encryption of information.

The quantum key distribution (quantum cryptography) ensures absolute confidentiality of the transmitted key because the level of confidentiality is guaranteed by a physical principle. The principle of transmission of the encryption key is to reduce the light to its lowest level, the photon [13]. In digital communications, the key consists of a random sequence of 1s and 0s. To represent these different values, we use two particular states of the photon. The states are chosen so that they are not fully discernible. Thus, there is no means by which to measure, duplicate perfectly and simultaneously these two states. An incorrect action may bring a change in the rate of errors. Using this physical property

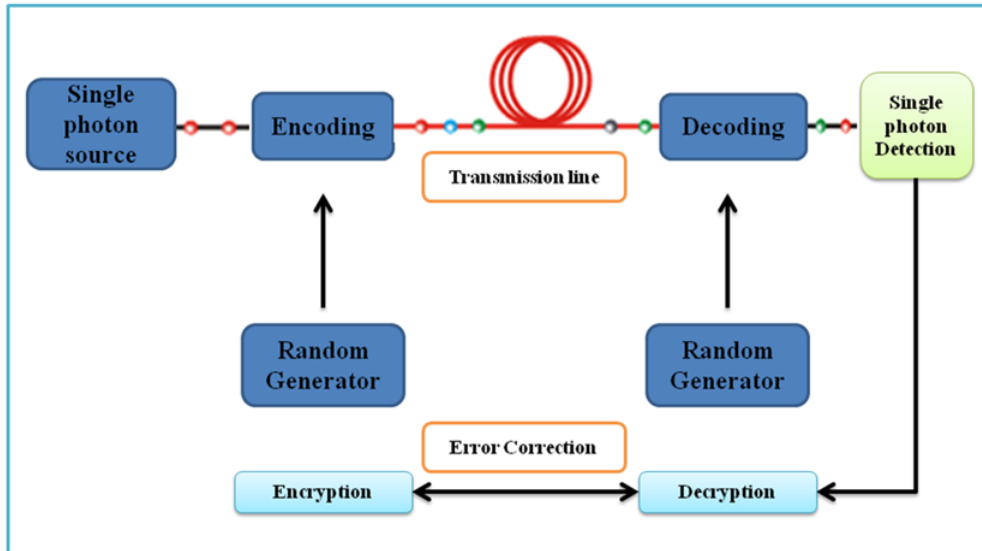


FIGURE 2. Quantum key distribution architecture

and an appropriate protocol, it is possible to ensure that some of the photons received by the corresponding self have not been heard. The encryption key used to mask the information will be made only of these photons [14]. The transmission and the reception between Alice and Bob is single photon (see Figure 2).

7. BB84 Protocol Decomposition. This protocol consists of:

A. Alice randomly chooses one of two symbols (0 or 1) and one of two bases (+ Vertical base or \times Horizontal base). She codes choices on the polarization of a photon and sends it to Bob via a quantum channel.

B. Bob randomly chooses a base (+ or \times) to perform its measurement. To establish a good transmission in BB84 protocol, the proposed idea is produced several times to Alice and Bob having a first series of bits. Bits of Bob being the result of a measurement performed in a randomly selected basis are not identical to those of Alice. Therefore, the series features Bob in principle 25% of errors resulting from anti coincidence bases.

C. On a public channel, Bob reveals to Alice his choice of basis for each photon received. If their choices of bases coincide, Bob deduced from his position the bit transmitted by Alice. Otherwise, Alice and Bob discard the corresponding bit. At the end of this stage of reconciliation, Alice and Bob share an identical set of bits constituting the key encryption key called refined (sifted key). Before, the series has a bit of Bob average error rate of 25% compared to that of Alice. The reconciliation can in principle reduce the error rate to 0.

In return, the size of the common set is halved compared to the series issued by Alice.

8. Practical Order Consideration of BB84. During the creation of the quantum system, practical order considerations complicate the development of BB84 protocol [13]:

- **The luminous impulses** containing exactly one photon are technically difficult to produce,

- **The photo detectors** are not 100% efficient and they can be disrupted by the noise,

- **During the reception:** it is necessary to consider the fundamental problem that creates incoherence bits between Alice and Bob: the choice of bases (H/V or Diagonal $+45^\circ$, -45°) that relies on the Heisenberg uncertainty principal,

- **The spying:** the protocol requires from Alice and Bob to eliminate their data as soon as they identify an error (restart the BB84 protocol from the beginning).

9. **Quantum Blind Detection Code.** The performance of a QKD system depends on the established protocol; we choose the protocol or the most appropriate algorithm according to our application, based on the compromise between distance and maximum communication rate. Such a quantum algorithm is shown in the following figure.

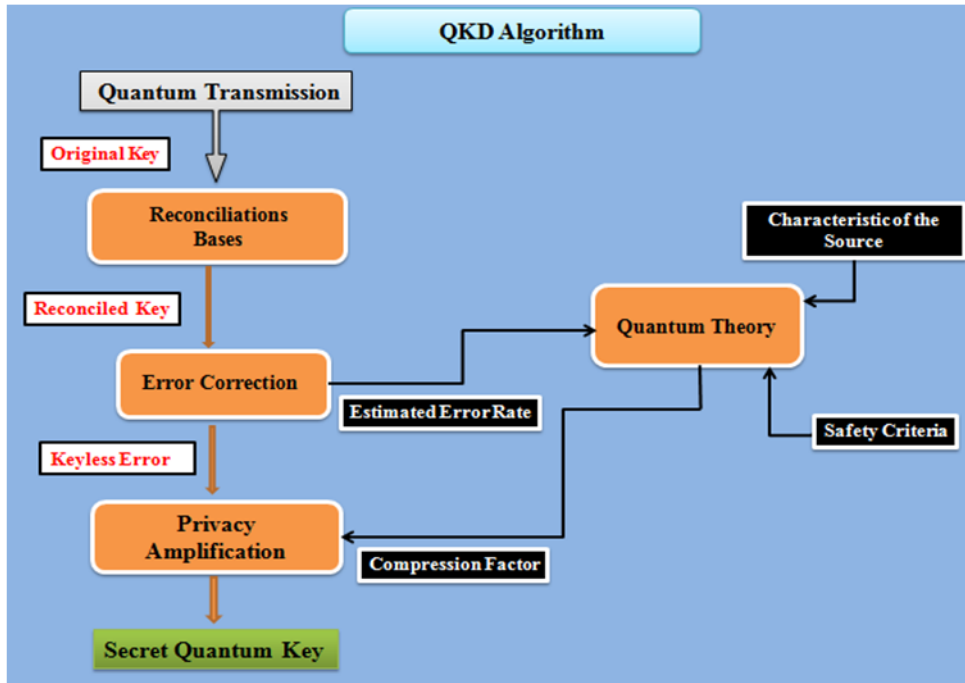


FIGURE 3. Quantum key distribution algorithm

The protocol requires from Alice and Bob to eliminate their data when they identify an error therefore they will never succeed to exchange a secret key following this protocol [15]. In order to solve this problem, we must make an additional stage to the protocol, a stage which allows Alice and Bob to send the key with more security. For this purpose, Alice and Bob would use the protocol with a novel approach method instead of eliminating their data when they identify errors. In order to have a total secured emission, we introduce in this coding part some changes on the key, before making the base choices by Alice and therefore before the photon emission by the quantum channel (see Figure 4).

- The mixing matrix S containing the qubit of the key must be transmitted from Alice to Bob.

$$S = \begin{bmatrix} S_{11} & S_{12} & \cdot & \cdot & S_{1i} \\ S_{21} & S_{22} & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ S_{i1} & \cdot & \cdot & \cdot & S_{ii} \end{bmatrix}$$

In the algorithm our objective is to find the symbol C , but by applying the BB84 protocol using the proposed detection method is to replace every faith in the C key qubit sent. Following the procedure of our work the key distribution is to transmit the final matrix to the receptor with a qubit centered in the diagonal which will be well protected:

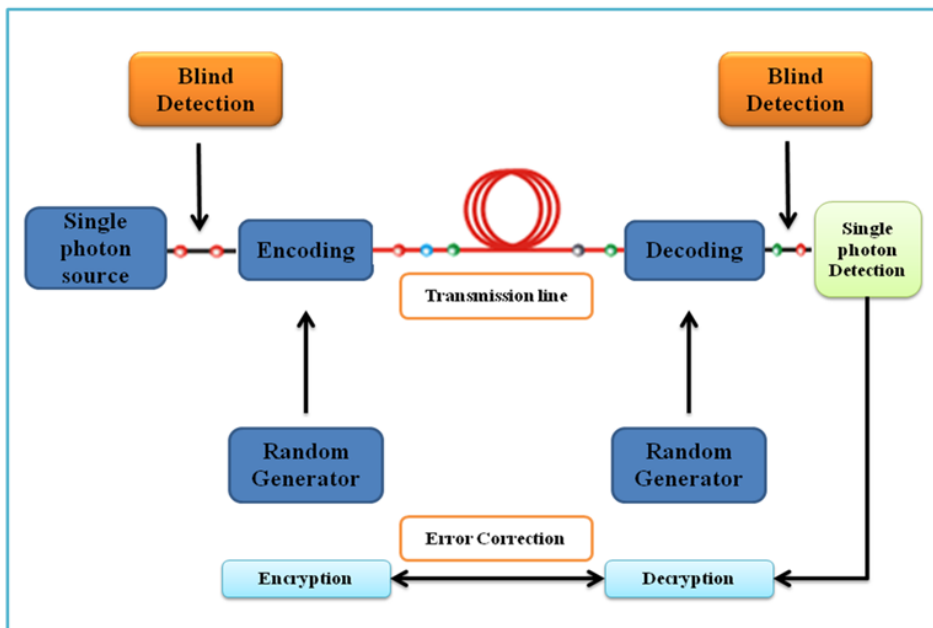
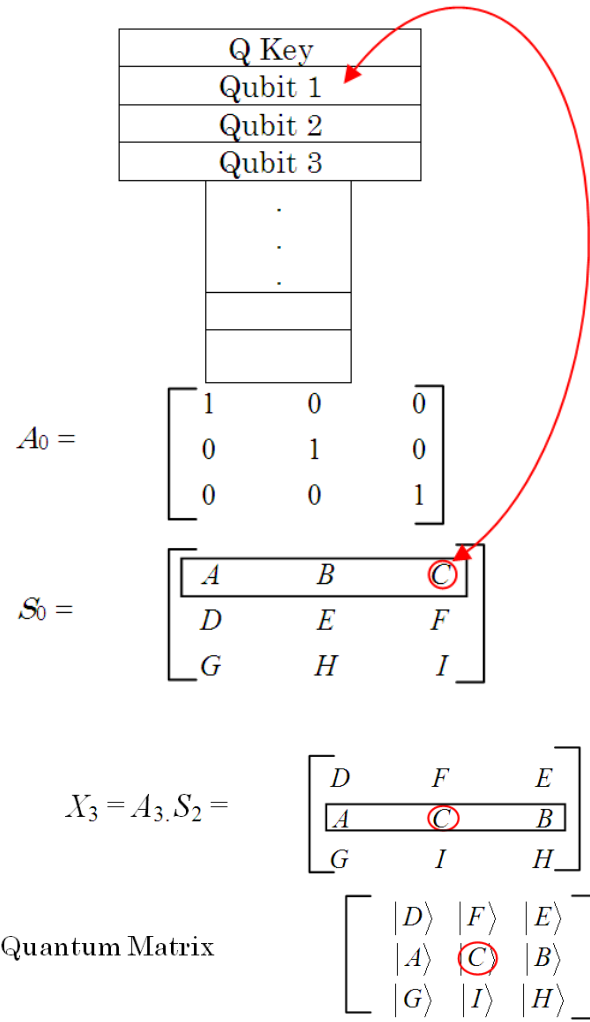


FIGURE 4. Quantum blind detection implementation

The final result Matrix is then transmitted by the quantum channel. This emitted matrix message does not contain any information unless for Bob because nobody except himself knows this method. Our objectives are summarized as follows:

- * A high security key: by creation of the masking and coding stages in the beginning of transmission between Alice and Bob (see Figure 5).
- * With this method instead of sending directly the key, Alice sends the masking and the coding of key in order not to be detected by Evesdropping.
- * Let us suppose that Eve discovers the secret key that Alice and Bob will try to exchange, with this method she will not be able to decipher it.
- * Let us now suppose that Eve looks for discovering the key, Bob may easily detect it and he can even inform Alice during the correction that there had been spying during the secret key transmission.

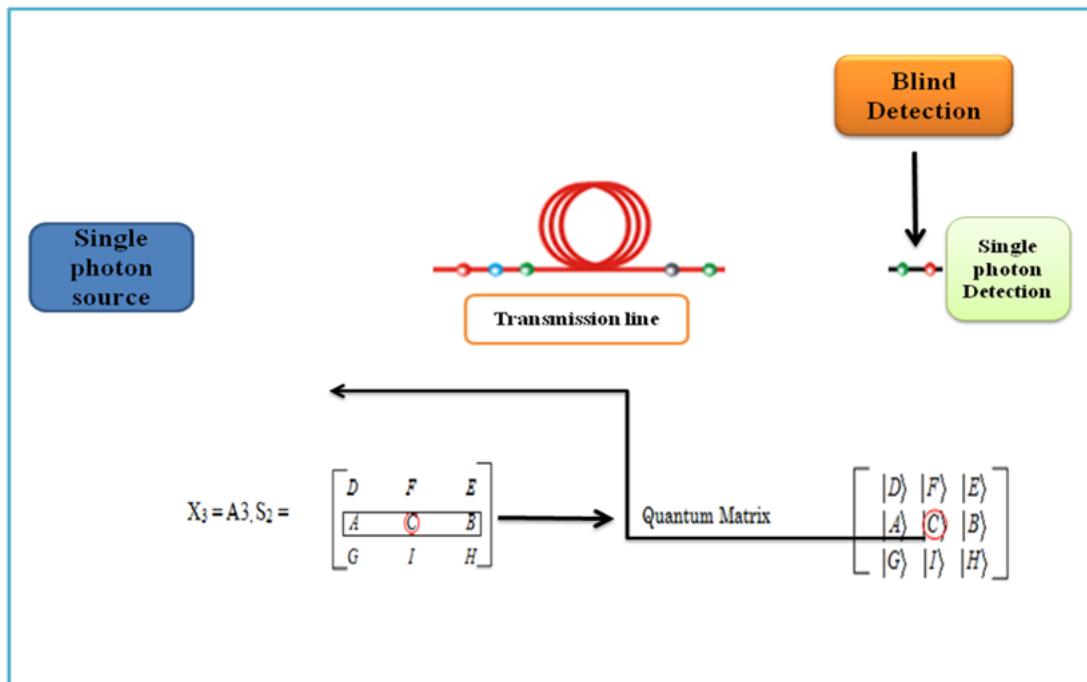


FIGURE 5. Quantum blind detection algorithm structure

10. Practical Consideration. The main problem discussed in this article is the elimination of key raw data when the presence of an adversary is identified in a protocol distribution quantum key. This problem has been addressed by using a method of mixing the source signals quantum cryptography protocol.

Based on the description of the mixing process in the article a number of questions arise. First, as described in the protocol, all qubits next to Alice gathered in the quantum S matrix, which is then sent to Bob. Here, the first problem occurs because in QKD protocols qubits are sent to Bob immediately after their creation. In the event that they must be stored and mixed quantum memory must be used [16]. This fact is not clearly described in the proposed algorithm. Secondly, the creation of matrices A_0 to A_3 is based on the position of the element to be sent in the matrix S . It must be clearly defined to Bob to cancel the mixing procedure since this procedure is performed next, Alice and Bob do not know which item is being sent. However, the fact that the essential element is attracted towards the center of the matrix, Bob must know the beginning of the number of elements of the square matrix. In this case because the opponent (spy) has

been the method of transmission, the number of rows and columns of the matrices is not known. Thirdly, that Alice and Bob work with the same measurement bases replacement (polarization 45 and 135 degrees). If Alice and Bob use different bases implications for the mixing procedure and measurement alongside Bob is not valid.

11. Simulation and Results. Evaluation of quantum bit error rate can be used with a choice to continue or not quantum key distribution. Comparing the number of Qubits must be sufficiently large that the error rate is representative in transmission to effect that error correction adapted. Moreover, the choice of random bits to be compared provides a high quality of service in the quantum transmission. There are many error correcting codes to obtain an identical key between Alice and Bob. Some are relatively simple to implement, but very effective. All measure the exact value of the error rate of the original key without having to fully disclose. However, this key can be used in the state since Eve knows one thing. Then Alice and Bob evaluate the amount of information received by Eve in order to assess the reliability of the protocol exchanged between them. Indeed, Alice and Bob can establish a secret key if [17]:

$$\begin{aligned} I_{Alice \rightarrow Bob} &\geq I_{Alice \rightarrow Eve} \\ I_{Alice \rightarrow Bob} &\geq I_{Bob \rightarrow Eve} \end{aligned} \quad (8)$$

$I_{Alice \rightarrow Bob}$ represents the mutual information within the meaning of Shannon between Alice and Bob. Alice and Bob are able to establish a secret key when either Alice or Bob has more information on the other Eve. Interception-emission strategy is probably the most intuitive. Eve placed between Alice and Bob, with a probability ω intercepting the photon emitted by Alice's measurement condition and then returning towards Bob a photon prepared in the state depending on the result of the measurement. Instead of photons not intercepted (complementary probability $1 - \omega$), Eve randomly chooses the symbol as its key. Eve's intervention is then repeated for each photon [18]. By putting (a, b, e) states, respectively, Alice, Bob and Eve, the mutual information between Alice and Bob is expressed:

$$I_{Alice \rightarrow Bob}(A, B) = \sum_{j=1} \sum_{i=1} p(a, b) \cdot \log_2 \cdot \left(\frac{p(a, b)}{p(a) \cdot p(b)} \right) \quad (9)$$

And the mutual information between Alice and Eve is written:

$$I_{Alice \rightarrow Eve}(A, E) = \sum_{j=1} \sum_{i=1} p(a, e) \cdot \log_2 \cdot \left(\frac{p(a, e)}{p(a) \cdot p(e)} \right) \quad (10)$$

To evaluate the mutual information, it is necessary to calculate the probability of detecting a symbol knowing the transmitted symbol.

In our study the execution of the BB84 protocol with blind detection of experimental imperfections introduces errors between the two keys, and the error rate is then noted QBER (Quantum Bit Error Rate). This average is the asymptotic limit the number of errors compared to the number of bits transmitted during a transmission; it is calculating the QBER arriving in the different simulations below.

$$I_{Alice \rightarrow Eve} = \frac{1}{2} \log_2 \left(1 - \frac{\omega^2}{2} \right) + \frac{\omega^2}{2} \log_2 \left(\frac{2 + \omega^2}{2 - \omega} \right) \quad (11)$$

$$I_{Alice \rightarrow Bob} = \frac{1}{2} \log_2 \left(2 - \frac{\omega}{2} \right) + \frac{\omega}{2} \log_2 \left(\frac{2}{\omega} - 1 \right) \quad (12)$$

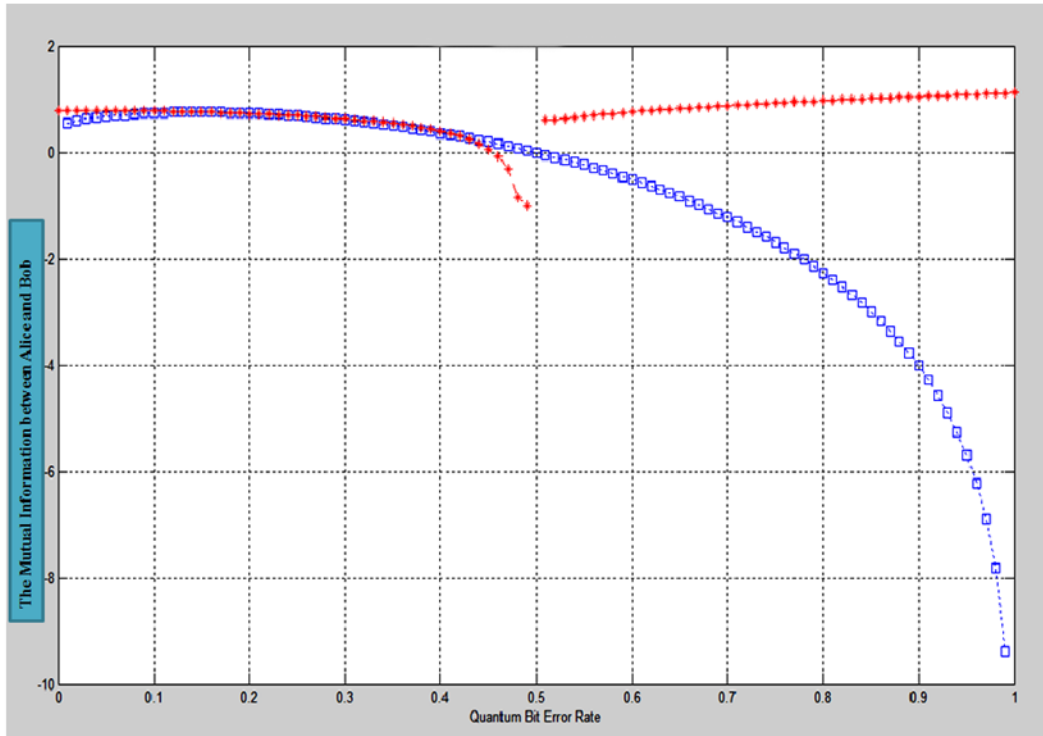


FIGURE 6. Mutual information between Alice, Bob in attack interception-emission

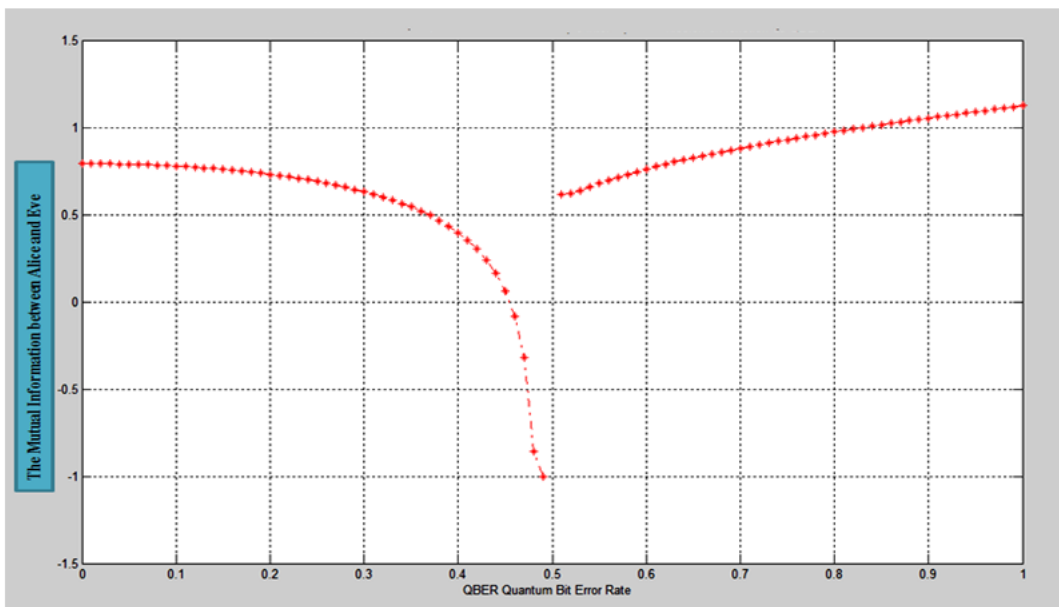


FIGURE 7. Mutual information between Alice, Eve in attack interception-emission

In these figures, we see that the mutual information between the legitimate users (Alice and Bob) begins to decrease when the QBER reaches 0.05, and that between Alice and Eve, we see that the increases, as the mutual information QBER, exceeds the value 0.5.

From these simulation results, it can be noted that transmission in the presence of a spy attack using emission-Interception becomes bad if the QBER higher than 0.05 after this value the information exchanged between user-spy is greater to that exchanged between users.

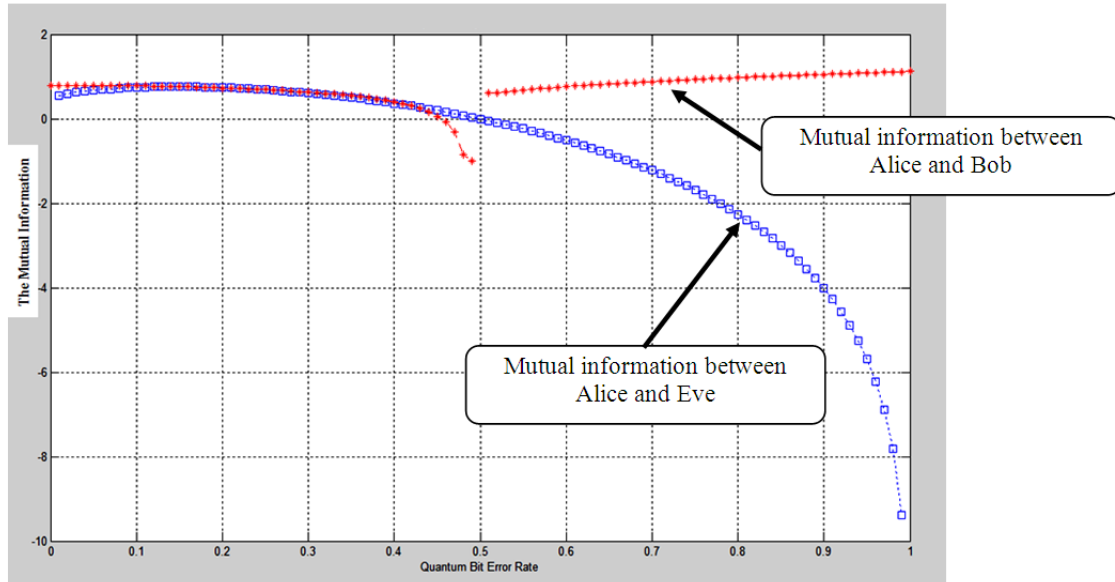


FIGURE 8. Mutual information between Alice, Bob and Eve in attack interception-emission

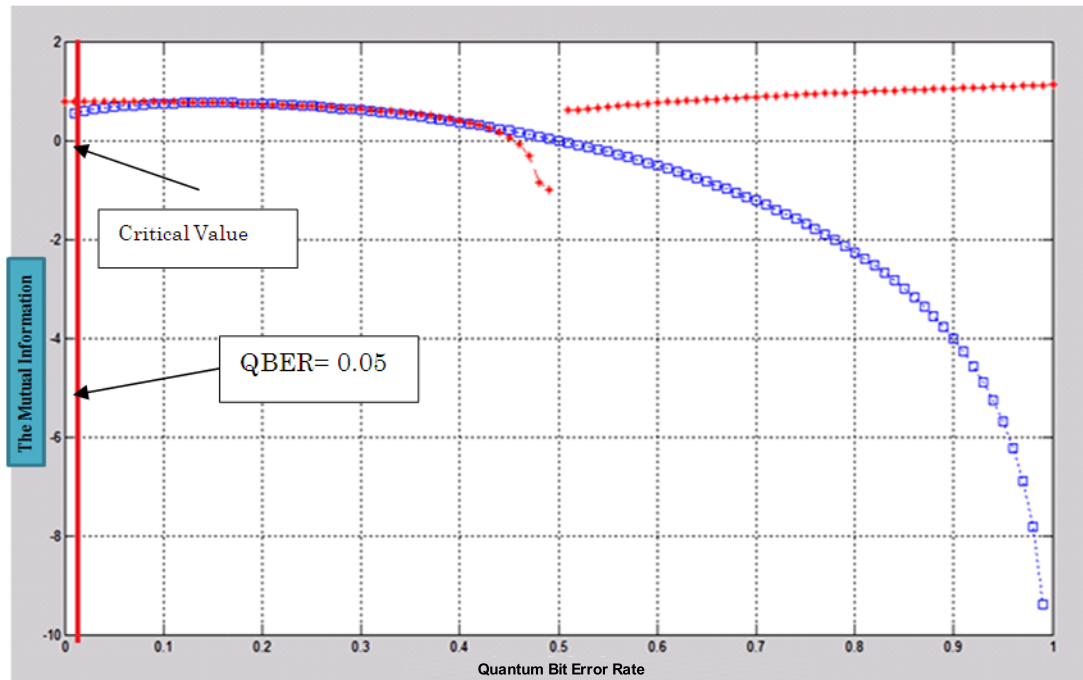


FIGURE 9. Practical limitations in attack interception-emission

It implies in our case practice a critical value that the user of the BB84 protocol with blind detection is generally well located in a perfect case compared with the work of [19-21] or QBER is less than 0.1.

12. Quantum Blind Satellite Transmission Idea. The use of satellites for the quantum distribution is our objective; the transmission of photons can be considered as a unique solution for long distance [21]. This principle has overcome the limitations of Earth-related technology [22,23], namely, the range of about 100 km made possible by

optical fibers. Quantum Blind detection scenarios involving an issuer based on Earth allows sharing quantum transmission is between the ground and the satellite, or between two ground stations, or between two satellites and thus communicate with terminals using such quantum communication protocols. In the simplest case, a direct uplink to a satellite receiver can be used to perform quantum key distribution (QKD) between the transmitter and the receiver station. Our implementation principle of blind detection is to provide a method of coding for a reliable and secure communication.

13. Conclusions. Our study expressed that Alice and Bob are the people who want to share a secret message, and Eve the eavesdropper. When Eve tries to intercept the quantum signals sent by Alice, it must necessarily be measured, which disrupts the link.

This disturbance is one of the practical and theoretical limits that can impair information between Alice and Bob. The principles of quantum cryptography are well known by Bennett and Brassard who proposed a protocol, called BB84, based on the coding of the single photon polarization. However, they proved security under realistic conditions; there has been a lot of research that requires the application of information theory to physical systems. For example, security proofs exist for the BB84 protocol taking into account various experimental imperfections (presence pulse unstable transmission of a finite impulse noise detector...).

In addition, the implementation of this investigation will improve the theoretical aspects of quantum cryptography in conjunction with a method of error detection and correction code "The blind detection". As such, it can lead to a theoretical thesis. It is not manipulation, but the proposal of a new method as an application in quantum cryptography and network security at world wide scale level. We have made a contribution for securing quantum information using error code correction approach in quantum detection [22-24].

To evaluate a quantum system, it is necessary to calculate the probability of detection of a qubit knowing the total number of transmitted qubits. In the general case calculate the error rate QBER (Quantum Bit Error Rate). This average is the asymptotic limit of this method during a transmission with or without sound. According to the theory of Heisenberg uncertainty (in the noisy environment), if a spy chooses an incorrect base (encoded by a known method) to measure the state of a photon, it will change the state of the photon, that is to say, it may cause errors. For example in the BB84 protocol, we do not distinguish between errors created by the noises with those created by espionage. Therefore, we consider that all errors are created by a spy.

From these results of mutual information computations, we demonstrated that the transmission in the presence of such a spy attack becomes poor if the QBER exceeds 0.05 after this value the information exchanged between the user-spy is higher than that exchanged between users so our algorithm is well placed in the quantum structure as the critical value of QBER is less than 3% practical.

Several experiments have shown the viability of the conduction of free space quantum cryptography at the surface of the Earth; we propose in this survey a new idea for coding error correction in order not to safeguard the information, and to secure the information during the communications between the users. As perspective work we foresee the elaboration of an algorithm capable of detecting and correcting errors in quantum cryptography.

REFERENCES

- [1] H. Cirpan and M. Tsatsanis, Blind receiver for non linearly modulated signals in multipath, *Proc. of SPAWC*, pp.149-152, 1997.

- [2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, *Proc. of IEEE International Conference on Computer System and Signal Processing*, Bangalore, India, pp.175-179, 1984.
- [3] C. H. Bennet et al., Experimental quantum cryptography, *Journal of Cryptology*, vol.5, no.1, pp.3-28, 1992.
- [4] L. Ma, M. Alan and T. Xiao, High speed quantum key distribution over optical fiber network system, *J. Res. Natl. Inst. Stand. Technol.*, vol.114, pp.149-177, 2009.
- [5] I. Peterson, Bits of uncertainty: Quantum security, *Science News*, vol.137, no.2, pp.342-343, 1990.
- [6] E. Biham and T. Mor, Bounds on information and the security of quantum cryptography, *Physical Review Letters*, vol.79, pp.4034-4037, 1997.
- [7] D. Wubben, V. Kuhn and K.-D. Kammeyer, On the robustness of lattice-reduction aided detectors in correlated MIMO systems, *IEEE the 60th Vehicular Technology Conference*, vol.5, pp.3639-3643, 2004.
- [8] N.-D. Sidiropoulos and G.-Z. Dimic, Blind multiuser detection in W-CDMA systems with large delay spread, *Proc. of IEEE Signal Processing Letters*, vol.8, no.3, pp.87-89, 2001.
- [9] S. Aris, M. Planat and M. Benslama, The quantum cryptography – Solution to the problem due to the principle of uncertainty of Heisenberg, *WSEAS Trans. Communications*, vol.5, no.5, pp.948-955, 2005.
- [10] S. Aris, N. Merabtine and M. Benslama, A new information theory in quantum security systems: BB84 protocol, *Georgian Electronic Scientific Journal: Computer Science and Telecommunications*, vol.4, no.11, 2006.
- [11] D. Miloslav, H. Ondrej and H. Martin, Generalized beam-splitting attack in quantum cryptography with dim coherent states, *Optics Communications*, vol.169, pp.103-108, 1999.
- [12] S. Aris, N. Merabtine and M. Benslama, A necessary of Xor linear code with generator matrix in quantum communications protocols, *Proc. of NATO Advanced Research Workshop Metamaterials for Secure Information and Communication Technologies*, Marrakesh, Morocco, 2008.
- [13] N.-A. Muhammad and Z.-A. Zukarnain, Implementation of BB84 quantum key distribution protocol's with attacks, *European Journal of Scientific Research*, vol.32, no.4, pp.460-466, 2009.
- [14] P.-W. Shor, Quantum error-correcting codes need not completely reveal the error syndrome, *ArXive e-print quant-ph/9604006*, 1996.
- [15] G. Ribordy, J.-D. Gautier, N. Gisin, O. Guinnard and H. Zbinden, Automated 'plug and play' quantum key distribution, *Electronics Letters*, vol.34, no.22, pp.2116-2117, 1998.
- [16] C. Simon et al., Quantum repeaters with photon pair sources and multimode memories, *Phys. Rev. Lett.*, 2007.
- [17] G. Brassard, N. Lütkenhaus, T. Mor and B.-C. Sanders, Limitations on practical quantum cryptography, *Phys. Rev. Lett.*, vol.85, pp.1330-1333, 2000.
- [18] N. Gisin et al., Quantum cryptography, *Reviews of Modern Physics*, vol.74, no.1, pp.145-195, 2002.
- [19] P. Kumar and A. Prabhakar, Bit error rates in a frequency coded quantum key distribution system, *Optics Communications*, vol.282, pp.3827-3833, 2009.
- [20] B.-C. Jacobs, T.-B. Pittman and J.-D. Franson, Quantum relays and noise suppression using linear optics, *Phys. Rev. A*, 2002.
- [21] E. Waks, A Zeevi and Y. Yamamoto, Security of quantum key distribution with entangled photons against individual attacks, *Phys. Rev. A*, 2002.
- [22] C.-Z. Peng, T. Yang, X.-H. Bao et al., Experimental free-space distribution of entangled photon pairs over 13 km: Towards satellite-based global quantum communication, *Phys. Rev. Lett.*, 2005.
- [23] S. Aris, A. Messai, M. Benslama, N. Merabtine and M.-M. Elharti, Integration of quantum cryptography through satellite networks transmission, *American Journal of Applied Sciences*, vol.8, no.1, pp.71-76, 2011.
- [24] S. Aris, A. Messai, M. Benslama, N. Merabtine and M. M. Elharti, A novel idea of quantum cryptography coupled with handover satellite constellation for world cover communications, *Proc. of PIERS*, Marrakesh, Morocco, pp.1754-1759, 2011.