Available online at www.sciencedirect.com
ScienceDirect
PERGAMON
Acta Astronautica 61 (2007) 151–159
ACTA ASTRONAUTICA
www.elsevier.com/locate/actaastro

Satellite communication over quantum channel

Laszlo Bacsardi*

Department of Telecommunications, Budapest University of Technology and Economics, Hungary

Available online 19 March 2007

Abstract

Quantum computing offers revolutionary solutions in the field of computer sciences, applying the opportunities of quantum physics which are incomparably richer than classical physics. Although quantum computers are going to be the tools of the far future, there are already a few algorithms to solve problems which are very difficult to handle with traditional computers.

Perhaps the easiest example of a structure of a quantum system is a quantum channel. Typically, one is interested in some basis in the Hilbert space representing the input of a channel, which is entangled with a second Hilbert space representing the environment, and then another (possibly the same) basis for the first space at a later time. Free-space quantum key distribution (QKD)—over an optical path of about 30 cm—was first introduced in 1991, and recent advances have led to demonstrations. Indeed there are certain key distribution problems in this category for which free-space QKD has practical advantages (for example it is not practical to send a courier to a satellite).

Quantum computing algorithms can be used to affirm our communication in several ways (open-air communication, satellite communications, satellite broadcast, satellite-satellite communication). We set up a free-space quantum-channel-model at the university and made several simulations. The main aim is to trace some adoptable algorithms in the communication between Earth and the satellite and also between satellites. This paper is a theoretical study to compare the simulation results of the three models.

1. Short introduction to quantum computing

In this chapter a short introduction is given into the interesting field of quantum informatics. After the postulate of this informatics the qubit is presented, which is the basic element of quantum computing; the quantum interference and the quantum cryptography. This all is necessary to understand the great power of quantum computing and quantum communications.

1.1. The Moore law

Building electronic computers is a fast improving technology, but we have to determine the future of this technology. Gordon Moore, founder of Intel observed an interesting rule called Moore's law in 1965. He concluded that since the invention of the transistors the number of transistors per chip roughly doubled every 18–24 months (see in Fig. 1). It means an exponential increase in the computing power of computers. Although this was en empirical observation in 1965 the law seems to be valid nowadays. This law estimates serious problem around 2015.

The growth in processor's performance is due to the fact that we put more transistors on the same size microchip. 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. Around nanometer thickness we reach the nanoworld, where the new rules are explained by the quantum mechanics.

* Tel.: +36 1 463 3261; fax: +36 1 463 3263.
E-mail address: bacsardi@hit.bme.hu.

0094-5765/$ - see front matter © 2007 Elsevier Ltd. All rights reserved.
doi:10.1016/j.actaastro.2007.01.024

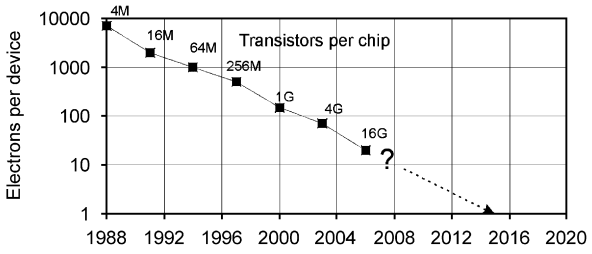

Fig. 1. Representation of the Moore law. Horizontally the years, vertically the number of electrons per device are represented.

1.2. The postulates

The quantum computing is based on postulate of the quantum mechanics, let us summarize them.

First postulate (about state space): 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.

Second postulate (about evolution): 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.

Third postulate (about measurement): Let X to be the possible results of the measurement. A quantum measurement can be described by means of a set of measurement operators:

$$M = \{\mathbf{M}_x\},\ x \in X,\ \mathbf{M}_x \in \mathbf{H}.$$

The operators should be satisfy the completeness relation:

$$\sum_x \mathbf{M}_x^{\mathrm{T}}\mathbf{M}_x = \mathbf{I}.$$

The probability of measuring m if the system is in state v can be calculated as

$$p_x = \langle\varphi|\mathbf{M}_x^{\mathrm{T}}\mathbf{M}_x|\varphi\rangle.$$

The state of system after measurement is the following:

$$\frac{\mathbf{M}_x|\varphi\rangle}{\sqrt{p_x}}.$$

Fourth postulate (about composite system): The state space of a composite physical system W can be determined using the tensor product of the individual system $W = V \otimes Y$.

1.3. A basic element: the quantum bit

In the classical information the smallest information-bearing unit is called a bit. Classical computer-use can do calculations on only one set of numbers at once. 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. But 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 quantum mechanics tells us that apart from the two distinct electronic states the atom can be also prepared in a coherent superposition of the two states. This means that 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 once. The simplest quantum system can be described by means of a two-dimensional complex valued vector in a two-dimensional Hilbert space. We call it quantum bit, qubit or qbit (Fig. 2). A quantum computer manipulates qubits by executing a series of quantum gates, each being unitary transformation acting on a single qubit or pair of qubits [1].

In applying these gates in succession, quantum computers can perform complicated unitary transformations to a set of qubits in some initial state. The qubits can then be measured with this measurement serving as the final computational result. This similarity in calculation between a classical and quantum computer affords that in theory, classical computers can accurately simulate quantum computers. The simulation of quantum computers on classical ones is a computationally

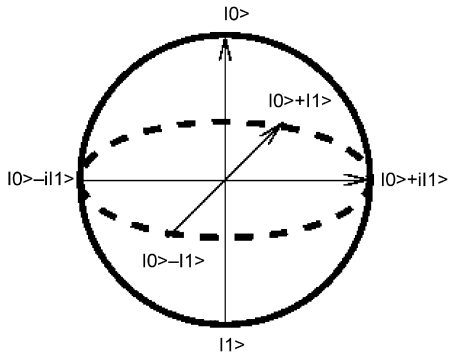

Fig. 2. The general representation of a qubit in a two-dimensional Hilbert-space.

difficult problem because the correlations among quantum bits are qualitatively different from correlations among classical bits, as first explained by John Bell [1]. For example: take a system of only a few hundred qubits, this exists in a Hilbert space of dimension $\sim 10^{90}$ that in simulation would require a classical computer to work with exponentially large matrixes (to perform calculations on each individual state, which is also represented as a matrix), meaning it would take an exponentially longer time than even with a primitive quantum computer.

The simplest quantum system is a half-state of the two-level spin. Its basic states, spin-down $|\downarrow\rangle$ and spin-up $|\uparrow\rangle$, may be relabelled to represent binary zero and one, i.e. $|0\rangle$ and $|1\rangle$, respectively. The state of such a single particle is described by the following wave function:

$$\mathbf{\Psi} = \alpha|0\rangle + \beta|1\rangle.$$

The squares of the complex coefficients—$|\alpha|^2$ and $|\beta|^2$—represent the probabilities for finding the particle in the corresponding states.

Generalizing this statement to a set of **k** spin-$\frac{1}{2}$ particles we find that there are now 2^k basis states (quantum mechanical vectors that span a Hilbert space) which equals telling that there are 2^k possible bit-strings of length **k**.

However, observing the system would cause it to collapse into a single quantum state corresponding to a single answer—a single list of 500 1s and 0s—as dictated by the measurement axiom of quantum mechanics. The reason for this is an exciting result derived from the massive quantum parallelism achieved through superposition, which would be the equivalent of performing the same operation on a classical super-computer with $\sim 10^{150}$ separate processors.

1.4. An interesting experiment

This is an elementary experiment to introduce and understand quantum informatics. In this experiment the photon first encounters a half-silvered mirror, then a fully silvered mirror, and finally another half-silvered mirror before reaching a detector, where each half-silvered mirror introduces the probability of the photon travelling down one path or the other (Fig. 3).

Once a photon strikes the mirror along either of the two paths after the first beam splitter, one might presume that the photon will reach the two detectors A (the top one) and B (the right one) with equal probability.

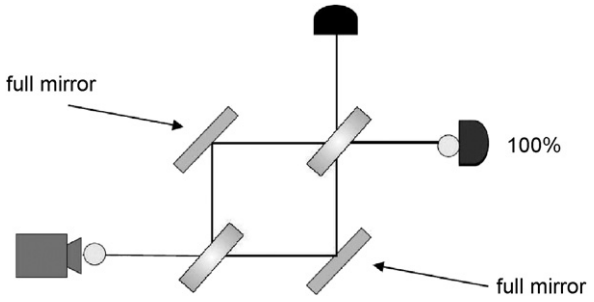

Fig. 3. Arrangement of an experiment for quantum-interference with two full and two half-silvered mirrors. On the top and right side can be the detectors, on the left side the source founded. This experiment is showing that a qubit can exist simultaneously as both 0 and 1.

However, experiments show that in reality this arrangement causes all collisions at detector A and none at detector B. The only conceivable conclusion is that the photon somehow travelled both paths simultaneously creating interference at the point of intersection that destroyed the possibility for the signal to reach detector B.

This is known as quantum interference and results from the superposition of the possible photon states or potential paths. So although only a single photon is emitted, it appears as though an identical photon exists and only detectable by the interference it causes with the original photon when their paths come together again.

If, for example, either of the paths is blocked with an absorbing screen, detector B registers hits again, just as in the first experiment. This unique characteristic, among others, makes the current research in quantum computing not merely a continuation of today's idea of a computer, but rather an entirely new branch of thought.

1.5. Quantum applications

One of the most gripping application of a quantum computer capable of implementing this algorithm lies in the field of encryption, where RSA—a common encryption algorithm, described in 1977 by Ron Rivest, Adi Shamir and Len Adleman at MIT; the letters RSA are the initials of their surnames—relies heavily on the difficulty of factoring very large composite numbers into primes. A computer which can do this easily is naturally of great interest to numerous government agencies that use RSA—previously considered to be 'uncrackable'—and anyone interested in electronic and financial privacy.

Generally cryptography allows two parties (named 'Alice' and 'Bob') to render their communications

illegible to a third party (named 'Eve'), provided they both possess a secret random bit sequence, known as a cryptographic key, which is required as an initial parameter in their encryption devices. Secure key distribution is then essential; Eve must not be able to obtain even partial knowledge of the key. Key distribution using a secure channel (named 'trusted couriers') is effective but cumbersome in practice, potentially vulnerable to insider betrayal and may not even be feasible in some applications.

Encryption is only one application of quantum computers. In addition, Shor, a pioneer researcher of quantum computing, has put together a toolbox of mathematical operations that can only be performed on a quantum computer, many of which he used in his factorization algorithm [1]. Furthermore, Feynman asserted that a quantum computer could function as a kind of simulator for quantum physics, potentially opening the doors to many discoveries in the field. Nowadays the power and capability of a quantum computer is primarily theoretical speculation; the advent of the first fully functional quantum computer will undoubtedly bring many new and exciting applications [1].

2. The model of free-space quantum channel

This chapter presents a general model of a quantum channel, introducing the quantum key distribution (QKD) and the free-space quantum channel.

2.1. General model of quantum channel

Perhaps the simplest example of a structure involving multiple times histories of a quantum system is a quantum channel (Fig. 4). Typically, one is interesting in some basis for the Hilbert space representing the input of a channel, which is tensored to a second Hilbert space representing the environment, and then another (possibly the same) basis for the first space at a later time.

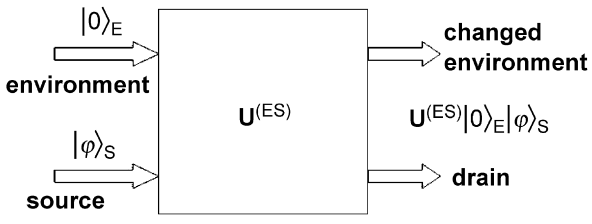

Fig. 4. General model of quantum channel. On the left side are the input variables (environment and the source), on the right side is the drain and the changed environment.

Any device taking classical or quantum systems of a certain type as input and (possibly different) classical or quantum systems as output may be referred to as a 'channel' [2]. Mathematically a channel is represented by mapping input states to output states or, dually, output observables to input observables. For many questions in quantum information theory it is crucial to characterize precisely the set of maps describing 'possible' devices. One way to characterize the possible channels is 'constructive'. That is, we allow just those channels, which can be built from the basic operations of tensoring with a second system in a specified state, unitary transformation, and reduction to a subsystem [3].

The noise appearing in the channel is the result of the interlocking with the environment, which is the adverse consequences of quantum communication, and causes problems in building such quantum applications.

2.2. Quantum key distribution

Quantum cryptography was introduced in the mid-1980s as a new method for generating the shared, secret random number sequences, known as cryptographic keys that are used in cryptosystems to provide communications security. The appeal of quantum cryptography is that its security is based on laws of nature, in contrast to existing methods of key distribution that derive their security from the perceived intractability of certain problems in number theory, or from the physical security of the distribution process. Since the introduction of quantum cryptography, several groups have demonstrated quantum communications and QKD over multi-kilometer distances of optical fibre [4].

QKD is a promising approach to the ancient problem of protecting sensitive communications from the enemy. QKD is not in itself a method of enciphering information: it is instead a means of arranging that separated parties may share a completely secret, random sequence of symbols to be used as a key for the purpose of enciphering a message.

2.3. Free-space quantum channel

From 1991, when the free-space QKD was first introduced over an optical path of about 30 cm several demonstrations (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. There are certain key distribution problems in this category for which free-space QKD would have definite

practical advantages (as for example, it is impractical to send a courier to a satellite).

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 [4]. Four years later, in 2002 the same laboratory have demonstrated that free-space QKD is possible in daylight or at night, protected against intercept/resend, beamsplitting and unambiguous state discrimination (USD) eavesdropping, and even photon number splitting (PNS) eavesdropping at night, over a 10 km, 1-airmass path, which is representative of potential ground-to-ground applications and is several times longer than any previously reported results. Their system provided cryptographic quality secret key transfer with a number of secret bits per one second quantums. This research published in their report is as follows: 'we believe that the methodology that we have developed for relating the overall system performance to instrumental and quantum channel properties may also be applicable to other QKD systems, including optical fiber based ones' [5].

3. Telecommunication over quantum channel

In this chapter we examine how can we use the free-space quantum channel in the future year's telecommunication.

At first we should know a bit about the earth-satellite communication. If we would like to detect a single QKD photon, it is necessary to know when it will arrive. The photon arrival time can be communicated to the receiver by using a bright precursor reference pulse. Received bright pulses allow the receiver to set a 1-ns time window within which to look for the QKD-photon. This short time window reduces background photon counts dramatically, and the background can be further reduced by using narrow bandwidth filters.

According to Buttler's report, the atmospheric turbulence impacts the rate at which QKD photons would be received at a satellite from a ground station transmitter. Assuming 30-cm diameter optics at both the transmitter and the satellite receiver, the diffraction-limited spot size would be 1.2-m diameter at a 300-km altitude satellite.

Errors would arise from background photons collected at the satellite. The background rate depend on full or new moon: the error rate will be dominated by background photons during full moon periods and by detector noise during a new moon.

Because the optical influence of turbulence is dominated by the lowest 2 km of the atmosphere, the results show 'that QKD between a ground station and a low-earth orbit satellite should be possible on night-time orbits and possibly even in full daylight. During the several minutes that a satellite would be in view of the ground station there would be adequate time to generate tens of thousands of raw key bits, from which a shorter error-free key stream of several thousand bits would be produced after error correction and privacy amplification [4].

At present, quantum computers and quantum information technology remains in its pioneering stage. Error correction has made promising progress to date, nearing a point now where we may have the tools required to build a computer robust enough to adequately withstand the effects of decoherence. Quantum hardware, on the other hand, remains an emerging field, but the work done thus far suggests that it will only be a matter of time before having devices large enough to test quantum algorithms. Thereby, quantum computers will emerge as the superior computational devices at the very least, and perhaps one day make today's modern computer obsolete. Quantum computation has its origins in highly specialized fields of theoretical physics, but its future undoubtedly lies in its profound effect.

In my point of view the quantum computing algorithms can be use to affirm our communication in following four ways [6]:

1. Open-air communication (horizontal telecommunication, below 100 km, instead of optical cable, using the twisted surface of Earth).
2. Satellite communications (between 300 and 800 km altitude, signal encoding and decoding). Quantum error correction allows quantum computation in noisy environment. Quantum computation of any length can be created as accurate as desired, as long as the noise is below a certain threshold, e.g. $P < 10^{-4}$.
3. Satellite broadcast (our broadcast satellite orbit at 36,000 km, using 27 MHz signal) [7]. In quadrature phase shift keying (QPSK) every symbol contains two bits, this is why the bit speed is 55 Mbs. Half the bits is for error-coding, in the best case we only have 38 Mbs, but in common solutions there is only 27–28 Mbs, in which 5–6 TV-channels can be stored with a bandwidth of 2–5 Mbs each. The quantum algorithms can prove the effective bandwidth to fill better the brand as in the traditional case.
4. Satellite-satellite communication (between broadcast or others satellite, using free-space, for signal coding and encoding, super density coding etc.).

4. Simulating communication over a quantum channel

A three-type simulation model is reviewed in this chapter, with a detailed description and simulation results, and some plans for the future.

4.1. Simulation model

We hope that the free-space quantum channel will be an important part of our communication, this is why we are studying the free-space quantum channel at Budapest University of Technology and Economics, Faculty of Electrical Engineering and Informatics, Department of Telecommunications. As computer engineers our project is to study and understand this type of channel and to set up a working model. The supervisor of the program is Dr. Sandor Imre [6].

We set up our quantum channel model in the following three ways:

1. Distance-independent model (infinite channel with a source and a drain).
2. Linear model (linear parameter for noise).
3. Fractional distances model (different items have their own noise-parameters).

In each case we started by examining the bit error rate (BER) on the empty channel, in second phase we attacked the channel, last we tried to find different methods to protect the channel.

In the third case (the distance exists fractional) the distances are divided into three items:

1. 0–20 km: bottom layer of atmosphere.
2. 20–1000 km: top layer of atmosphere.
3. 1000–36,000 km: space.

Firstly, each of this items is characterised by a constant noise-parameter depending on different physically parameters, like probability of turbulence, of cloudy or rainy weather etc. These parameters are increasing by function of the distance simulating the real environment. These noise-parameters will be refined by comparing our results with effective physical measures from around the world.

4.2. Description of the simulated model

In our channel overview the third party named Eve (the eavesdropper) can step between the two communication party, named Alice and Bob, as can be seen in the Fig. 5.

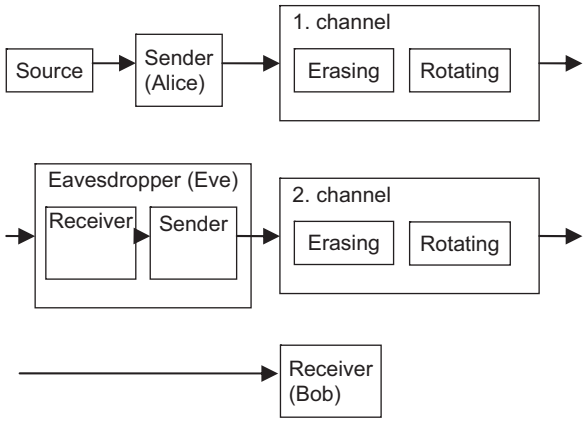

Fig. 5. Overview of simulated channel. Some elements between Alice (source) and Bob (drain) can be dropped out.

First of all we simulated the Bennett–Brassard 1984 (BB84) QKD protocol, which is the simplest quantum key distribution protocol. Shor and Preskill already proved concisely the unconditional security of this protocol [8].

We had to find the BER of the empty channel, to be able to calculate with it furthermore. After we simulated a successful QKD with BB84 and we built a more complicated channel.

4.3. Simulation results

The first version simulator-program was written in Microsoft C++ language, the second in Microsoft.NET language to make it more comfortable and easier to design. The name of the beta-version- program is Quantum Circuit, written by Attila Pereszlenyi. Although we are able to handle different gates which allow to use other than the BB84 algorithm, most of simulation were made with this protocol, which is a significant element of the quantum cryptography.

The first step was the calibration of the simulating-model, examining the independent, depolarizing errors in a channel, to determine the minimum number of required bits (one of the results showed in Fig. 6).

We determined the necessity of at least 1000 bits. In the second step we carried the BB84 into execution, with different type of noise-parameters and different number of bits. The simulation results for parameters $X = 0.1$, $Y = 0.2$, and $Z = 0.3$ (three different directions, the value is the error probability) with different number of bits is shown in Fig. 7. This is a good type

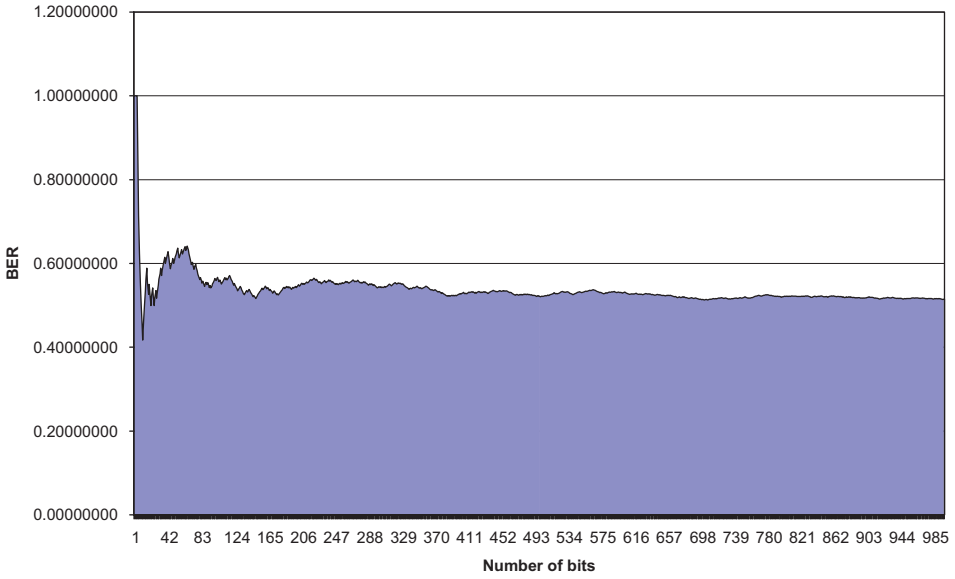

Fig. 6. Simulated channel, horizontally the number of bits, vertically the BER is represented. The chart is a special field-diagram.

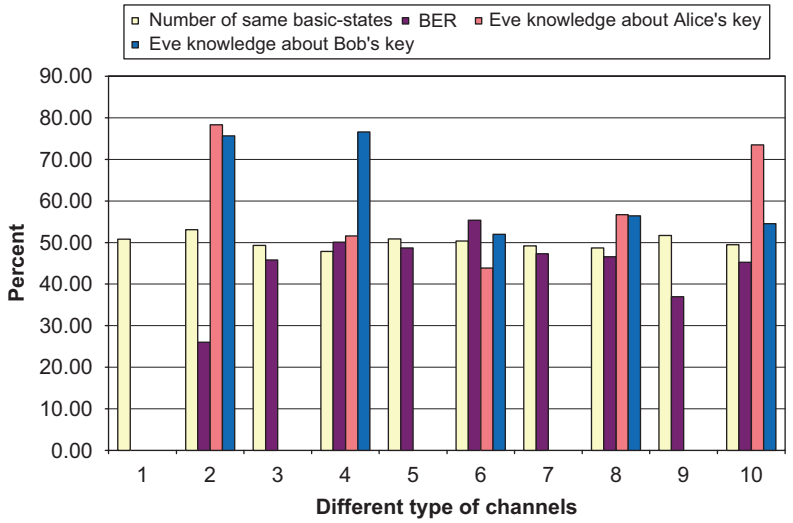

Fig. 7. Independent, depolarizing errors at BB84-simulated channel. Horizontal is the number of bits (10,000, 1000, 100), vertical the percentages (in the first case the same basic-states, in the second the BER).

of channel, because the error-rate is lower with less of bits.

In the third step I examined different noise-parameters of more than 20 different theoretical-channels.

In Fig. 8 a summary chart shows 10 different type of channel. The main-parameters for this simulation-summary are represented in Table 1.

The figures proves the need of a accurate selection of channel–noise-parameter. The sixth type of channel seems to be to have the best properties.

4.4. Future plans

This is just one step on the way to reach our object, to simulate a real free space quantum channel. The main

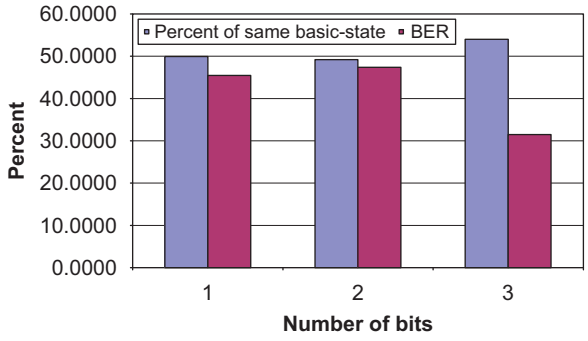

Fig. 8. Summary diagram with 10 different type of channels, source-length 1000 bit. The different values: number of same basic-states, BER, Eve knowledge about Alice's key, Eve knowledge about Bob's key.

aims that should be achieved in quantum communication are the followings:

1. production of single quantum bits (e.g photons),
2. amplification of the quantum-based signal, and
3. solution of the one-to-many communication (broadcast).

In the field of free space channel the aims are the following (most of them are physical problems):

1. minimizing the disturbing influence of atmosphere,
2. increasing the free-space distance of the quantum channel, and
3. building respective receivers and senders for the free-space quantum communications.

There is a lot of work to be done with the simulation model as well. At first we should find a correct noise parameter to describe the different type of atmosphere (setting the parameter should be based on the American team's report or measurement from the other's team or ITU-recommendations).

Eve's attendance raises some issues. The main question is whether there exists a method or equipment to discover and/or eliminate Eve's presence in the communication. The examination of the satellite communication with quantum informatics algorithms seems to be only valid within this step. The programs used for the simulations allow to simulate optional quantum-networks and quantum channels.

In the not so distant future I would like to realise other protocols than BB84 for better simulation of the broadcast and the data transmission, because in this case other type of bitstream are used.

These are only the first steps, I hope to continue studying this type of communication in the next years.

5. Summary

Quantum communications is one of the promising new fields of the new millennium. Quantum mechanics forces us to redefine the notions of information, information processing and computational complexity. More and more people are becoming interested in the quantum computing and not only physicists or mathematicians but also engineers.

We hope that in the next years algorithms based on quantum computing will appear in more technologies as they do now. The field of satellite communications

Table 1
Different type of simulated channels

No.	Channel description
1.	Noiseless channel
2.	Noiseless channel, attendance of Eve
3.	In the first part noise channel (parameters $X=25\%$, $Y=25\%$, and $Z=25\%$), in the second part noiseless channel
4.	In the first part noise channel (parameters $X=25\%$, $Y=25\%$, and $Z=25\%$) in the second part noiseless channel, attendance of Eve
5.	In both parts noise channel (parameters $X=25\%$, $Y=25\%$, and $Z=25\%$)
6.	In both parts noise channel (parameters $X=25\%$, $Y=25\%$, and $Z=25\%$), attendance of Eve
7.	In both parts noise channel (parameters $X=10\%$, $Y=20\%$, and $Z=25\%$)
8.	In both parts noise channel (parameters $X=10\%$, $Y=20\%$, and $Z=25\%$), attendance of Eve
9.	In the first part rotating channel (with probability 0.2), in the second noise channel (parameters $X=10\%$, $Y=20\%$, and $Z=25\%$)
10.	In the first part rotating channel (with probability 0.2), in the second noise channel (parameters $X=10\%$, $Y=20\%$, and $Z=25\%$), attendance of Eve

should be an important field in developing quantum communications. Although several problems are waiting to be solved, the results promise the possibility of a better type of communications.

The next step of the simulation process introduced above is setting and redefining the noise parameters for a better and more exact simulation of the earth-satellite and satellite-satellite communication over quantum channel, and to model other protocols than BB84.

The author gratefully acknowledges the help of Dr. Sandor Imre, Andras Keri, Gergely Racz and Melinda Jambrich.

References

[1] S. Imre, B. Ferenc, Quantum Computing and Communications: An Engineering Approach, Wiley, New York, 2005.

[2] E. Knill, R. Laflamme, A. Ashikhmin, H. Barnum, L. Viola, W.H. Zurek, Introduction to quantum error correction, arXiv:quant-ph/0207170.

[3] C.H. Bennett, D.P. DiVincenzo, J.A. Smolin, Capacities of quantum erasure channels, arXiv:quant-ph/9701015.

[4] W.T. Buttler, R.J. Hughes, P.G. Kwiat, S.K. Lamoreaux, G.G. Luther, G.L. Morgan, J.E. Nordholt, C.G. Peterson, C.M. Simmons, Practical free-space quantum key distribution over 1 km, arXiv:quant-ph/9805071.

[5] R.J. Hughes, J.E. Nordholt, D. Derkacs, C.G. Peterson, Practical free-space quantum key distribution over 10 km in daylight and at night, New Journal of Physics 4 (2002) 43.1–43.14.

[6] L. Bacsardi, Using quantum computing algorithms in future satellite communication, Acta Astronautica 57 (2–8) (2005) 224–229.

[7] A. Gschwindt, Satellite broadcast, in Hungarian, Muszaki Konyvkiado, Budapest, 1997.

[8] C.H. Bennett, G. Brassard, Quantum cryptography: public key distribution and coin tossing, in: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, IEEE, New York, 1984, pp. 175–179.