American Journal of Applied Sciences 4 (8): 597-604, 2007
ISSN 1546-9239
© 2007 Science Publications

A New Error Correction Intuitive Approach in Quantum Communications Protocols

Aris Skander, Merabtine Nadjim and Malek Benslama
Electromagnetism and Telecommunication Laboratory, Department of Electronics
Faculty of Engineering, Constantine University, 25000 Algeria

Abstract: Quantum Error Correction will be necessary for preserving coherent states against noise and other unwanted interactions in quantum computation and communication. We develop a general theory of quantum error correction based on encoding states into larger Hilbert spaces subject to known interactions. We obtain necessary and sufficient conditions for the perfect recovery of an encoded state after its degradation by an interaction. The conditions depend only on the behavior of the logical states. We use them to give a recovery operator independent definition of error-correcting codes. We relate this definition to four others: The existence of a left inverse of the interaction, an explicit representation of the error syndrome using tensor products, perfect recovery of the completely entangled state and an information theoretic identity. Two notions of fidelity and error for imperfect recovery are introduced, one for pure and the other for entangled states. The latter is more appropriate when using codes in a quantum memory or in applications of quantum teleportation to communication. We show that the error for entangled states is bounded linearly by the error for pure states. A formal definition of independent interactions for qubits is given. This leads to lower bounds on the number of qubits required to correct errors and a formal proof that the classical bounds on the probability of error-correcting codes applies to error correcting quantum codes, provided that the interaction is dominated by an identity component.

Key words: The Heisenberg uncertainty principle, BB84 protocol, noise, quantum protocol, error code corrector

INTRODUCTION

Within the past few years, quantum computation and communication have undergone a dramatic evolution. From being subjects of primarily academic interest, they have become fields having an enormous potential for revolutionizing computer science and cryptography, as well as an impact on issues of national security and even potentially commercializable applications.

This has resulted not only from the development of new algorithms such as quantum factoring[1], but also as a consequence of recent experimental work on implementations of individual quantum gates[2, 3, 4]and of quantum cryptography[5].

Teleportation: Besides the most common known concept of teleportation, widely explained on sci-fi stories, we will use this intuitive approach as a way to understand how quantum communication works.For this reason, we will give a deffinition of what teleportation is and how it can be applied to carry information from one transmission point to a receiving one. In order to avoid the problem which represents the Heisenberg uncertainty principle, we will consider the teleportation as the acquisition at a receiver of a particle with the same characteristics as another one at an emitter without a spatial transmission of this particle, being both receiver and emitter separated at a random distance. This concept requires the previous explanation of the superposition principle and the entanglement, which are the sustainers of the theory.

A proceeding to teleport information: To explain how the teleportation of information works, we will introduce two characters: Alice and Bob, being the first one the emitter of the information and the second one the receiver (Fig. 1).

In this example we will use photons as elemental particle and the spin as the quantum state to be measured.

Bob, the receiver, is the one to take the first step, the generation of the EPR couple of photons.

He stores one of them and sends the other one to Alice. To make sure that the entanglement between both photons is not lost, the particles must be kept isolated from their environment[6]. Alice modifies her

Corresponding Author: Aris Skander, Electromagnetism and Telecommunication Laboratory, Department of Electronics Faculty of Engineering. Constantine University, 25000 Algeria

A proceeding to teleport information

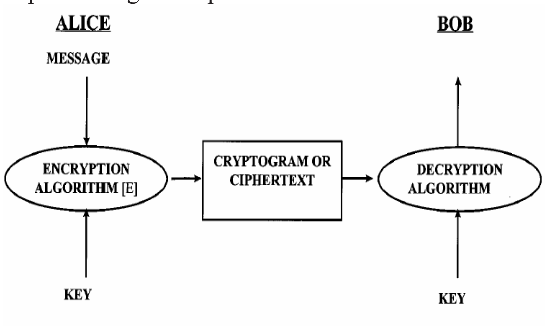


Fig. 1: Quantum teleportation

particle, using a quantum gate, which offers four possible operations (two bits of information in this case): do nothing or a 180. Spin rotation following one of the axes (*x, y* or *z*). For the photons, these operations are equivalent to a rotation of their polarization. It is important to take into account that these operations must be unitary in order to keep the coherence of the particle[7]. As we explained previously, because of the fact that both particles are entangled, the modifications applied by Alice will affect the state of Bob's particle.

Then, Alice will give her particle back to Bob, who will be able to measure them jointly (which is not limited by the uncertainty principle), using another quantum gate M and necessary to determine which one of the four possible operations Alice has done to her particle and then know which is the original message she wanted to send him[6].

Qubits: It is considered that a bit is discrete binary information unit which can take the values 0 or 1. The quantum mechanics equivalent is called qubit (quantum bit) and represents a bidimensional Hilbert space[8, 9] with the basic states |0> and |1>. It is also possible to define a general state (Fig. 3) as a coherent superposition of the basic states:

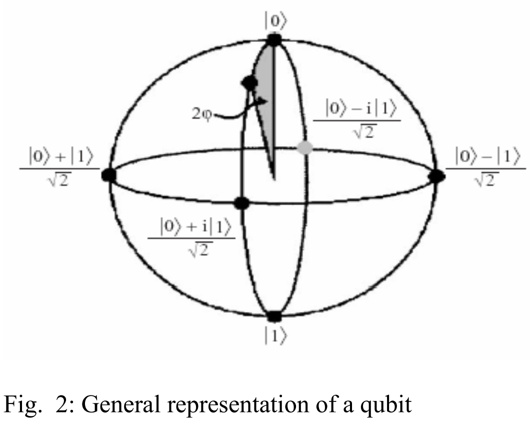

$|0\rangle$
2φ
$\frac{|0\rangle - i|1\rangle}{\sqrt{2}}$
$\frac{|0\rangle + |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle - |1\rangle}{\sqrt{2}}$
$\frac{|0\rangle + i|1\rangle}{\sqrt{2}}$
$|1\rangle$

Fig. 2: General representation of a qubit

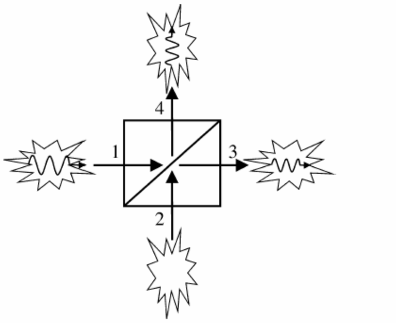


Fig. 3: Generalized four-port device representing the quantum structure of a distribution node or an amplifier

$|Q> = \alpha|0>+\beta\ e^{j\phi}|1>.$ (1)

Where

$|\alpha|^{2+}\ |\beta|^{2}=1.$ (2)

When you make a measurement over |Q> you find with a probability equal to $|\alpha|^2$ that its value is |0>and with $\beta|^2$ that it is |1>.

Coherent superpositions of states are place on the shell of the sphere whereas the incoherent superpositions are placed close to the centre. Opposite superpositions form an orthonormal basis[4].

This can lead to misunderstandings which have to be explained: the qubit is not an incoherent mixture among two states but a coherent superposition of both.

Quantum cryptographic methods: The first demonstration of a quantic cryptographic system was performed in 1989 over 32 cm of free space[10]. Ranges have been improved along the years reaching 23 km in 1997[11] and currently being 100 km (using optic fiber)[12] and 23.4 km[13].

BB84 protocol: The BB84 is the first successful quantum key exchange protocol, developed by Bennett and Brassard in 1984. Next, we are going to explain the protocol with an example.

Alice and Bob want to start a secure communication. In order to do so, they decide to exchange a private key safely using the BB84 protocol. Just to simplify the example, we will consider that Alice only generates 10 photons, which will represent 10 possible bits. She will make a measurement of the polarization over them, which might be rectilinear (+) or circular (O). She keeps the results secret and then sends, via a quantum channel, the created photons to Bob, who will receive them all (the probability of failure at the detection is 0 in this case). The sequence measured and sent by Alice is as follows:

Bob:>< II< – < I< I.

Where I stands for vertical polarization, > represents right-circular polarization, < is left-circular polarization and finally. − Represents an horizontal polarization. Bob then makes his own measurements of the polarization over the received photons, taking into account that he will apply the correct measurement with a probability of 50%. This limits the number of expected correct bits to 5. The decisions made by Bob are: + O O + + + + + + O.
Obtaining the following results:
− < < I I − I I I< .
Then Alice and Bob compare, via a public channel, which are the correct measurements (X):
Bob: + O O + + + + + + O
Alice: X   X   X X.

In this case, the raw key has a length of four bits. In order to know if someone (Eve) is eavesdropping, they have to share publicly half of the key, being these check bits chosen randomly and discarded from the final secure key. Due to the fact that Eve will also apply the correct measurement over the intercepted photons only at 50% of the cases she might provoke a mistake detectable at this comparison. Just one difference betrays Eve's presence[14].

Ekert protocol: This protocol, called Ekert 90 or EPR protocol is based on the properties of quantum-correlated pairs.

In the case of EPR pairs, we have the phenomena called entanglement, explained before, which allows us to create a series of states and measurements, which will allow us to design a protocol similar to the BB84. As in the previous case Alice and Bob initiate their key exchange via a quantum channel. A source generates one pair of EPR photons per bit of information and then sends one to Alice and one to Bob. They apply one of the possible measurements and record the result. On the second stage of the protocol, again over a public channel, they compare the measurements, being the raw key in this case the correct bits and the rejected key the rest.

To detect if Eve has been eavesdropping, Bob and Alice compare the rejected key. Because of the fact that Eve has to make a measurement over one of the photons of the EPR couple in order to read the relevant information, she breaks the entanglement properties and then makes Bell's inequality true (hidden variable)[14].

Heisenberg uncertainty principle: The Heisenberg uncertainty principle is one of the quantum physics central pillars and the first one you have to overcome when considering the possibility to make a transmission of quantum information between two distant points[15].

This principle, which has been well proved and it is the starting point of numerous theoretical and experimental formulations, states that we can neither determine the exact impulse position of a given particle nor the energy and time necessary to carry out the measurement.One of the most simple and popular formulations of the Heisenberg uncertainty principle is:

$$\Delta\chi\ \Delta P \geq h/2.$$
$$\Delta t\ \Delta E \geq h/2. \qquad (3)$$

An illustrative way to understand this is the following: to observe the position of a particle, an electron for example, we would need to use photons in order to light the particle. These photons would interact with the electrons (due to the Compton Effect), disturbing the measurement. If you do not light the electron it cannot be observed, so it cannot be detected[16].

This might also be considered as a coherence problem, derived by the random interaction between particles, is one of the most important facts to take into account when considering the possibility to establish a stable quantum communication between two points. As a consequence, the factors position/quantity of movement and time/energy do not commute (you cannot obtain simultaneous own functions), being impossible to know at the same time the position and the state of a single particle among others.

If we could manage to put some information on a particle and then send it, thanks to the uncertainty principle, we would be able to provide a better security than conventional cryptographic systems, which are only based on mathematical problems which are difficult to solve from a computational point of view and which, by the way, have been never mathematically proved as secure.

Noise due to quantum uncertainty: In quantum mechanics, Heisenberg's uncertainty principle forbids two non-commuting observables to both take a definite value simultaneously. For instance, in a state of the electromagnetic field in which the energy is well-defined, the field amplitude cannot take a definite value. This is true, in particular, in the electromagnetic vacuum (*i.e.*, in the total absence of light) where the measurable energy is strictly zero. Because of the uncertainty principle, however, the field amplitude cannot also take the value of zero but must fluctuate randomly.

These vacuum fluctuations have very important consequences for optical telecommunications, as they constitute a fundamental source of noise that contaminates an optical signal at every stage of its life, its generation, propagation and distribution, or amplification. Since the subject of the quantum noise is limitations of optical communications systems. We review here very briefly a few well-known examples of the direct manifestations of vacuum fluctuations in the different functionalities of a telecommunications system[17].

Quantum noise in signal generation: In signal generation, the vacuum fluctuations manifest themselves in two distinct ways: (a) in the existence of spontaneous emission in the amplifiers and lasers used in optical communications; and (b) in the shot noise of the optical signals.

Spontaneous emission is a process whereby the energy stored in the active medium of the laser is given off as light, with the emission of photons being triggered by the vacuum fluctuations, at random time intervals. Spontaneous emission is an indispensable ingredient in the operation of lasers, as it is this phenomenon that provides the first photon that triggers the stimulated emission, characteristic of the laser output, which is coherent and directional. However, the light that is emitted spontaneously is incoherent and omni directional and thus, apart from triggering stimulated emission, it represents an energy loss mechanism and a source of excess phase and amplitude noise both for optical amplifiers and lasers.

Shot noise is caused by the granularity of energy flow due to the existence of light quanta, the photons. An ideal laser emits coherent light that is a wave with a relatively well-defined amplitude and phase, whereas a photodiode detects energy, which is the number of photons incident on it. In other words, the process of coherent light generation and the process of light detection deal with two different variables (amplitude and photon number), which according to quantum mechanics are not compatible. Thus, in measuring the energy of a perfect coherent laser pulse, the detector will measure a fluctuating number of photons, with Poisson statistics. Shot noise is not a technical shortcoming of the detector but is another aspect of the phenomenon of vacuum fluctuations. One of the consequences of shot noise is to set a minimum energy for error-free detection, since the Poisson statistics require the detection of a few tens of photons to obtain an acceptable signal-to-noise ratio[18].

Quantum noise in distribution and propagation: Following the life history of an optical signal after it is generated, it generally propagates in a transmission system. Optical transmission systems are generally complex networks that include nodes and branching points in which the signal is divided into two or more channels. Upon branching, the relative fluctuations of the photon number of the emerging pulses are increased with respect to those of the incoming pulses, giving rise to partition noise. The origin of partition noise can be understood in quantum optics by considering the simplest model for a branching device that of a beam splitter, which is a mirror with partial transmission *T* and reflectivity *R* = 1- *T*. It is a device with two output ports (3 and 4 on Fig. 3) but also with two input ports (1,2). Translating the fact that an electromagnetic field in port 1 is partially transmitted into port 3 and partially reflected into port 4, the electric field amplitudes at the four ports can be linked by a unitary input–output transformation of the form[19]:

$$a_1 = (T)^{1/2} a_3 - (1- T)^{1/2} a_4$$
$$a_1 = (T)^{1/2} a_4 + (1- T)^{1/2} a_3 \qquad (4)$$

Input port 1 receives the signal which is channelled, after splitting or amplification, to the output ports 3 and 4. Input port 2 receives vacuum fluctuations (quantum noise) which are also channelled to the output ports after mixing with the signal. This can also be written as:

$$a_3 = (T)^{1/2} a_1 + (1- T)^{1/2} a_2$$
$$a_4 = (T)^{1/2} a_2 + (1- T)^{1/2} a_1 \qquad (5)$$

These equations indicate that the outputs at ports 3 and 4 result from a mixing of the incoming signals in ports 1 and 2. It is interesting to note that Eqs. (4) And (5) retain exactly the same form when written with quantum field operators rather than classical field amplitudes. This actually means that when the beam splitter is used as a branching device, *i.e.*, when a signal is introduced into port 1, then the ‘empty’ port 2 actually carries the vacuum state of the electromagnetic field. Splitting the incoming signal then corresponds to an electromagnetic interference process that mixes the signal field in port 1 and the vacuum fluctuations in port 2. The two emerging beams then, in ports 3 in 4, inherit amplitude derived from the amplitude of the incoming signal but also inherit a noise due to the vacuum fluctuations that enter through the second input port. It should be noted that the four-port model for a branching device is imposed by the requirement that the input and output fields be related by a unitary transformation and is independent of the geometry the device. Thus, even a 3 dB fiber Y-coupler, commonly used in fiber networks, whose apparent geometry displays only three ports, is actually a four-port device (the fourth port corresponding to refractive leakage modes) that mixes the signal with additional vacuum fluctuations, thus introducing partition noise. Cascading of branching points produces an accumulation of partition noise and this imposes limitations on the network architecture with respect to the number of nodes or read-out ports[20].

In the course of its propagation in an optical fiber, an optical signal is also subject to attenuation due to the residual absorption and the Rayleigh scattering of silica. Viewed from the perspective of quantum optics, this process continually increases the relative noise of the signal by mixing it with vacuum fluctuations. This can be seen by considering the fiber as a ‘distributed four-port device’ that gradually divides the energy of the signal between the propagation channel and the loss channel, thus adding partition noise.

Quantum noise in amplification: When a light pulse is too weak to be detected because of attenuation, energy can be injected into it through optical amplification. This increase of the pulse energy, however, is also accompanied by an increase in its noise degrading the signal to noise ratio by 3 dB (this is an asymptotic value that is reached for large gain). The origin and the fundamental nature of this excess noise (Fig.3) also can be viewed in quantum optics as a consequence of the requirement that the input and output fields be related by a unitary transformation. Considering formally the amplifier as an ‘inverse attenuator’, with a transmission coefficient larger than 1 (it corresponds to a gain), the input–output relation can be written as:

$$a_3= (G)^{1/2} a_1 + (G-1)^{1/2} a_2^{\circ} \qquad (6)$$

Where the complex conjugate of the field amplitude in port 2 is used to account for the phase change introduced by the square root when *T* is larger than 1. The structure of this equation is also the same quantum mechanically, by changing the complex conjugate into the hermitian conjugate of the corresponding field operator. In Eq. (6), port 2 corresponds to a second ‘input port’ of the amplifier that is normally empty, *i.e*., it contains only vacuum fluctuations. Thus, according to this equation, the excess noise of a linear amplifier comes from its quantum mechanical structure which requires that, in addition to the channel in which amplification occurs, the device must include at least one additional channel, such as the non-lasing modes of the laser, into which the vacuum fluctuations produce spontaneous emission in a random way. The spontaneous emission events deplete randomly the energy stored in the amplifier and thus cause fluctuations of the gain which, in turn, produce noise in the amplified signal. It should be noticed that the corresponding noise is associated with photons that are really added to the signal, while this was not the case in Eq. (4). This is why the amplifier noise can also be interpreted as a noise due to amplified spontaneous emission. Obviously, this noise limits the number of amplifiers that can be cascaded and thus imposes a constraint on total length of a transmission link and on the architecture of optical networks. In lasers, Eq. (5) also holds for a single pass through the amplifying medium, but due to the cavity feedback the overall dynamics is quite different. This is due to the gain saturation mechanism, which basically damps the intensity fluctuations, down to a value that is simply shot-noise for a Poissonian laser pumping mechanism[20].

Quantum error correction code: Large scale quantum information processing will be enormously sensitive to the effects of noise on quantum systems. Shor[21] and Steane[22] have introduced methods for doing quantum error correction in order to preserve quantum information in the presence of noise. These methods have been developed much further by a large number of researchers, notably Gottesman[23] and Calderbank *et al*[24], who developed a powerful framework for the study of quantum codes and by Preskill[25] and Shor[26], who developed methods for performing quantum information processing in the presence of noise.

In this paper we study quantum error correction from an information-theoretic point of view. Information-theoretic necessary and sufficient conditions for doing quantum error correction are formulated and the information-theoretic point of view is used to study quantum error correction as an informatic process.

MATERIALS AND METHODS

In order to have a total secured emission, we introduce in this coding part some changes on the key.

Coding part

$$\underbrace{1101001110010111\ldots\ldots\ldots\ldots\ldots}_{2^n}\ldots\ldots\ldots$$

Example

$2^n=32 \longrightarrow n=5.$

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:

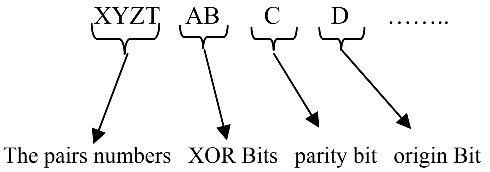
XOR =0:

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)
Emission part (1)



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. The original key is 2^n bits applied XOR; we have $2^n/2$ plus the parity bits of every pairs, with the number of pairs and the bits of XOR us 2^p bits.
The key receipt by Bob is:

$$\underbrace{00011000\ 00100111\ 00110000\ldots}_{2^p}\ldots\ldots$$

If at the reception, there are $2^{p'}$ bits that Bob will send directly to Alice a code by the classic channel that indicates to Alice there is a mistake in the number of the pure key a new emission that indicates losses of the bits on the quantum channel.

Part 2-2

at the reception, there are 2^p bits, Bob knows the number of the bits of origin, number of the parity bits, number of the bits of XOR, number of bits of the pairs (stage *). Bob cuts the key by slices with the previous calculation:
00011000/0100111/ 00110000/…………
Part 2-3

This time Bob controls the bits of the numbers, he makes calls to the reconstruction of the key to recover the slices by orders. If one finds incoherence in the numbers (same numbers for two slices):

00011000 / 00110111/00110000/………..

↓

Error in the level 3

we looks for the slice that misses in the key, since he shows the incoherence in the key and one makes calls to Alice by the classic channel to indicate with a code follows by the untraceable mistake number in the key, in our example one makes calls to the level (0011), to arrive him of the level that misses makes the difference of it:
The Bob's key:
00011000/0110111/00110000/………..
Bob décohérence in the level: 0011.
Alice receives the décohérence by Bob.
The slice incoherence to send by Alice: 00110000.
The problem is solved by Bob:
Alice: 00110000
Bob: 00011000 / 00100111/00110000/………..
Error control correction by Bob.
Part 2-4

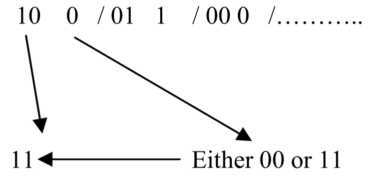
This time bob eliminates the bits of the numbering and tests the bits of origin and the parity bits with the XOR bits:
1000/ 0111/ 0000/………..
If all three identical bits of the 000 or 111 steps of problem, if no one makes calls to the level that shows the incoherence in the key:

1000/ 011**0**/ 0000/………..

↙

Error reception and correction by Bob:
1000/ 011**1**/ 0000/………..
Bob does not call to Alice this time because the correction is going to be so much immediate that the bits remain identical, the problem is solved.
Part 2-5
So much that the correction Part 2-4 is finished, Bob eliminates the parity bit or the bit of origin:
100/ 011/ 100/………..
Part 2-6

This time the reconstruction of the key in makes calls contrary to the Part 1-2 the XOR sum of the key and the Part 1-4 the Bit XOR.



10 0 / 01 1 / 00 0 /………..

11 ← Either 00 or 11

Bob reconstitutes the key: 1101001110010111……………………..

DISCUSION

The noise in physical qubits is fundamentally asymmetric: in most devices, phase errors are much more probable than bit flips. We propose a quantum error correcting code which takes advantage of this asymmetry and shows good performance at a relatively small cost in redundancy, requiring less than a doubling of the number of physical qubits for error correction. 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 (Noise due to quantum uncertainty).

In order that the quantum cryptology becomes an efficient method with application to large scales, we must introduce some techniques for real applications to coding and encoding. This precise point is the aim of our work; we will try knowing a new error correction code in quantum method cryptography thus coupling them with techniques borrowed from signal processing with purely quantum theories in order not to lose the information or to make sure to maintain the communication between Alice and Bob.

The advantages and disadvantages of BB84 error code corrector: The advantages: A high security key: by creation of the masking and coding stages in the beginning of transmission between Alice and Bob. 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.

CONCLUSION

We have made a modest contribution for securing quantum information using error code correction approach by the BB84 protocol. Several experiments have demonstrated 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 codinq error corrector in BB 84 in order not to lose and to secure the information during the communications between the users. Our future aim is to elaborate an algorithm capable of detecting and correcting errors in quantum cryptography.

ACKNOWLEDGEMENTS

I would like to thank Dr. Nadjim Merabtine for providing support and material related to educational research and for his valuable feedback as tutor. Also, I am grateful to Prof. Malek Benslama for his support in Electromagnetism and Telecommunication Laboratory which he is heading and for his supervising.

REFERENCES

1. Shor, P. 1994. Algorithms for Quantum Computation: Discrete Logarithms and Factoring. 35th Annual Symposium on Foundations of Com. Sci., U.S.A., IEEE Press.
2. Monroe, C. 1995., *et al*. Demonstration of a Universal Quantum Logic Gate NIST preprint, to appear in Physical Review Letters.
3. Domokos, P., M. A. Raimond, M. Brune and S. Haroche, 1995. Simple Cavity- QED Two-bit Universal Quantum Logic Gate: The Principle and Expected Performances. Phys. Rev. Lett., pp: 52:3554.
4. Turchette, Q. A. and all, 1995. Measurement of Conditional Phase Shifts for Quantum Logic. Phys. Rev. Lett.
5. Richard, J.H., D.M. Alde, P. dyer, G.G. Luther, G.L. Morgan and M. Schauer, 1995.Quantum Cryptography, Contemporary Physics, pp: 36-149.
6. Tittle, W., G. Weihs, 2001. Photonic entanglement for fundamental tests and quantum communication, Quantum Information and computation, Rinton Press.
7. Deutsch, D., A. Ekert, 1993. Quantum communications move into the unknown, Physics World.
8. Keyes, R., 2001. Fundamental limits of Silicon Technology, Proceeding of the IEEE 89: 227-239.
9. Svennson, C., 2001. en Futur of CMOS-Physical limits and perspectives in QNANO Workshop.
10. Steffen, M., L. Vandersypen, I. Chuang, 2002.Toward quantum computation a five qubit quantum processor, IEEE MICRO, 21:24- 34.
11. Shor, P.W., 1996. Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer, SIAM J. Sci. and Stat. Com. 26: 1484.

12. Hughes, R.J., 1994. Quantum Cryptography.
13. Bennett, C.H. and all1992. J. Cryptology, pp: 5-3.
14. Ribordy, G., J.D. Gautier, N. Gisin, O. Guinnard, H. Zbinden, 1998. Automated'plug and play'quantum key distribution, Elec. Let., 34: 2116-2117.
15. Aris, S., M. Planat, M. Benslama, 2006. The quantum cryptography: Solution to the problem due to the principle of uncertainty of Heisenberg, in WSEAS Transactions on Communication.
16. Hatcher, M., 2003. Cryptography Breaks 100 Km. Barrier, Physics World.
17. Kurtsiefer, C. and all, 2003. Quantum Cryptography: a step towards key distribution, Nature, pp: 419-450.
18. Lomonaco, S., 1998. A quick glance at Quantum Cryptography.
19. Petermann, K., 1986. IEEE J. Quantum Electron. Q.E-15 (1979) 566. See also A.E. Siegman, Lasers, University Science books, Mill Valley, CA.
20. Van der Lee, A.M., A.J.Van Druten, M.P. Van Exter, J. Woerdman and all 2000. Phys. Rev. Lett. 85.
21. Shor, P.W., 1995. Scheme for reducing decoherence in quantum memory. Phys. Rev., pp: 52:2493.
22. Steane, A.M., 1996. Error correcting codes in Quantum theory, Physical Rev. Let., pp: 77-793.
23. Gottesman, D. 1996. Class of Quantum error-correcting codes saturating the Quantum Hamming bound. Phys. Rev., pp: 54:1862.
24. Calderbank, A.R. and all, 1997. Quantum Error Correction and Orthogonal Geometry. Phys.Rev.Lett.,78: 405-8.
25. Preskill, J., 1998. Reliable Quantum Computers. Rev. Math, Phys. and Eng., 454: 385–410.
26. Shor, P.W., 1996. Quantum Error correcting codes need not completely reveal the error syndrome. ArXive e-print quant-ph/9604006.