Quantum Based Information Transfer in Satellite Communication

Laszlo Bacsardi and Sandor Imre
Department of Telecommunications, Budapest University of Technology and Economics
Hungary

1. Introduction

The first electronic computer, the ENIAC (Electronic Numerical Integrator And Computer) was developed in 1943 at the University of Pennsylvania to calculate artillery firing tables. It contained around 17500 vacuum tubes and it weighed about 27 tonnes. Since that we construct smaller and smaller computers from year to year, whose performance is becoming higher and higher. Gordon Moore, co-founder of the Intel Corporation examined the number of transistors that can be placed inexpensively on an integrated circuit in 1965. He found that this number had doubled every second year. In his original paper he examined the time interval between 1958 and 1965. However, the trend – called Moore-law - has continued more than half a century and is not expected to stop in the next five years (Moore, 1965). The law is represented on Fig. 1.

Capabilities of many electronic devices are linked to the Moore-law, for example processor speed, memory capacity etc. We can observe a continuing size decreasing in the field of integrated circuits as well. The growth in the performance of the processor is due to putting more and more transistors on the microchip of same size. This requires smaller and smaller transistors, which can be achieved if we are able to draw thinner and thinner lines onto the surface of a semiconductor disk. The big question is how long this trend can continue? We will reach the limit of our technology and won't be able to place more transistors on an integrated circuit. Researches offer different solutions for this problem like using parallel computers, DNS-technology or informatics based on quantum mechanics. Why quantum mechanics? If we want to place more transistors on an integrated circuit of a given size, the size of transistors have to be decreased. At a point we will cross the line to the world of the atoms. In that world the classical Ebers-Moll equals are not valid anymore, and quantum mechanical equals have to be used instead. Informatics based on quantum mechanical models is called quantum informatics.

In the last years, quantum theory has appeared in satellite communications offering answers for some of nowadays' technical questions. Although quantum computers are going to be the tools of the far future, there exist already algorithms to solve problems which are very difficult to be solved by traditional computers (Imre & Ferenc, 2005).

The quantum informatics can play a key role in the field of cryptography. In present classical cryptographic methods, the key exchange is generally based on public key methods. The security of modern cryptographic methods like asymmetric cryptography, relies heavily on the problem of factoring integers. In the future, if quantum computers become reality, any information exchange using current classical cryptographic schemes will be immediately insecure. Current classical cryptographic methods are not able to guarantee long-term security. Other cryptographic methods, with absolute security must be applied in the future (Gyongyosi & Imre, 2009). The quantum cryptography gives better solutions for communication problems than the classical cryptographic methods.

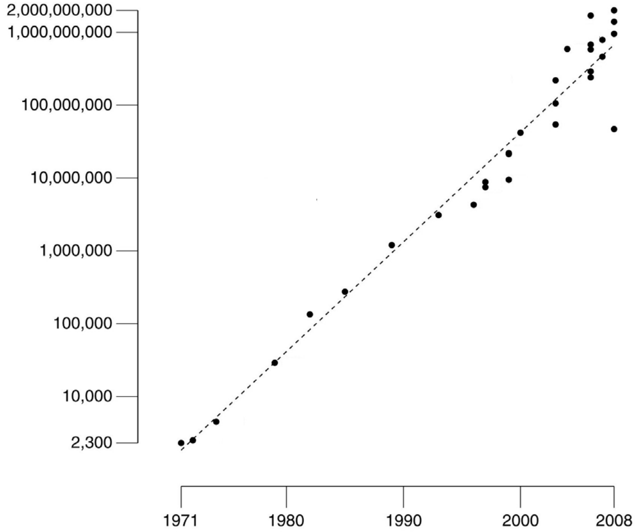


Fig. 1. One representation of the Moore-law. Horizontally the years, vertically the number of transistors in a CPU are represented. The points are for different CPU's between 1971 and 2008. The dashed line represents the Moore-law.

One of the interesting communication problems is how we can distribute a secret key for a secure communication between different parties. This is the so-called key distribution. The free-space Quantum Key Distribution (QKD) has a 16-year-old history. The first quantum cryptography protocol, the BB84 was introduced in 1984 and offered a solution for secure key distribution based on quantum theory principles like No Cloning Theorem.

The free-space quantum communications can be extended to ground-to-satellite or satellite-satellite quantum communications, which could be an ideal application for global quantum cryptography (Bacsardi, 2005).

One of the primary requirements of long-distance and free-space quantum communications is the capability of the effective transmission of quantum states in non-ideal, noisy environments. The free-space and satellite quantum channels are possible ways to increase significantly the distance limit of current quantum communication systems. To exploit the advantages of free-space quantum channels, it will be necessary to use space and satellite technology. The free space optical technology has been combined successfully with entangled pairs and satellite communications.

One of the main advantages of the usage of space for future quantum communication is the loss-free and distortion-free optical communication. In space, communication between satellites can exploit the advantages of vacuum, where the noise of the channel can be negligible. Entanglement can be used in satellite communication to enhance the security level of key agreement process, and to realize a more secure communication compared to faint pulse quantum-key distribution technology.

This chapter is organized as follows. At first we introduce basics of quantum computing (Section 2) and quantum communication (Section 3). In Section 4, we discuss the possible connections between quantum and satellite communication including different approaches for quantum based information transfer in satellite communication, which can help to establish a secure communication link. Section 5 introduces our solutions with zero redundancy error correction which can help to establish an efficient communication link.

2. What is Quantum Computing?

2.1 Short Introduction to Quantum Informatics

From the viewpoint of quantum informatics the traditionally used communication methods are called classical methods. Communication algorithms based on classical methods are called classical algorithms. Quantum research started more than 25 years ago, and a lot of interesting results has been published since that. Although Deutsch has published the theoretical plan of a quantum computer, until now it hasn't been possible to build a real working quantum computer. Researches have had a lot of success in this area, and a lot of interesting physical implementation has been demonstrated. However, quantum informatics could not play a key role because quantum based algorithms are impossible to use without a working computer. These algorithms are very different from classical ones. Their properties have advantages in factoring, encrypting messages or creating unbreakable cryptography methods. Such solutions can be bought for commercial use from different quantum companies like id Quantique, MagiQ Technologies, Quintessence Labs.

The mathematical background of Quantum Informatics can be described by four postulates. In the first postulate the state space is defined. The second axiom describes the evolution of a closed system. The third postulate deals with measurements to create connection between quantum and classical world. In the fourth one composite systems are specified (Nielsen & Chuang, 2000).

1st postulate. The actual state of any closed physical system can be described by means of a so-called state vector **v** having complex coefficients and unit length in a Hilbert space *V*, i.e. a complex linear vector space equipped with an inner product.

2nd postulate. The evolution of any closed physical system in time can be characterized by means of unitary transforms depending only on the starting and finishing time of evolution.

3rd postulate. Let *X* be the set of possible results of the measurement. A quantum measurement can be described by means of a set of corresponding measurement operators .

$$M = \{\mathbf{M}_x\}, x \in X, \mathbf{M}_x \in \mathrm{H} \qquad (1)$$

The operators should satisfy the completeness relation:

$$\sum_x \mathbf{M}_x^T \mathbf{M}_x = \mathbf{I} \qquad (2)$$

The probability of measuring *x* if the system is in state $|\varphi\rangle$ can be calculated as

$$p_x = \langle\varphi|\mathbf{M}_x^T\mathbf{M}_x|\varphi\rangle \tag{3}$$

The state of system after measurement is the following:

$$|\varphi\rangle = \frac{\mathbf{M}_x|\varphi\rangle}{\sqrt{p_x}} \tag{4}$$

4th postulate. The state space of a composite physical system *W* can be determined using the tensor product of the individual system *V* and *Y:*

$$W = V \otimes Y \tag{5}$$

2.2 Quantum bits

In classical information theory, the smallest unit is the bit. In digital computers, the voltage between the plates of a capacitor represents a bit of information: a charged capacitor denotes bit value 1 and an uncharged capacitor bit value 0. The smallest unit of the quantum informatics is the quantum bit (or qbit). One bit of information can be encoded using two different polarisations of light or two different electronic states of an atom. However, if we choose an atom as a physical bit, then apart from the two distinct electronic states the atom can be also prepared in a coherent superposition of the two states according to the rules of quantum mechanics. Therefore the atom is both in state 0 and state 1. Quantum computers use quantum states which can be in a superposition of many different numbers at the same time. In long distance communication photons are used as carriers of quantum bits. The channel can be a wired optical cable or the free-space. The problem is caused by No Cloning Theorem (NTC). According to NCT, copies can not be made of a non classical state, which means it is impossible to copy an electron spin based quantum bit to a photon based quantum bit without destroying the original quantum bit (Wootters & Zurek, 1982).

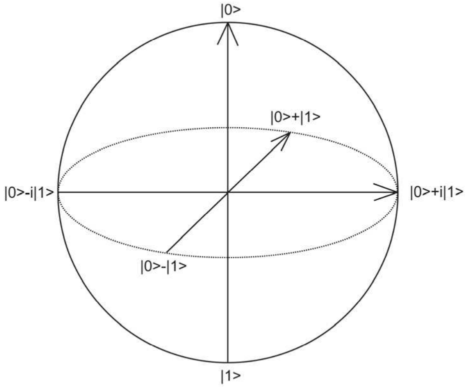


Fig. 2. Bloch sphere – a special visual representation of a quantum bit

A simple quantum system is a half-state of the two-level spin. Its basic states, spin-down |↓> and spin-up |↑>, may be relabelled to represent binary zero and one, i.e. |0> and |1>, respectively. The state of a single such particle is described by the wave function |ψ> = λ |0> + β |1>. The squares of the complex coefficients – $|\lambda|^2$ and $|\beta|^2$ – represent the probabilities for finding the particle in the corresponding states. The representation of a two dimensional quantum bit can be seen in Fig.2.

For example, |ψ> = 0.6 |0> + 0.8 |1> means that we get 0 as result after the measurement with probability of 0.6, and we get 1 as result after the measurement with probability of 0.8. Generalizing this to a set of *k* spin-1/2 particles we find that there are now 2^k basis states which equals to 2*k* possible bit-strings of length *k* (Nielsen & Chuang, 2000).

2.3 Quantum algorithms

ased on the postulates of quantum informatics quantum gates can be created, which perform a typical operation and/or transformation like identity, rotation, controlled NOT etc. A quantum gate can be described with its result or with its transformation matrix.

Some important gates are the following

$$I \equiv |0\rangle\langle 0| + |1\rangle\langle 1| \tag{6}$$

$$X \equiv |0\rangle\langle 1| + |1\rangle\langle 0| \tag{7}$$

$$\mathbf{Y} = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} \tag{8}$$

$$\mathbf{Z} = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{9}$$

$$\mathbf{H} = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{10}$$

where I is the identity transformation, X is the bit flip, Z is the phase flip, Y exchanges the probability amplitudes multiplied by *j*, and H is the Hadamard transformation.

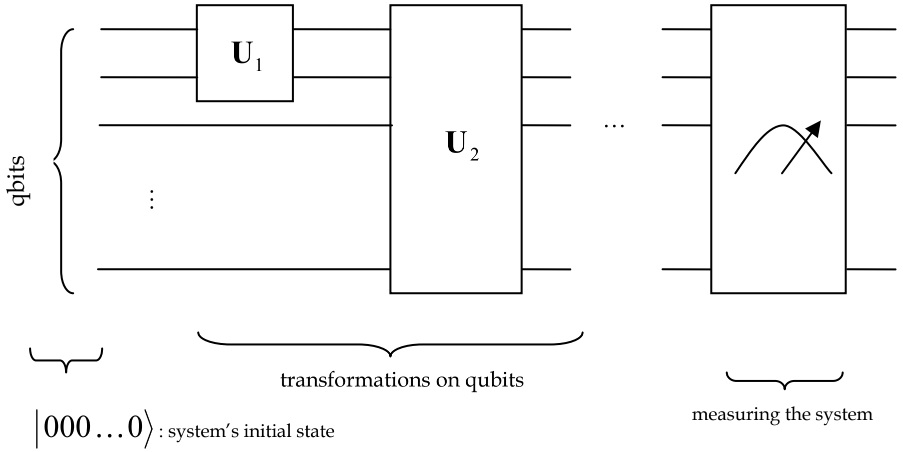

qbits
$\mathbf{U}_1$
$\mathbf{U}_2$
...
transformations on qubits
measuring the system
$|000\ldots0\rangle$: system's initial state

Fig. 3. General model of a quantum circuit

From the quantum gates, quantum circuits can be built. The quantum circuit is equivalent to the quantum algorithm, therefore quantum algorithms can be described by quantum circuits. The general model of a quantum circuit is illustrated in Fig.3. A quantum computer manipulates qbits by executing a series of quantum gates, each being unitary transformation acting on a single qbit or pair of qbits. At the end of the process, a classical result like 0 or 1 is determined by a measurement.

Let us create a quantum circuit like in Fig. 4. H is for Hadamard transformation, and the other gate is the Controlled-NOT gate (Imre & Ferenc, 2005). The final state of the system is

$$|\psi\rangle = \mathbf{CNOT} \cdot (\mathbf{H} \otimes \mathbf{I})(|0\rangle \otimes |0\rangle) = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{11}$$

If we try to decompose the $|\psi\rangle = |00\rangle + |11\rangle$, our effort provides an interesting result because individual one-qbit states do not exist . States whose decomposition comprise one-qbit states are called product states while qbit and qregisters bounded together by a special phenomenon are referred to as entangled states. There are four distinguished entangled pairs called EPR pairs (named after Einstein, Podolsky and Rosen) or the Bell states.

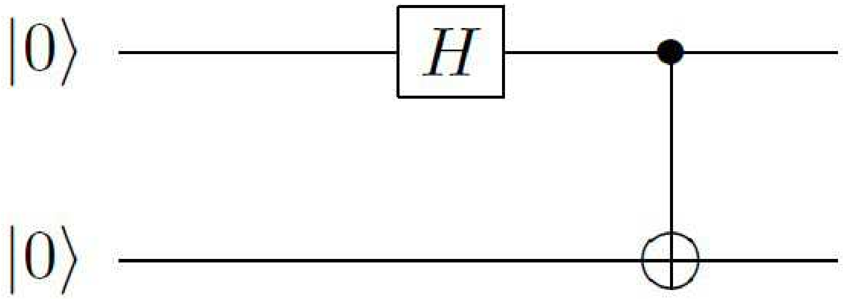


Fig. 4. EPR pairs generator quantum circuit

There are many interesting quantum algorithms, we would like to highlight some of them (Imre & Ferenc, 2005). In the quantum teleportation we use entangled pairs to transport information from point A to point B. The search in an unsorted database is faster with the Grover-algorithm than with the classical methods. We can break and decrypt the keys based on RSA algorithm with the help of Shor-algorithm. With the so-called superdense coding algorithm, two classical bits can be sent over a channel with only one quantum bit, using EPR pairs. This algorithm is illustrated in Fig.5.

From the viewpoint of the communication system, a secure key distribution is essential. In present classical cryptographic methods, the key exchange is generally based on public key methods. The security of modern cryptographic methods like asymmetric cryptography, relies heavily on the problem of factoring integers. In the future, if quantum computers become reality, any information exchange using current classical cryptographic schemes will be immediately insecure. Current classical cryptographic methods are not able to guarantee long-term security.

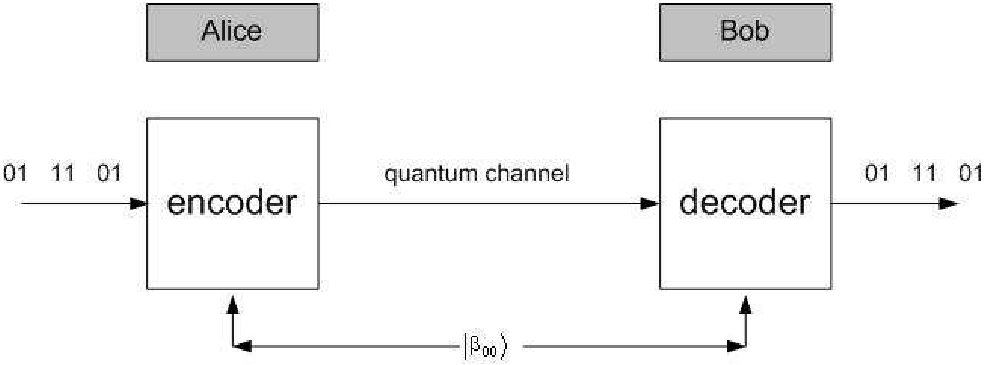


Fig. 5. In the superdense coding scenario we can send two classical bits over a channel with only one quantum bit.

3. Quantum Computing and Key Distribution

Quantum cryptography provides new ways to transmit information securely, using the fundamental principles of quantum-mechanics. As classical cryptography uses and manipulates classical bits, quantum cryptography does the same with qbits to realize provable absolute secure communication (Gyongyosi & Imre, 2009). In quantum cryptographic schemes, the secret information is not encoded directly into the quantum states, the qbits are used only to generate a secret cryptographic key, shared between two legal parties, called Alice and Bob. The main idea behind the quantum cryptographic protocols was the absolute secure key distribution. This is why we rather call these cryptographic methods as Quantum Key Distribution (QKD) systems.

These systems can provide unbreakable quantum communication. Therefore the QKD schemes may have a big relevance in future's space communication. There exist several fields, where private information must be sent through a free-space quantum communication channel. The QKD schemes solve the problem of key exchange, however some security steps are integrated after the process of quantum-based key exchange to provide provable safeness. Using quantum cryptography, the safety of future's space communication against various forms of possible attacks can be guaranteed.

The first QKD protocol was the BB84 protocol. The inventors of the BB84 protocol were C. H. Bennett and G. Brassard, and they published it in 1984 (Bennett & Brassard, 1984). C. H. Bennett in 1992 published the B92 protocol, the simplified version of the four state BB84 protocol (Bennet et al., 1992). The B92 protocol based on the similar principles of quantum mechanics like the BB84, however it uses only two polarization states.

The QKD schemes can solve the problem of key exchange and help to support sending private information through a free-space quantum channel. Using quantum cryptography, the safety of future's space communication against various forms of possible attacks can be guaranteed.

The QKD protocols are symmetric cryptographic systems. In these protocols, the action of encryption transforms the original message into an encoded message. The reverse operation of encryption is called decryption, which decodes the encoded message into the original message. The decryption operation is based on a secret key, which is a symmetric key, hence the sender and the receiver have the same one to encode and decode the given message.

In the BB84 protocol Alice draws two random series of bits. One of these are the bits for the key, the second one is for the basis of measurement. If she has 0, she sends the $\left|0\right\rangle$ state, in other case she sends $\left|1\right\rangle$ state. If the base of the measurement is 1, than she performs a Hadamard transformation on the qubit. She sends the qubit to Bob. Bob draws a random series of bits. If he has 1 bit, he performs a Hadamard transformation on the received qbit. If he has a 0 bit, he performs an Identity transformation. Bob measures the quantum bit. Alice and Bob reconcile the base of their measurement on a public channel. They delete the quantum bits on which they used different measurement base. If the channel is noiseless and there is no eavesdropper in the channel, then they have the same series of qbits. To get ensured, they conciliate some selected bits.

If Eve wants to eavesdrop the channel, then she must measure Alice's qbits with a random selected measurement base, and send new qbits. However, if Alice and Bob conciliate their bits, they will notice the errors occurred by Eve's random selection. If they conciliate *N* bits, then they can find Eve's present Eve (?) with $1-\left(\frac{3}{4}\right)^N$ probability.

4. Quantum Satellite Communications

The quantum cryptography means distributing secret keys over a public communication channel, and not encrypting and decrypting of qbits like in the classical cryptography. The main task of the QKD protocols is to achieve an absolute secure key exchange process on the quantum channel.

Currently we use quantum algorithms in space communication mostly to secure key exchange. The values of quantum bits are encoded by photon polarizations. For the communication multilaser sources and optical receiver units are used. The current satellite and free-space schemes use weak laser pulses, instead of single photon communication. The polarization states of photons are related to the logical values of quantum states, and the particles of special photon-pairs can form entanglement (Lo & Chau, 1999).

The free-space QKD was first introduced over an optical path of about 30 cm in 1991. Since that several demonstrations (like indoor optical paths of 205 m and outdoor optical paths of 75 m) increased the utility of QKD by extending it to line-of-site laser communications systems during the 90's. In 1998, a research group at Los Alamos National Laboratory, New Mexico, USA developed a free-space QKD over outdoor optical paths of up to 950 m under night time conditions (Buttler et al., 1998). Four years later, in 2002 the same laboratory demonstrated that free-space QKD is possible by daylight as well as at night. The optical path had a length of appr. 10 km (Hughes et al., 2002). In 2006, an European research group reached the distance of 144 km (Schmitt-Manderbach et al., 2007). Space quantum communication systems have been implemented over a free-space distance of 23.4 km in Germany. The proposed satellite based quantum key distribution scheme used optical devices, improved spatial filtering and narrowband passfilter to control the transmitter lasers. In this implementation, the error rate was below 6%, and the polarization preparation devices and analysis modules were stable.

Establishing a successful free-space communication is not simple. The errors would arise from background photons collected at the satellite. The background rate depends on full or new moon: the error rate will be dominated by background photons during full moon periods, and by detector noise during new moon. During the daytime orbits the background radiance would be much larger

According to our models the quantum computing algorithms can be used to affirm our free-space communication in four different ways, which are the open-air communications, earth-satellite communications, satellite broadcast and inter-satellite communications (Bacsardi, 2007).

1. *Open-air communications:* a 'horizontal' communication channel is used. The communication happens below 100km height.

2. *Earth-satellite communications:* the communications take place through greater heights than in the Open-air communication, usually between 300 and 800 km altitude. Signal encoding and decoding can be used to produce quantum error correction that allows operation in noisy environment.

3. *Satellite broadcast:* the broadcast satellites are in orbit at 36,000 km using 27 MHz frequency for signalling. The quantum algorithms can play an important role to improve the effective bandwidth, thus the brand is better utilized as in traditional cases.

4. *Inter-satellite communication:* Equals the satellite-to-satellite communications. In this case the channel is the free-space. Any kind of coding and encoding can be used, to increase stability.

The future's free-space quantum communication should be able to realize secret key distribution over long distances using low, median and geostationary satellite system. The QKD can be extended to achieve global quantum data protection. The future free-space satellite QKD schemes can be applied in two schemes [24, 25]:

1. Global quantum key distribution based on satellite-to-ground faint pulse quantum communication,

2. Simultaneous key generation between ground stations using EPR-based QKD scheme.

In Fig. 6 we illustrated the schematic of a global key exchange QKD system in free-space. The global key free-space QKD scheme uses symmetric key encoding at the space satellite modules, and the decoding process is implemented at ground level. According to the security requirements of free-space communication, the global key free-space method requires the generation of new keys regularly. In this scheme, QKD is applied during the key upload to satellites, which (?) key will be used by the satellite module to data scrambling. The satellites scramble the transmitted data to the licensed users only, and in this process, a QKD based key can be applied efficiently to ensure the advantages of quantum mechanics.

The global key exchange based QKD scheme uses faint pulse quantum cryptography. The bitrate of the key agreement process is about 1000 bit/sec. The tested implementations have worked between 600 km and 2000 km distances. The global key exchanging satellite QKD systems can be implemented with more than one ground receiving stations for a single satellite module. The exchanged keys can be used by ground stations on long distances (Koashi et al., 2008).

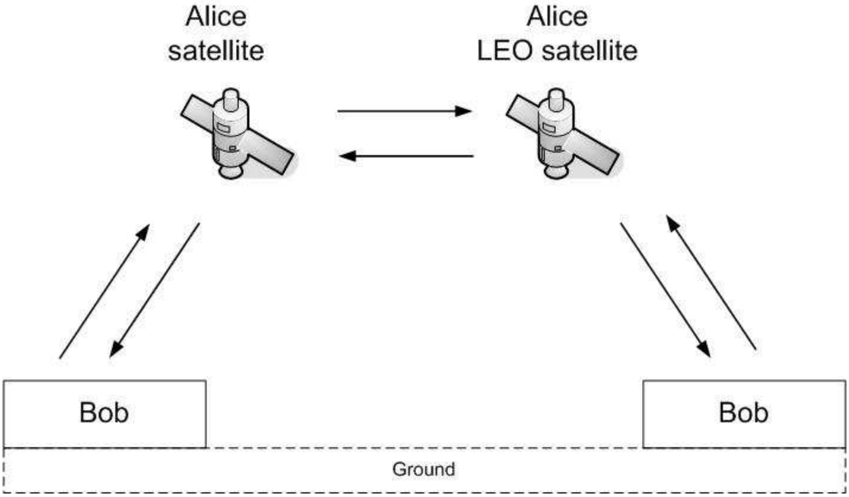


Fig. 6. Global key exchange based free-space QKD

We illustrated a satellite-to-ground free-space QKD scheme in. Fig 7. This method uses entangled photons. The bitrate of the key agreement process in the current implementations is greater than 100 bit/s.

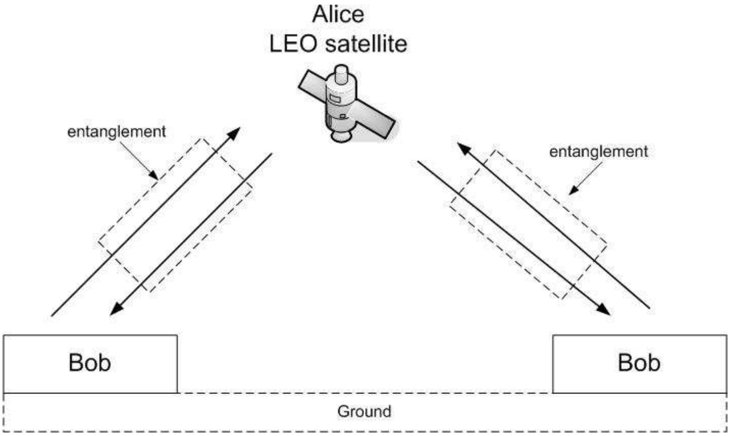


Fig. 7. Satellite-to-ground free-space QKD

The secret key agreement process requires two optical paths from the space module to the ground communication module, which increments the error rate in the current solutions. Another drawback of polarization based satellite-to-ground QKDs, that Alice and Bob rotate to each other according to the movement of the Earth, thus it is necessary to continuously compensate this movement in polarization detection (Schmitt-Manderbach et al., 2007). This kind of cryptography uses EPR-based QKD scheme. There are still many challenges in practical implementation to use entanglement. However, the free-space EPR technology can be implemented easily in current free-space QKD realizations (Ho et al., 2008; Ling et al., 2008; Tsurumaru & Tamaki, 2008).

5. Redundancy-free Quantum Channels

5.1. Importance of Redundancy-free Quantum Channels

In the classical communication we need a channel coding to handle the errors appearing in a communication channel. The error correction can be performed only with the help of redundancy in the classical system. The error correction capabilities are required for any large scale computation and communication. In these classical systems the simplest form to give redundancy to the communication is to encode the bits more than once. However, the quantum communication can be performed by more complex strategies.

In quantum computing the classical error coding methods could not be used because of the following three reasons (Nielsen & Chuang, 2000):

1. The errors are continuous. The errors can result either amplitude or phase decoherence. Moreover both errors have complex coefficients. This means that their co-domains are continuous.
2. Through the No Cloning Theorem a simple copy-based redundancy is not possible.
3. Problems occur at the measurement of the transmitted states. For the error correction the type of error has to be known. But if the quantum bits are measured for determination of the failure, then the original bits are lost.

Many quantum error correction methods have been introduced to overcome these problems and to try to handle the limitations of quantum theory principles. Since the quantum states cannot be cloned perfectly, or cannot be measured nondestructively, a simple copy-based solution is not possible. In these proposals some redundancy is required for successful error correction. However, best would to implement a redundancy-free proposal.

The redundancy-free solutions could be very useful in the long-distance free-space communication, because there would be no need to use redundant error correction codes as nowadays. With the redundancy-free techniques the effective capacity of the satellite link could also be increased

In our solution we would like to provide error correction by sending certain amount of qbits over a noisy quantum channel. The qbits are independent. Each contains information that needs to be processed. We show two different redundancy-free solutions. In the first one the noise of the quantum channel is modeled by a rotation angle. In the second one we consider the redundancy-free implementation of a unitary error correcting operator $\mathcal{R}_\theta$.

5.2. Redundancy-free Quantum Channel – Solution 1.

Our initial assumption is that the channel rotates the qbit with a ω degree which is considered to be constant. We wish to create a system where error correction is possible. To achieve this we mix the qbits and send them over the channel, as shown in Fig. 8.

We use *n* long qbits for the communication so $2^n = N$, where *n* is the length of the qbits and *N* is the size of the space. If we code the classical states into the eigenvectors of the *U* matrix, we can construct a description which leads to a redundancy-free solution With the appropriate selection of the matrix *A*, we can restore one quantum bit sent over the channel without any other (redundant) information.

Because U is unitary, it can be written in the following form

$$U = \sum_i \lambda_i \left|u_i\right\rangle, \P \tag{12}$$

where λ_i, $\left|u_i\right\rangle$ are the eigenvalues and the eigenvectors of matrix U and

$$\lambda_n = e^{j\alpha_n}. \P \tag{13}$$

Because U is unitary, it acts on each qbits and changes it as

$$\left|\psi\right\rangle = U\left|\psi_k\right\rangle. \P \tag{14}$$

Using the eigenvalues we get the following matrix for U

$$U_k = \begin{bmatrix} e^{j\alpha_{k1}} & 0 \\ 0 & e^{j\alpha_{k2}} \end{bmatrix}. \P \tag{15}$$

For the eigenvalues, we have two cases. In the first case we can describe U as

$$U = \begin{bmatrix} e^{j+\alpha} & 0 \\ 0 & e^{j+\alpha} \end{bmatrix} \otimes \begin{bmatrix} e^{j+\alpha} & 0 \\ 0 & e^{j+\alpha} \end{bmatrix} = \begin{bmatrix} e^{j2\alpha} & 0 \\ 0 & e^{j2\alpha} \end{bmatrix}, \P \tag{16}$$

In the second case we can describe U as

$$U = \begin{bmatrix} e^{j+\alpha} & 0 \\ 0 & e^{j+\alpha} \end{bmatrix} \otimes \begin{bmatrix} e^{j-\alpha} & 0 \\ 0 & e^{j-\alpha} \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I. \P \tag{17}$$

This description leads to a redundancy-free solution because the classical states are coded into the eigenvectors of the U matrix. The eigenvalues can be written in the form shown in (13) in case of a unitary transformation. The whole mathematical background of the algorithm is described in (Bacsardi et al., 2009).

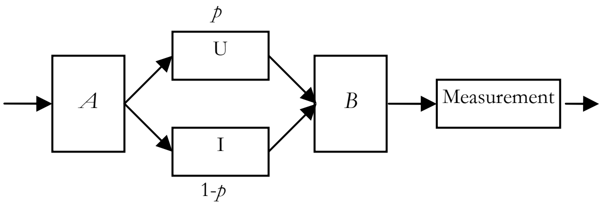


Fig. 8. Our channel model for redundancy free-error correction.

5.3. Redundancy-free Quantum Channel – Solution 2.

In this solution we consider the redundancy-free implementation of a unitary error correcting operator $\mathcal{R}_\theta$. The solution achieves the redundancy-free quantum communication using local unitary operations and unitary matrices. The error correcting operator is illustrated on Fig. 9.

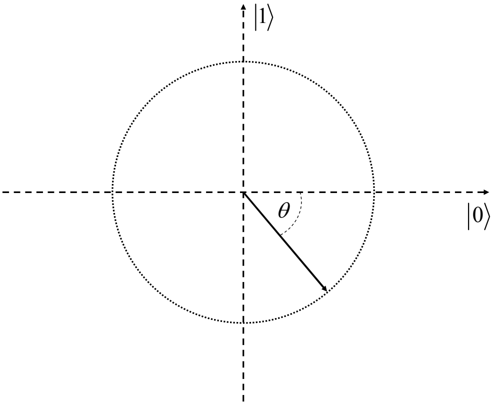


Fig. 9. Redundancy-free error correction, circle

The error of the satellite quantum channel can be modeled by a unitary rotation $\mathcal{R}_{\theta}^{\dagger}$, thus the error of the satellite quantum channel can be expressed as an angle: $\theta_i \in [0, 2\pi)$. At the beginning of the communication, Alice sends her quantum state $|\psi_A>$ on the quantum channel, which transforms it to $|d\rangle = \mathcal{R}_{\theta}^{\dagger}(\psi_A)$ with given probability *p*. The error of the quantum channel is denoted by $\mathcal{R}_{\theta}^{\dagger}$. In the error-correcting process while reading the sent quantum state, Bob doesn't know the properties of the noise on the quantum channel. In the redundancy-free coding mechanism, Alice's initial state is $|\psi_A>$, the correction transformation denoted by $\mathcal{R}_{\theta}$. Bob uses a CNOT to correct the error of the quantum channel. In order to read the sent quantum bits correctly, Bob must rotate the *i*-th data quantum bit by the angle θ_i in the opposite direction of that rotated by the error of the quantum channel. The method is illustrated on Fig. 10.

Bob has a chance not greater than $\varepsilon = \sin^2(\theta_i)$ to correct the sent states, because he doesn't know the original rotation angle θ_i of the quantum channel's error on the *i*-th sent qbit. The rotation operation $\mathcal{R}_{\theta}$ of the error correcting mechanism can be given by the angle $|\theta\rangle$, where

$$|\theta\rangle = \frac{1}{\sqrt{2}}\left(e^{i\frac{\theta}{2}}|0\rangle + e^{-i\frac{\theta}{2}}|1\rangle\right) \tag{18}$$

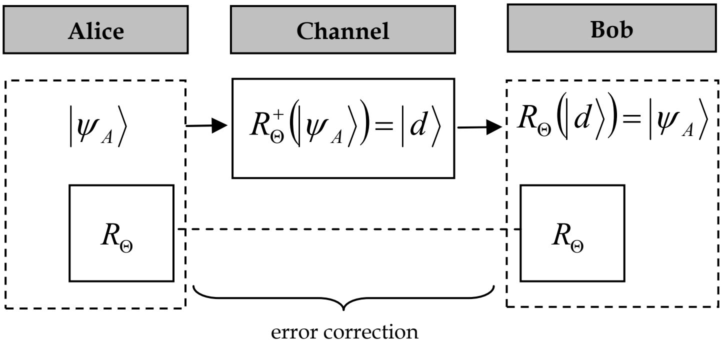

Alice
Channel
Bob
$|\psi_A\rangle$
$R_\Theta^+(|\psi_A\rangle)=|d\rangle$
$R_\Theta(|d\rangle)=|\psi_A\rangle$
R_Θ
R_Θ
error correction

Fig. 10. Redundancy-free error correction, solution 2.

The error-correcting method consists of a control qbit, which corresponds to the modified qbit $|d\rangle$, and a target qbit, which is equal to the error-correction angle state $|\theta\rangle$. To correct state $|d\rangle$ to ket(ψ_A), Bob uses a simple CNOT transformation, thus our state is transformed to

$$|d\rangle\otimes|\theta\rangle\rightarrow\frac{1}{\sqrt{2}}\left(\mathcal{R}_\theta|d\rangle\otimes|0\rangle+\mathcal{R}_\theta^\dagger|d\rangle\otimes|1\rangle\right), \tag{19}$$

and therefore a projective measurement in the $\{|0\rangle,|1\rangle\}$ base of the correction-state $|\theta\rangle$ will make the modified qbit $|d\rangle$ collapse either into the desired state $\mathcal{R}_\theta|d\rangle$ or into the wrong state $\mathcal{R}_\theta^\dagger|d\rangle$. Bob cannot determine the received state exactly, since he does not know the angle of the error θ_i. In this phase, Bob can not be sure whether the *i*-th quantum state $|d_i\rangle$ is identical to the original sent state $|\psi_i\rangle$ or not. The whole algorithm is described in (Bacsardi et al., 2009).

6. In the near future

Although the free-space QKD seems to be a tool for the future, the QKD implementations include some challenges, like the extremely high precision of optical devices, the nano-second time interval synchronization of key exchange process, and the generation of entangled photons for long distances (Ho et al., 2009; Ling et al., 2008). The future free-space QKD applications can include direct communication between satellites, where the secret quantum key agreement process will be achieved between satellites in the space. The current low, medium and geostationary earth orbit satellites between the range of 1000 km and 35,000 km can be used to achieve secure future space quantum communication (Schmitt-Manderbach et al., 2007). The fiber based results are promising as well. The Japanese Researches at National Institute of Information and Communications Technology

(NICT) reported a QKD field test through a 97 km installed fiber. Their experiments established the clock transmission technique for long distance QKD without degrading the quantum signal, using an optical amplifier for the clock signal (Tanaka et al., 2008). The first experimental implementation of a scheme for single-photon exchange between an Earth-based satellite was reported by Italian researches. They have built such an experiment which has a single photon source on a satellite, exploiting the telescope at the Matera Laser Ranging Observatory to detect the transmitted photons. Returning signals were detected from a low-earth orbit geodetic satellite (Ajisai), whose orbit has a perigee height of 1485 km.

Space-QUEST (Quantum Entanglement in Space Experiments) is a promising project. This project is led by a European research consortium and supported by the European Life and Physical Sciences in Space Program of ESA. The aim is to make a quantum communication space-to-Earth experiment from the International Space Station According to their mission scope, bringing quantum entanglement for the first time in the space environment will open a new range of fundamental physical experiments (Ursin et al., 2009).

7. Conclusions

In the next years we have to handle the problems originated from the decreasing size of microchips. As everyday life is getting faster it requires researchers and engineers to respond to the growing needs. In telecommunication applications one of the most crucial issue to solve is how to transmit as many bytes at a given frequency in a second as possible. One way to determine the system’s efficiency is to measure the number of bytes sent per second.

In this chapter we presented the base of quantum mechanic based communication. We showed that there exist already algorithms to solve problems which are very difficult to be solved by traditional computers. The quantum theory has appeared in satellite communications offering answers for some of nowadays’ technical questions. We introduced two solutions which can be useful in redundancy-free communications. One of the primary requirements of long-distance and free-space quantum communication is the capability of the effective transmission of quantum states in non-ideal, noisy environments. The free-space and satellite quantum channel could be the way to increase significantly the distance limit of current quantum communication systems. The current earthbound free-space quantum channels have the advantage in that they can be combined with satellite quantum communication. In the future, we will be able to overcome the current distance limits in quantum communication by transmitting EPR-states from space to Earth.

8. References

Bacsardi, L. (2005). Using Quantum Computing Algorithms in Future Satellite Communication. *Acta Astronautica*, Vol 57., No. (2005) 224-229, ISSN 0094-5765

Bacsardi, L. (2007). Satellite communication over quantum channel. *Acta Astronautica*. Vol 61. No. 1-6. (June-August 2007), 151-159, ISSN 0094-5765

Bacsardi, L.; Gyongyosi, L. & Imre, S. (2009). Solutions for Redundancy-free Error Correction in Quantum Channel, *Proceeding of the QuantumComm 2009*, Vico Equenso, Italy, October 2009, ICST, Gent

Bennett, C. H. & Brassard, G. (1984). Quantum cryptography: Public key distribution and coin tossing. *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, Bangalore, India, December 1984, IEEE, New York

Bennett, C. H.; Brassard, G. & Ekert, A.K. (1992). Quantum cryptography. *Scientific American*. Vol. 267(4) Issue. 50 (October 1992), ISSN 0036-8733

Buttler, W. T.; Hughes, R. J.; Kwiat, P. G. ; Lamoreaux, S. K.; Luther, G. G.; Morgan, G. L.; Nordholt, J. E.;Peterson, C. G. & Simmons, C. M. (1998) Practical free-space quantum key distribution over 1 km. *Phys. Rev. Lett.* Vol 81., October 1998, ISSN 1079-711

Gyongyosi, L & Imre, S. Fidelity Analysis of Quantum Cloning Based Attacks in Quantum Cryptography, *Proceedings of the 10th International Conference on Telecommunications*, Zagreb, Croatia, 2009

Ho, C; Lamas-Linares, A & Kurtsiefer, C (2009). Clock synchronization by remote detection of correlated photon pairs. *New Journal of Physics* Vol. 11, April 2009, ISSN 1367-2630 (2009)

Hughes, R. J.; Nordholt, J. E; Derkacs, D. & Peterson, C. G (2002). Practical free-space quantum key distribution over 10 km in daylight and at night. *New Journal of Physics*. Vol. 4., Issue 1, Jul 2002, ISSN 1367-2630

Imre, S. & Ferenc, B. (2005) *Quantum Computing and Communications: An Engineering Approach.* Wiley, ISBN 9780470869024

Ling, A. ; Peloso, M.P.; Marcikic, I.; Scarani, V. ; Lamas-Linares, A. & Kurtsiefer:, C. (2008). Experimental quantum key distribution based on a Bell test. *Physical Review A.* Vol.78 , Issue 2, 2008, ISSN 1050-2947 (2008)

Lo, H.-K. & Chau, H.F. (1999). Unconditional security of quantum key distribution over arbitrarily long distances. *Science* Vol. 283 No. 2050 (March 1999), ISSN 0036-8075

Koashi, M. ; Adachi, Y. ; Yamamoto, T. & Imoto, N. (2008). Security of Entanglement-Based Quantum Key Distribution with Practical Detectors. http://arxiv.org/abs/0804.0891, 2008.

Nielsen, M.A. & Chuang, I.L. (2000). Quantum Computation and Quantum Information. Cambridge University Press, ISBN 9780521635035, Cambridge

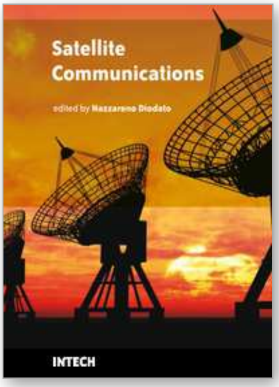
Schmitt-Manderbach, T., Weier, H; Fürst, M; Ursin,R; Tiefenbacher, F; Scheidl, T; Perdigues, J.; Sodnik, Z.; Kurtsiefer, C.; Rarity, J. G., Zeilinger, A.; & Weinfurter, H (2007). Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km, *Physical Review Letters,* Vol. 98, Issue 1, 2007, ISSN 1079-7114

Tanaka, A; Fujiwara, M.; Nam, S. W.; Nambu, Y.; Takahashi, S. ; Maeda, W. ; Yoshino, K.; Miki, S.; Baek, B.; Wang, Z.; Tajima, A.; Sasaki, M. & Tomita, A. (2008) Ultra fast quantum key distribution over a 97 km installed telecom fiber with wavelength division multiplexing clock synchronization. *Optics Express* Vol. 16, Issue 15, July 2008, ISSN 1094-4087

Tsurumaru, T. & Tamaki, K. (2008). Security Proof for QKD Systems with Threshold Detectors. http://arxiv.org/abs/0803.4226, 2008.

Ursin, R. et al. (2009), Space-QUEST. Experiments with quantum entanglement in space. *Europhysics News* Vol. 40, Issue 3, 2009, ISSN 0531-7479

Wootters, W. K. & Zurek, W. H. (1982) A single quantum cannot be cloned, *Nature* Vol. 299 No. 802–803, 1982, ISSN 0028-0836



Satellite Communications

Edited by Nazzareno Diodato

ISBN 978-953-307-135-0

Hard cover, 530 pages

Publisher Sciyo

Published online 18, August, 2010

Published in print edition August, 2010

This study is motivated by the need to give the reader a broad view of the developments, key concepts, and technologies related to information society evolution, with a focus on the wireless communications and geoinformation technologies and their role in the environment. Giving perspective, it aims at assisting people active in the industry, the public sector, and Earth science fields as well, by providing a base for their continued work and thinking.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Laszlo Bacsardi and Sandor Imre (2010). Quantum Based Information Transfer in Satellite Communication, Satellite Communications, Nazzareno Diodato (Ed.), ISBN: 978-953-307-135-0, InTech, Available from: http://www.intechopen.com/books/satellite-communications/quantum-based-information-transfer-in-satellite-communication

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821