A New Information Theory in Quantum Security Systems: Bb84 Protocol

Aris Skander, Merabtine Nadjim, Benslama Malek
Electromagnetism and Telecommunication Laboratory, Department of Electronics, Faculty of Engineering. Constantine University, 25000 Algeria.
merabtinenadjim@yahoo.fr arisskander@yahoo.fr malekbenslama@hotmail.com

Abstract

All the data that flows through optical fibres such as electronics trade, bank transaction, electronics messages etc…..…are concerned by this promising technique of the quantum cryptography or the distribution of secret keys and this because it secures the communications making them inviolable.

Why does the quantum cryptography allow a secret keys exchange? Thanks to the laws of the quantum physics which usually impose restrictions to the classic physics and permits to offer an absolute protection to the information. In spit of the considerable progress in the quantum encryption (encoding) many questions remain asked and many problems cannot be solved using the present techniques.

In order that the quantum cryptology becomes an efficient method with application to large scales, we must introduce techniques for real applications to coding and encoding.

This precise point is the aim of our work; we will try knowing the practical limits for the quantum cryptography thus coupling them with techniques borrowed from signal processing with purely quantum theories in order to elaborate correction error methods in quantum cryptography.

Keywords: *Quantum cryptography, security, encryption, quantum error correction.*

1. Introduction

The quantum cryptography is structured on the distribution protocol of secret keys: the BB84. Many experimental successes exist, but we still face several problems that the present techniques are not able to solve.

We will be particularly interested by the problem that consists in the risk to introduce incoherence in Alice and Bob's data.

Alice being the source and Bob the addressee, they are connected by a channel which on one hand will propagate the information and on the other hand will be the source of disruptive phenomena. These disruptions that alter the transmitted message are the main channel property.

It may seem strange that we attack such importance to these phenomena even though they are rarely perceived. But we should not forget that the reception of the message sent by the source results from a physical measure whose precision is limited. These disruptions will restrict the possibilities of communications.

2. The quantum encryption

In the quantum key transmission [1], the information is transmitted by the photons (elementary constituents of the light). Each photon can be polarized, that means that we impose a direction to its electric field.

The polarization is measured by en angel that varies form 0° to 180°. In the protocol that we describe, due to the Canadian **Bennett and Brassard 1984** (BB84) [2], the polarization can take 4 values: 0°, 45°, 90°, and 135°. There is a rectilinear polarization for 0° and 90° polarized photons and a diagonal polarization for the45° and 135° polarization (figure1).

Fig.1. The photons polarisation

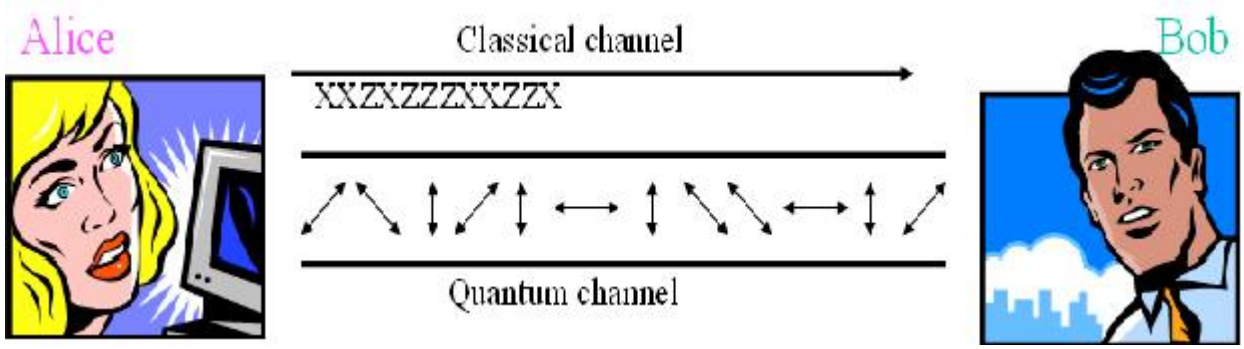
2.1. The quantum channel

It is an optical fibre; an optical fibre is a wire made of glass allowing the photons transmission, i.e. light particles.

2.2. The classic channel

It generally is an internet network which permits to precede verification to transmit the message once encrypted (figure2).

Fig.2. The quantum system



3. The practical limits of the quantum encryption

The spying: In order to obtain information on the secret key that Alice and Bob attempt to exchange [3], Eve should intercept the photon transmitted by Alice, them for each intercepted photon measure its polarization according to one of the two bases: rectilinear or diagonal, and finally transmit to Bob a new polarized photon for each intercepted photon. This attack is practically impossible to realize successfully, no matter the computational power of Eve (figure3).

Fig.3. The spying

In fact for each intercepted photon, like Bob, Eve must decide to measure its polarization according to one of the two bases: rectilinear or diagonal and again like Bob, Eve ignores the bases chosen by Alice.
Because of Heisenberg uncertainty principal and the fact that the tow bases form a pair of complementary properties [4], any spy attempting this takes the risk to introduce incoherence in Alice and Bob's data.
If there had been a spying, Alice and Bob should restart the protocol BB84 from the beginning.

4. Practical order considerations

During the creation of the quantum system [5], certain practical order considerations complicate the development of BB84 protocol:

4.1. The luminous impulses containing exactly one photon are technically difficult to produce.

4.2. The photo detectors are not 100% a hundred percent efficient and they can be disrupted by the noise.

4.3. 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°, -45°) that relies on the Heisenberg uncertainty principal.

4.4. 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).

5. The methods for error correction in quantum cryptography

5.1. In order to create luminous impulses containing exactly one photon, we produce very weak intensity luminous impulses which are easy to obtain while using **lasers.**
5.2. Even if there is no spying on the quantum channels the problem of the imprecision leads necessarily to incoherence in Bob's data. To solve this problem, we have chosen a photo detector that is compatible with optical fibre telecommunications (quantum channels).
5.3. 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 [6]. In order to solve this problem (restart), we must add an additional stage to the protocol, a stage which allows Alice and Bob to correct their errors with some conditions. For this purpose, Alice and Bob would use the protocol with an error correction method instead of eliminating their data when they identify errors.
Elaboration of a method for: the quantum error correction between Alice and Bob.

6. The protection method in BB84

Coding Part: (1)

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.

The key emitted by Alice is:

1101001110010111……..

2^n

Example

~~$2^n = 32$~~ → **n =5.**

Part 1-1:

11/01/00/11/10/01/01/11/…….. We cut the key by pairs of bits and we find 16 pairs.

Part 1-2

We carry out the XOR sum for the bits existing in the pairs of the key to find an **origin Bit**: (0), (1), (0) ……..

Part 1-3

We call on a **parity bit**: how many 1 bits are there in the pair?

- If the number is even → 0.
- If the number is odd → 1.

A new key that is a set of 00 and 11 with a masking technique at the some time, then we risk the least error detection to Bob's message reception: (00), (11), (00)…

Part 1-4

There is a problem that intervenes in this part and that is how to know whether the XOR = 1, if the bits (01) or (10) and whether the XOR =0 the bits (00) or (11), thus additional bits are necessary, they are the **XOR Bits:**

XOR =0:

00 → (0 for the bits 00, 0 for the XOR) 00

11 → (1 for the bits11, 0 for the XOR) 10

XOR =1:

01 → (0 for 01, 1 for XOR) 01

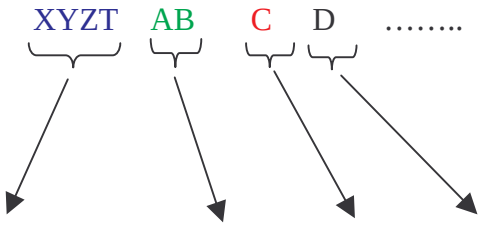
10 → (1 for 10, 1 for XOR) 11

The Key: 1000/ 0111/ 0000 ……...

Part 1-5

The pair's numbers, if the number of the bits (2^n =32) then the pair's numbers are coded by n/2 bits = in our example 4, for instance the first pair 0001(1000) of continuations 0010(0111), 0011(0000) …….

The emission part:



The pairs numbers XOR Bits parity bits origin Bits

Observation

1 / the XOR Bits: to include it in the key to control at the reception either the 1 bit or the 0 bits.
2 / the Parity bits: to know the numbers of 1 bit at the reception.
3 / the origin Bits: in this case the key with the XOR masking is more secured.
4 / the origin and the Parity bits: 00 and 11 pairs to increase errors detection in the key at the reception.
5 / the pairs numbers: it just a masking method.
6 / the origin, Parity and the XOR bits:
When we call on all combinations that may appear while applying this method:

00 ⟶ **1000**
11 ⟶ **0000**
01 ⟶ **0111**
10 ⟶ **1111**

The first three bits have always the some which speeds up the errors detection.
The new key before the bases choices by Alice:
00011000 00100111 00110000……

Reception and Correction part (2)

The result is then transmitted by the quantum channel, this emitted message does not contain any information unless for Bob because nobody except him knows this method.

7. The advantages and disadvantages of the method

7.1. The advantages

A high security key: by creation of the masking and coding stages in the beginning of transmission between Alice and Bob.
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 Eve.
Let's 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.

7.2. The disadvantages

The key initially 2n bits, but with the application of this method it rises up to 2^p bits:
$2^n \leq 2^p$
The key will likely lose a certain number of bits in the quantum channel; even with the detection end error correction there is enough time to waste to get to the proper key.

8. Conclusion

The BB84 protocol requires from Alice and Bob to eliminate their data as soon as they identify an error (restart from beginning), so they will never succeed to exchange a secret key following this protocol.
Therefore, Alice and Bob should use the protocol with this method for the error correction with the some conditions.

References

1. C. Bennet, et al, *La cryptographie quantique. Pour la Science hors série*, 2002, n° 36, pp. 114-117.
2. Bennett H Charles, F. Bessette, G. Brassard, L. Salvai, J. Smolin, Experimental quantum cryptography, Journal of Cryptology Volume 5, Number 1, pp-3-28 January 1992. Springer New York.
3. M. Planat, S. Aris, N. Merabtine, M. Benslama: Complementary and Quantum security. IEEE, ISESC'05 19-21 June 2005 Jijel Algeria.
4. S. Aris, M. Planat, M. Benslama: The quantum cryptography: *Solution to the problem due to the principle of uncertainty of Heisenberg*, WSEAS TRANSACTIONS on COMMUNICATIONS issue5, Volume5, May 2006.
5. M. Boyer, R. Geles, "Security of BB84 against collective attacks" Inprreparation, pp 13-20, edition 2006.
6. C.H. Bennet, G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing, in: Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore," India, IEEE, New York, 175–179 (1984).

Article received: 2006-07-30