

Detectors fiability improvement of quantum information in last generation radar systems.

¹A. R. Messai, ²A. Bennia

Signal processing Laboratory, Department of Electronics
Faculty of Engineering. Constantine University, 25000 ALGERIA.

¹r_messai@yahoo.fr; ²abdelhak.bennia@laposte.net

Abstract:

Error reconciliation is a necessary step for quantum key distribution process. In this paper, the correction ability of error reconciliation procedure called BB84 protocol is analyzed and estimated. Moreover, the experimental results proved that the capability of BB84 protocol is excellent but the protocol requires from Alice and Bob to restart their data as soon as they identify a different error in message.

In order not to lose the information or to make sure to maintain the communication between Alice and Bob we should use the QCCER-BB84 protocol with cryptography control error reconciliation.

Our contribution in this survey is on the one hand to improve the detectors fiability in order to ensure their compatibility in optical fibres telecommunications. On the other hand, introducing an error correction method in order for quantum detection last generation radar systems to be used at large scale.

Key words: Radar, quantum communications, quantum detection, quantum error correction.

1. Introduction

The quantum communications structures are based on concepts of quantum physics and information theory since they apply principals of the quantum cryptography. We are concerned by the differents techniques used for the photons to transmit data. Applying these techniques in the radars to track mobile targets requires knowledge of quantum logic and information theory to make sure to avoid perturbations existing in classical radars.

As mentioned above, the main problem of classical radar is secure data. It is here that quantum mechanics comes in handy and readily offers a solution. While the security of classical radar methods can be undermined by advances in technology and mathematical algorithms, the quantum approach can provide unconditional security.

The security is guaranteed by the Heisenberg uncertainty principle, which does not allow us to discriminate nonorthogonal states with certainty. Within the framework of classical physics, it is impossible to reveal possible eavesdropping, because information encoded into any property of a classical object can be acquired without affecting the state of the object. All classical signals can be monitored passively. In classical communications, one bit of information is encoded in billions of photons, electrons, atoms or other carriers.

It is always possible to passively listen in by deviating part of the signal and performing a measurement on it.

2. Quantum information

The creation of a physical communication system is only useful if there is a parallel development of the characterization and processing of the information to be sent through this new system, taking into account the fact that we are all the time manipulating quantum states of discrete particles.

2.1 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 [5] with the basic states $|0\rangle$ and $|1\rangle$. It is also possible to define a general state (see Fig. 1) as a coherent superposition of the basic states:

$$|Q\rangle = \alpha|0\rangle + \beta e^{i\phi}|1\rangle. \quad (1)$$

Where

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

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

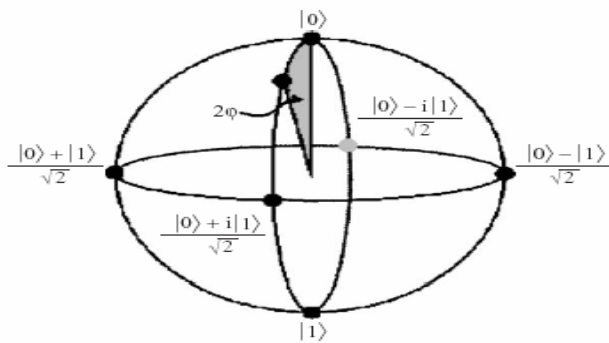


Figure (1) General representation of a qubit.

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

2.2 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 [1]. This principle, which has been well proved and it is the starting point of numerous theoretical and experimental formulations, says that you cannot determine at the same time the exact position impulse of a particle with the energy [2].

One of the most simple and popular formulations of the Heisenberg uncertainty principle is

$$\begin{aligned} \Delta x \Delta p &\geq h/2. \\ \Delta t \Delta E &\geq h/2. \end{aligned} \quad (3)$$

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

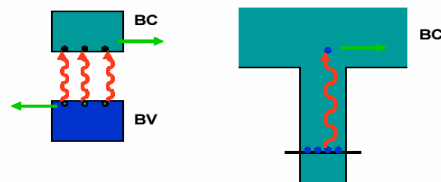
If we could manage to put some information on a particle and then send it, thanks to the uncertainty principle, we would be able to provide a better security than conventional cryptographic systems, which are only based on mathematical problems which are difficult to solve from a

computational point of view and which, by the way, have been never mathematically proved as secure [3].

2.3 the quantum detection

The principal of the quantum photo-detection is quite simple: it is about, with the help of a photon, to allow an electron to transit between a basic level, where it does not conduct the current, and an excited level where it conducts the current.

The pure semiconductor can behave as a quantum photo-detector (**figure 4**): at a basic state it does not conduct the current, but a photon can create, by photoelectric effect, an electron-hole pair and place an electron in the conduction band, allowing the current transport.



Transition interbande Transition inter-sousbande

Figure (2) Two mechanisms of quantum detection. On the left, we use the semiconductor band structure. On the right a quantum well.

3. Quantum cryptographic methods

The first demonstration of a quantum cryptographic system was performed in 1989 over 32 cm of free space [4]. Ranges have been improved along the years reaching 23 km in 1997 [5] and currently being 100 km (using optic fibre) [6] and 23.4 km (free space) [7].

3.1 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 them via a quantum channel to Bob who will receive them all. 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:

- < < II - III < .

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].

4. 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 [8].

4.1 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 [9].

4.2 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 and 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 [10]:

$$\begin{aligned} a_1 &= (T)^{1/2} a_3 - (1 - T)^{1/2} a_4 \\ a_2 &= (T)^{1/2} a_4 + (1 - T)^{1/2} a_3 \end{aligned} \quad (4)$$

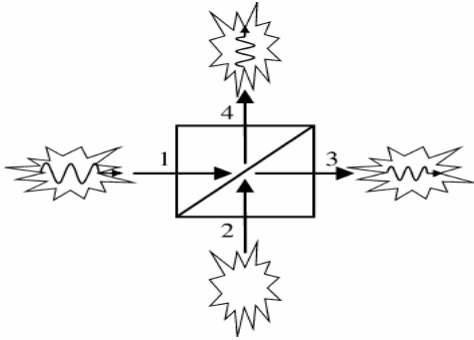


Figure (3) Generalized four-port device representing the quantum structure of a distribution node or an amplifier.

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

$$\begin{aligned} a_3 &= (T)^{1/2} a_1 + (1 - T)^{1/2} a_2 \\ a_4 &= (T)^{1/2} a_2 + (1 - T)^{1/2} a_1 \end{aligned} \quad (5)$$

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 of 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 [11].

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.

4.3 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 (that is, it corresponds to a gain), the input–output relation can be written as:

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

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 [12].

5. Quantum error correction code

The quantum information processing at large scale can be sensitive to noise effects in quantum systems.

Shor [13] and Steane [14] introduced methods concerning Quantum **error correction code** in order to protect the quantum information in the presence of noise.

These methods had been more developed by a large number of researchers, particularly Gottesman [15] and Calderbank and al [16], who developed interesting theories about quantum codes studies. Similarly preskill [17] and Shor [18, 19] have also developed methods for the execution of quantum information processing in the presence of noise.

In this paper, we study the quantum error correction from a signal processing and information theory point of view.

6. Materials and methods

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

Radar emission part (1)

1 1 0 1 0 0 1 1 1 0 0 1 0 1 1 ...

$$2^n$$

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 \longrightarrow 0.
- If the number is odd \longrightarrow 1.

A new key that is a set of 00 and 11 with a masking technique at the same 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, if the bits (00) or (11), thus additional bits are necessary, they are the **XOR Bits**:

XOR = 0:

- 00 \longrightarrow (0 for the bits 00, 0 for the XOR) 00
- 11 \longrightarrow (1 for the bits 11, 0 for the XOR) 10

XOR = 1:

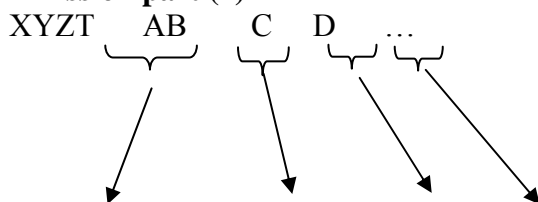
- \longrightarrow
- 01 \longrightarrow (0 for 01, 1 for XOR) 01
- 10 \longrightarrow (1 for 10, 1 for XOR) 11

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)



The pairs numbers XOR Bits parity bit origin Bit

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 same which speeds up the errors detection.

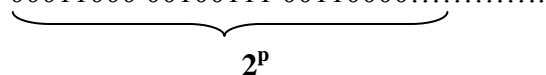
The new key before the bases choices by Alice: 00011000 00100111 00110000 ...

Radar 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:

00011000 00100111 00110000.....


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 *).

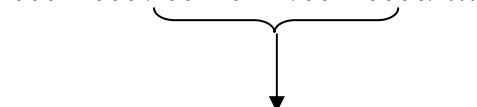
Bob cuts the key by slices with the previous calculation 00011000/0100111/ 00110000/...

Part 2-3

00011000 / 00110111 /00100000...

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 look for the slice that is transmitted in the key, since it shows the inconsistency in the key and one makes calls to Alice by the classic channel using a code that follows by the untraceable mistake number in the key, in our example one makes calls to the level (0011), when it reaches Bob the inconsistency is corrected:

The Bob's key: 00011000/0110111/00110000/.....

Bob's inconsistency in the level: 0011.

Alice receives the inconsistency from Bob.

The slice inconsistency 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/ 0110/ 0000/.....



Reception error by Bob → Correction error 1000/ 0111/ 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

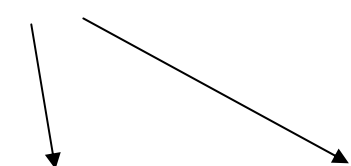
So much that the correction **Part 2-4** is finished, Bob eliminates the parity bit or the bit of origin:

100/ 011/ 100/.....

Part 2-6

This time, the reconstruction of the key in the calls is related 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.....

7. Discussion

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 spite 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 radar becomes an efficient 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 application thus coupling it 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.

7.1 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 2^n 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 and 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 in quantum detection.

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 coding error correction in order not to lose the information, 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.

References

1. M. Planat: Complementary and quantum security. IEEE, ISEC'05 19-21 June 2005 Jijel Algeria.
2. L. Bascardi: Using quantum computing algorithms in future satellite communications, *Acta Astronautica*, 57(2005), pp 224-229.
3. Z. J. Zhang: Multiparty quantum secret sharing of secure direct communication, *Physics Letters A* 342 (2005), pp 60-66.
4. Steffen M., Vandersypen L., Chuang I., "Toward quantum computation, a five qubit quantum processor, *IEEE MICRO* 21 (2) (2002), pp 24- 34.
5. Shor P.W, "Polynomial time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal of Science and statistical Computing* 26 (1996) 1484.
6. Hughes R.J., *Quantum Cryptography* (1994).
7. Bennett C.H. and all. *Journal of Cryptology* 5-3, (1992).
8. Ribordy G., Gautier J.D, Gisin N., Guinnard O., Zbinden H., "Automated'plug and play' quantum key distribution, *Electronics letters* 34 (22) (1998), pp 2116-2117.
9. Hatcher M., *Cryptography Breaks 100 Km Barrier*, *Physics World*, June 2003.
10. Kurtsiefer C., and all, *Quantum Cryptography: a step towards key distribution*, *Nature* 419 (2003) 450.
11. Lomonaco S., A quick glance at quantum cryptography, November 1998.
12. Petermann K., *IEEE J. Quantum Electron.* QE-15 (1979) 566; See also A.E. Siegman, *Lasers*, University Science books, Mill Valley, CA, 1986.
13. Van der Lee A.M., Van Druten A.J., Van Exter M.P., Woerdman J., and all *Phys. Rev. Lett.* 85 (2000).
14. Shor P.W, "Scheme for reducing decoherence in quantum memory". *Phys. Rev. A*, 52:2493, 1995.
15. Steane A.M., "Error correcting codes in quantum theory", *Physical Review Letters*, pp 77-793, 1996.
16. Gottesman D., "Class of quantum error-correcting codes saturating the quantum Hamming'bound". *Phys. Rev. A*, 54:1862, 1996.
17. Calderbank A.R, and all. "Quantum error correction and orthogonal geometry," *Phys-Rev Lett*, 78:405-8, 1997.
18. Preskill J., "Reliable quantum computers," *Rev- Math and Phys. and Eng.*, 454(1969):385-410, 1998.
19. Shor P.W, "Quantum error-correcting codes need not completely reveal the error syndrome," *ArXive e-print quant-ph/9604006*, 1996.

Article received: 2007-04-21