The Impact of Quantum Phenomena on the Complexity of Communication Systems

Aleksandar Stojanović

PhD student, Telecommunication Institute, Portugal, stojanovic.alex1@gmail.com

General survay

DOI: **10.7251/JIT1301005S** UDC: **004.056.55:004.087.5**

Abstract: This publication put the accent on strategical problems in information transmission. The analysis is based on substantially different structure between classical (bit) and quantum information unit (qubit). The scientific methodology used in this publication is relatively new (single qubit transfer based on no-cloning theorem). Important part of publication is devoted to solving problems where quantum information processing offers much more prolific solutions than classical information processing. From practical point of view, the advances of quantum based information technologies have been presented.

Keywords: quantum information, communication complexity, cryptography

Introduction

This publication is aimed to provide an outline of the current state of the quantum information technologies, as well as giving an insight into a possible direction of their further development. A quantum computer can be analyzed on the grounds of two completely different approaches:

1. by means of a model based on a family of quantum networks. [10]
2. by improving of the model of Turing machine.

Although the technical aspect was the most important in the delivery of this publication, its introductory part (i.e. the first three sections) deal with the essential changes the development of quantum algorithms have introduced into the mathematical theory of complexity. One should bear in mind that the greatest successes in the field of the quantum information processing came about by seeking quantum algorithms. At the same time, a new definition was thought of. Algorithm is computational method of the function which characterizes a given task [13].

The fourth section analyzes the quantum information from the point of view of finding an optimal code. By doing so, the results of the classical theory of information are used and new issues are pointed out, typical of quantum coding. The extent of the effects of applying quantum theory of information will heavily depend on how successfully these issues are solved.

The fifth section mirrors the dialectics in the development of technical systems – by combining two subsystems (RSA and BB84) a bi-system is created, which possesses a better average performance from its separate parts (which surprisingly enough, resembles the incidence of *'entanglement',* being the main resource of quantum cryptography).

Quantum crypto-analysis (still in its fledgling stage) is one of the main requirements for the physical realization of quantum computers.

Quantum Communication Complexi ty

The quantum communication model is based on the communication model of Yao[23]. This model

(the classical one) deals with the issue of communication by considering a situation in which two players *A, B* wish to evaluate a function *f(x, y)*. The input *x* is known only to *A*, and y is known only to *B*. In order to compute the function they have to communicate using some protocol. The resource in which the model is interested is the minimal amount of communication needed for this purpose [7]. In this context, it is necessary to mention Shanon's information theory, which also deals with the issue of transferring information and compare between the two models. Roughly speaking the main difference between this model and the well known Information theory of Shannon [19] is that information theory deals with the question of how to send messages (how to overcome problems of noise, bad links, etc.). The communication model on the other hand is concerned with the problem of what to send (i.e. design of protocols). The motive in construction of this model was the motivation to analyze computational models. This model has been proved to be successful in the area of computational complexity and many results were obtained by considering this model. Moreover, extensive research whose main subject was communication was conducted in the field of computer science. The reason for this is the importance of the abstract notions communication and information in computer science.

The quantum communication model deals with the information transfer in a quantum system. The model considers a quantum system divided into 3 parts *A, B and C,* where *A, B* are the parts which communicate via *C*. Similarly to the classical model, here is a situation in which some input *x* is coded in *A* and the other input y in *B*. The interest of this paper is the amount of information (communication) needed to be transferred by a quantum time evolution process until the value *f(x,y)* can be determined.

Motivation for this paper has been to show how quantum processes (which are more and more present from day to day) may influence complex (communication) systems (which already have enormous social importance and represent a scientific entity of our time).

Computational Complexity

Computational complexity is a mathematical branch of computer science which deals with the analysis of difficulties one comes up with in the calculation of functions. The purpose of the present section is to discuss various approaches used in solving problems in computational complexity. These differ in several aspects from those used in other areas of mathematics. For a more detailed discussion in this subject there is a good reference [16].

In order to investigate difficulties of computing certain function f it is necessary to specify some computational model which is a mathematical model (e.g. Turing machines, Boolean circuits). Having defined a particular model, 'algorithm' is the method of computing a desired function in this model. In the model, it is necessary to specify the various resources required in the computational process (the number of steps, memory requirements, etc.). These resources determine various measures of the "cost of the algorithm" which presents the central issue in computational complexity. The "cost of the algorithm" is normally calculated for the worst case situation ("worst input"). Most cases deal with Boolean functions $f: \{0, l\}^n \longrightarrow \{0,1\}$. It is assumed that f is defined for every *n*. It is of interest in the asymptotical behavior of the cost of the algorithm when $n \longrightarrow \infty$. The cost of the best possible algorithm [14] for a function ("cheapest" algorithm) defines the complexity of the function.

For every "computational model" a probabilistic variant can also be defined. This can be done in two ways which are equivalent:

1. Define a "random algorithm" as an algorithm which uses "random steps".
2. Define a "random algorithm" as constructing a probability distribution over deterministic algorithms.

The cost of the "randomized algorithm" or the reliability of the "randomized algorithm" in computing the function are measured by averaging over the random steps, or alternatively over the distribution of the algorithms. It should be marked that these results refer in most cases to the worst case input. Please note that no assumption is made regarding a specific distribution over inputs.

Complexity theory categorizes functions into classes according to their complexity. The aim is to find relations among different complexity classes. An important method in order to determine relations between two classes *A* and *B* is to find a complete function f (complete problem), which is a function of *A*, and to which it is possible to reduce every function *f* ' belonging to *A* (by reduction from *f* ' to *f* it is meant the transformation of a problem of computing *f'(x)* to a problem of computing *f(y)).*

Definition of the Model

Overview

In this section the model of quantum communication is defined.

The model of quantum communication deals with the complexity of the time evolution of many particle systems. It is based on the analysis of information transfer within the system [13]. For this purpose the system is divided into three parts: A, B and C. A and B are entities which communicate with each other. They correspond to Alice and Bob in Yao's model. Communication is transferred via C. This system is regarded as a model for computing Boolean functions $f: \{0,1\}^n X \{0,1\}^n \longrightarrow \{0,1\}$. The initial state of the system codes the input of the function: $x \in \{0, 1\}^n$ is coded in A and $y \in \{0, 1\}^n$ is coded in B. The final state codes the value of $f(x, y)$. The coding is done by the state of one of the particles (spinors). In terms of quantum mechanics, a random variable which can take the values from the set $\{0,1\}$ is obtained by measuring the state of the particle. The value of the random variable will be $f(x,y)$ with high probability. The process of computation (called the protocol) consists of a series of unitary transformations. Each unitary transformation can change either the state of the pair of components A, C or that of B, C. It is implied that there is no direct interaction between A and B. The amount of communication which is transferred is equal to the number of unitary transformations times the number of particles in C. This quantity is called the cost of the protocol. It is said that a protocol P computes the function f, if for every pair of values x, y the protocol changes the state of the system starting with a certain initial states coding x, y and ending in a final state coding $f(x, y)$. The quantum communication complexity of a function f is then defined as the minimal cost required in order protocol to compute f.

Quantum algorithm

As it has been already said, the model of Turing machine [8] does not seem to be the most appropriate to show how quantum processes work in computer science.

Therefore, the „quantum circuit" model is applied. The classical Boolean circuit is represented by Bull's elementary operations AND, OR and NOT which can simultaneously affect only one or two bits. They transform an incoming vector (represented by bits) into outcoming one (represented also by bits).

The „quantum circuit" is of a similar structure but, instead of Boolean operations it introduces elementary quantum operations - so called GATEs. A GATE is an operation over one or two qubits and it indirectly acts as an identity operator on other qubits of the quantum state.

Hadamar's transformation which copies the basic state $|b\rangle$ into $\frac{1}{\sqrt{2}}\left(|0\rangle + (-1)^b |1\rangle\right)$. is an example of a single qubit GATE. In the form of matrix it is given as:

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

An example of a two qubit GATE is a so called CNOT GATE which performs the following operation:

$$|c, b\rangle \rightarrow |c, b \oplus c\rangle$$

In the form of matrix it is given as:

$$C = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

It is known that the set of quantum logical operations (GATEs) containing CNOT and all single qubit quantum operations is universal. This means that any unitary operation can be written as a logical product of the set's elements.

The product of all elementary GATEs in a quantum circuit is a great unitary transformation which transfers an initial state into the state of the final superposition. The circuit outcome is the result of the measurements of certain parts of the system final state. It is said that the quantum circuit exactly calculates certain function f: $\{0, 1\}^n \rightarrow Z$ if it always determines the exact value of $f(x)$ for the given input x. The circuit calculates f with the final mistake if for each x gets exact $f(x)$ with a probability not less than $\frac{2}{3}$. It should be noted that quantum logic circuits could sustain only one measurement; more measurements would require additional memory, which illustrates TRADE OFF between the efficiency (complexity) of processor operation and the required amount of memory resources of the quantum computer. The complexity of the quantum logic circuits is usually measured by the number of elementary operations provided by the circuits.

A circuit is considered efficient if its complexity is, in the worst case, of the polynomial order for the set input lengths n. The brightest example of the efficiency of quantum circuits is Shore's algorithm [20] for factoring large integers.

Factorization (finding simple factors of a big number) illustrates so-called intractable problem of the following characteristics:

- The found solution is easily proven.
- Problem difficulty lies in discovering simple factors.

The point is, if p and q are large prime numbers, the product $n = pq$ is easily determined (number of elementary operations of bits is approximately of $\log_2 p \log_2 q$ size). However, it is difficult to find p and q for the given n.

The envisaged factorization time is of the super-polynominal order in relation to $\log(n)$. That means that, with the increase of n, the efficiency of the algorithm functioning is described by the function that has a faster growth rate than $\log(n)$. The best-known algorithm requires the following computer time:

$$time \approx exp[c(\ln n)^{1/3} (\ln \ln n)^{2/3}]$$

where c≈1.9. It is currently known that 65-digit factors of a 130- digit large number can be found within one month using a network of a hundred computers. Having this in mind, as well as the last formula, it can be estimated that the factorization of a 400-digit number would be completely out of reach of currently available computer networks.

The factorization problem is interesting from the aspect of the theory of complexity. For example, when referring to an intractable problem, it means the problem cannot be solved in computer time that is limited by the polynomial function of the input variable. In the case of this paper, that variable is $\log(n)$. This also is of practical importance since the scheme of public cryptography (e.g. RSA) is based on the assumed difficult factorisation of large whole numbers.

The importance of Shore's result lies in the fact that he pointed out the power of quantum computers that are capable of the factorisation in polynomial time. So, if a quantum computer capable of the factorisation of a 130-digit number during one month (which is unthinkable at the moment) was available, the use of Shor algorithm would enable factorisation of a 400-digit number in less than three years. On the basis of the fact mentioned, there is a clear insight into the direction and the extent of progress of complexity theory.

"Private quantum protocol" model

In a quantum communication model [14] Alice and Bob are holding quantum bits. The initial situation is when Alice has x, and Bob has y. The initial condition is simple $|x, y\rangle$. Let Alice start the game.

She can make a random unitary transformation over her qubits and send one or more of them to Bob. Sending quantum bits has no impact on the superposition, thus enabling Bob to apply this unitary

transformation on the received quantum bits. Each participant can measure their own qubits. At the end of the protocol the participans will have to say their values. The quantum protocol complexity is a number of quantum bits exchanged by the parties. It is said that the quantum protocol calculates $f:XxY\rightarrow\{0,1\}$ with the biggest error ε, if the likelihood that the protocol will determine the function $f(x,y)$ for each input (x,y) is at least 1-ε. The complexity of the best protocol (the lowest price) that computes f with the biggest error e is indicated as $Q_e(f)$.

"Public quantum protocol" model

An appropriate quantum protocol can be defined based on the analogy with the probability model, as in the case of the "private quantum protocol"(where analogy was also used) [14]. While, in the classical case, strings of classical bits are shared, in the quantum case, the parties share correlated quantum bits. For example, Alice and Bob share indefinitely many ERP pairs of quantum bits where Alice has the first qubit and Bob has the second qubit of one quantum pair. If Alice measures her part of the ERP pair, then both Alice and Bob look at the random string of bits. Therefore, this model represents generalisation of the"public protocol probabilistic model". The complexity of the communication of the public quantum protocol model is indicated as $Q_{\varepsilon}^{pub}(f)$.

Contrary to the classical case, the correlation between the public and private quantum protocol models has not been completely clarified.

Quantum Analogue of Huffman Coding

Quantum information is a natural generalization of classical information. The goal of this section is to find a quantum source coding scheme analogous to Huffman coding in the classical source coding theory [5] . Let us recapitulate the result of classical theory. Consider the simple example of a memoryless source that emits a sequence of inde-pendent, identically distributed signals each of which is chosen from a list $w_1, w_2,\ldots w_n$ with probabilities $p_1,p_2,\ldots,p_n$. The task of source coding is to store such signals with a minimal amount of resources. In classical information theory, resources are measured in bits. A standard coding scheme to use is the optimally efficient Huffman coding algorithm, which is a well-known lossless coding scheme for data compression. Apart from being highly efficient, it has the advantage of being instantaneous, *i.e.*, unlike block coding schemes the encoding and decoding of each signal can be done immediately. Note also that codewords of variable lengths are used to achieve efficiency. As it can be seen below, these two features—instantaneousness and variable length of Huffman coding are difficult to generalize to the quantum case. Now let us consider quantum information. In the quantum case, there is a quantum source which emits a time sequence of independent identically distributed pure-state quantum signals each of which is chosen from $|u_1\rangle,|u_2\rangle,\ldots|u_m\rangle$ with probabilities $q_1,q_2\ldots, q_m$, respectively. Notice that vectors are normalized *(i.e.*, unit vectors) but not necessarily orthogonal to each other. Classical coding theory can be regarded as a special case when the signals $|u_i\rangle$ are orthogonal. The goal of quantum source coding is to minimize the number of dimensions of the Hilbert space needed for almost lossless encoding of quantum signals, while maintaining a high fidelity between input and output. For a pure input state $|u_i\rangle$, the fidelity of the output density matrix ρ_i is defined as the probability for it to pass a yes/no test of being the state $|u_i\rangle$. Mathematically, it is given by $\langle u_i|\rho_i|u_i\rangle$ [12]. In particular, the paper is concerned with the average fidelity $F=\sum_i q_i\langle u_i|\rho_i|u_i\rangle$. It is convenient to measure the dimensionality of a Hilbert space in terms of the number of qubits (i.e. quantum bits) composing it; that is, the base-2 logarithm of the dimension. Though there has been some preliminary work on quantum Huffman coding [17], the most well-known quantum source coding scheme is a block coding scheme [12,17] . In block coding, if the signals are drawn from an ensemble with density matrix $\rho=\sum q_j|u_j\rangle\langle u_j|$, Schumacher coding, which is almost lossless, com-

presses N signals into $NS(\rho)$ qubits, where $S(\rho) = -tr\ \rho log \rho$ is the von Neumann entropy. To encode N signals sequentially, it requires $O(N^3)$ computational steps [5]. The encoding and decoding processes are far from instantaneous. Moreover, the lengths of all the codewords are the same.

Difficulties in a quantum generalization

A notable feature of quantum information is that measurement of it generally leads to disturbance. While measurement is a passive procedure in classical information theory, it is an integral part of the formalism of quantum mechanics and is an active process. Therefore, a big challenge in quantum coding is: How to encode and decode without disturbing the signals too much by the measurements involved? To illustrate the difficulties involved, a naive generalization of Huffman coding to the quantum case will be considered first. Consider the density matrix for each signal $\rho = \sum q_j \left|u_j\right\rangle\left\langle u_j\right|$ and diagonalize it into

$$\rho = \sum_i p_i \left|\phi_i\right\rangle\left\langle\phi_i\right| \qquad (1)$$

where $\left|\phi_i\right\rangle$ is an eigenstate and the eigenvalues p_i's are arranged in decreasing order.

Huffman coding of a corresponding classical source with the same probability distribution p_i's allows one to construct a one-to-one correspondence between Huffman codewords h_i and the eigen-states $\left|\phi_i\right\rangle$. Any input quantum state $\left|u_j\right\rangle$ may now be written as a sum over the complete set $\left|\phi_i\right\rangle$. Remarkably, this means that, for such a naive generalization of Huffman coding, the length of each signal is a quantum mechanical variable with its value in a superposition of the length eigenstates. It is not clear what this really means nor how to deal with such an object. If one performs a measurement on the length variable, the state-ment that measurements lead to disturbance means that irreversible changes to the N signals will be introduced which disastrously reduce the fidelity.

Therefore, to encode the signals faithfully, the sender and the receiver are forbidden to measure the length of each signal. The emphasis is on this difficulty—that the sender is ignorant of the length of the signals to be sent— is, in fact, very general. It appears in any distributed scheme of quantum computation. It is also highly analogous *to the synchronization problem in the execution of subroutines in a quantum computer: A q*uantum computer program runs various computational paths simultaneously. Different computational paths may take different numbers of computational steps. A quantum computer is, therefore, generally unsure whether a subroutine has been completed or not. There is no satisfactory resolution to those subtle issues in the general case. Of course, the sender can always avoid this problem by adding redundancies *(i.e.,* adding enough zeroes to the codewords to make them into a fixed length). However, such a prescription is highly inefficient and is self defeating for our purpose of efficient quantum coding. For this reason, such a prescription is rejected in this discussion. In the hope of saving resources, the natural next step to try is to stack the signals in line in a single tape during the transmission. To greatly simplify our discussion we shall suppose that the read/write head of the machine is quantum mechanical with its location given by an internal state of the machine (this head location could be thought of as being specified on a separate tape). But then the second problem arises. Assuming a fixed speed of transmission, the receiver can never be sure when a particular signal, say the sixth signal, arrives. This is because the total length of the signals up to that point (from the first to sixth signals) is a quantum mechanical variable (*i.e.*, it is in a superposition of many possible values). Therefore, Bob generally has a hard time in deciding when would be the correct instant to decode the sixth signal in an instantaneous quantum code.

Let us suppose that the above problem can be solved. For example, Bob may wait "long enough" before performing any measurements. We argue that there remains a third difficulty which is fatal for instantaneous quantum codes—that the head location of the encoder is entangled with the total length of the signals. If the decoder consumes the quantum signal (*i.e.,* performs measurements on the signals) before the encoding is completed, the record of the total length

of the signals in the encoder head will destroy quantum coherence. This decoherence effect is physically the same as a "which path" measurement that destroys the interference pattern in a double-slit experiment. One can also understand this effect simply by considering an example of N copies of a state $a|0\rangle + b|1\rangle$. It is easy to show that if the encoder couples an encoder head to the system and keeps a record of the total number of zeroes, the state of each signal will become impure. Consequently, the fidelity between the input and the output is rather poor.

Storage of quantum signals

Nevertheless, here will be shown that Huffman-coding inspired quantum schemes do exist for both storage and communication of quantum information. In this section, the problem of storage is considered. Notice that the above difficulties are due to the requirement of instantaneousness. This leads in a natural way to the question of storage of quantum information, where there is no need for instantaneous decoding in the first place. In this case, the decoding does not start until the whole encoding process is done. This immediately gets rid of the second (namely, when to decode) and third (namely, the record in the encoder head) problem mentioned in the last section. However, the first problem reappears in a new incarnation: The total length of say N signals is unknown and the encoder is not sure about the number of qubits that he should use. A solution to this problem is to use essentially the law of large numbers. If N is large, then asymptotically the length variable of the N signals has a probability amplitude concentrated in the subspace of values between $N\left(\bar{L}-\delta\right)$ and $N\left(\bar{L}+\delta\right)$ for any $\delta > 0$ [2,12,17]. Here $\bar{L}$ is the weighted average length of a Huffman codeword. One can, therefore, truncate the signal tape into one with a fixed length say $N\left(\bar{L}+\delta\right)$. ['0's can be padded to the end of the tape to make up the number, if necessary.] Of course, the whole tape is not of variable length anymore. Nonetheless, now it will be demonstrated that this tape can be a useful component of a new coding scheme—which we shall call quantum Huffman coding—that shares some of the advantages of Huffman coding over block coding. In particular, assuming that quantum gates can be applied in parallel, the encoding and decoding of quantum Huffman coding can be done efficiently. While a sequential implementation of quantum source block coding [2,12,17] for N signals requires $O(N^3)$ computational steps [5], a parallel implementation of quantum Huffman coding has only $O((\log N)^a)$ depth for some positive integer a. Now, our coding scheme for the storage of quantum signals will be desbribed. As before, we consider a quantum source emitting a sequence of independent identically distributed quantum signals with a density matrix for each signal shown in Eq. (1) where p_i's are the eigen-values. Considering Huffman coding for a classical source with probabilities p_i's allows one to construct a one-to-one correspondence between Huffman codewords h_i and the eigenstates $|\phi_i\rangle$. For parallel implementation, it is found useful to represent $|\phi_i\rangle$ by two pieces,[1] the first being the Huffman codeword, padded by the appropriate number of zeroes to make it into constant length,[2] $|0\cdots 0h_i\rangle$, the second being the length of the Huffman codeword, $|l_i\rangle$, where l_i = length(h_i). We also pad zeroes to the second piece so that it becomes of fixed length $\lceil \log l_{\max} \rceil$ where $l_{\max}$ is the length of the longest Huffman codeword. Therefore, $|\phi_i\rangle$ is mapped into $|0\cdots 0h_i\rangle|l_i\rangle$. Notice that the length of the second tape is $\lceil \log l_{\max} \rceil$ which is generally small compared to n. The usage of the second tape is a small price to pay for efficient parallel implementation. In this Section, the model of a quantum gate aggay for quantum computation is used. The complexity class **QNC** is the class of quantum computations that can be performed in polylogarithmic parallel depth. The well known fact that encoding or decoding of a quantum Huffman code for storage is in the com-

1 The second piece contains no new information. However, it is useful for a massively parallel implementation of the shifting operations, which is an important component in our construction.

2 The encoding process to be discussed below will allow us to reduce the total length needed for N signals.

plexity class **QNC**[18] will be used for the the results of the next subsection.

Communication

Now, the usage of the quantum Huffman coding for communication rather than for the storage of quantum signals is attempted. By communication, it is assumed that Alice receives the signals one by one from a source and is compelled to encode them one-by-one. As it will be shown below, the number of qubits required is slightly bigger, namely $N\left(\bar{L}+\delta+\left\lceil \log l_{\max}\right\rceil\right)+\left\lceil \log\left(Nl_{\max}\right)\right\rceil$. The code that will be constructed is not instantaneous, but Alice and Bob can pay a small penalty in stopping the transmission any time. In fact, there is the following:

Theorem 1: Sequential encoding and decoding of a quantum Huffman code for communication requires only $O(N^2(\log N)^a)$ computational steps.

The proof follows in the next three subsections.

Encoding

The encoding algorithm is done through alternating applications of the swap and shift operations.

$$|h_1\rangle|l_1\rangle|h_2\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|0\rangle_{tape}\otimes|0\rangle_{total\,length}$$

$$\xrightarrow{swap}|0\rangle|l_1\rangle|h_2\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|0\cdots0h_1\rangle_{tape}\otimes|0\rangle_{total\,length}$$

$$\xrightarrow{shift}|0\rangle|l_1\rangle|h_2\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_10\cdots0\rangle_{tape}\otimes|0\rangle_{total\,length}$$

$$\xrightarrow{add}|0\rangle|l_1\rangle|h_2\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_10\cdots0\rangle_{tape}\otimes|l_1\rangle_{total\,length}$$

$$\xrightarrow{swap}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_10\cdots0h_2\rangle_{tape}\otimes|l_1\rangle_{total\,length}$$

$$\xrightarrow{shift}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_1h_20\cdots0\rangle_{tape}\otimes|l_1\rangle_{total\,length}$$

$$\xrightarrow{add}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|h_N\rangle|l_N\rangle|h_1h_20\cdots0\rangle_{tape}\otimes|l_1+l_2\rangle_{total\,length}$$

$$\cdots$$

$$\xrightarrow{shift}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|0\rangle|l_N\rangle|h_1h_2\cdots h_N0\cdots0\rangle_{tape}\otimes|l_1+\cdots+l_{N-1}\rangle_{total\,length}$$

$$\xrightarrow{add}|0\rangle|l_1\rangle|0\rangle|l_2\rangle\cdots|0\rangle|l_N\rangle|h_1h_2\cdots h_N0\cdots0\rangle_{tape}\otimes|l_1+\cdots+l_N\rangle_{total\,length}$$

An ancillary space storing the total length of the codewords generated so far is included. This space requires $\log(Nl_{max})$ qubits.

Even though the encoding of signals themselves is done one-by-one, the shifting operation can be sped up by parallel computation. Indeed, as before, the required controlled-shifting operation can be performed in $O(\log N)$ depth. As before, if a sequential implementation is used instead, the complete encoding of one signal *stil* requires only $O\,(N(\log N)^a)$ gates. Now the encoding of the N signals in quantum communication is done sequentially, implying $O(N)$ applications of the shifting operation. Therefore, with a parallel implementation of the shifting operation, the whole process has depth $O\,(N(\log N)^a)$. With a sequential implementation, it takes $O\,(N^2(\log N)^a)$ steps.

Transmission

Notice that the message is written on the message tape from left to right. Moreover, starting from left to right, the state of each qubit once written remains unchanged throughout the encoding process. This decoupling effect suggests that rather than waiting for the completion of the whole encoding process, the sender, Alice, can start the transmission immediately after the encoding. For instance, after encoding the first r signals, Alice is absolutely sure that at least the first rl_{min} (where l_{min} is the minimal length of each codeword) qubits on the tape have already been written.

She is free to send those qubits to Bob immediately. There is no penalty for such a transmission because it is easy to see that the remaining encoding process requires no help from Bob at all. (Note that in the asymptotic limit of large r, after encoding r signals, Alice can even send $r\left(\overline{L}-\in\right)$ qubits for any $\in > 0$ to Bob without worrying about fidelity).

In addition, Alice can send the first r length variables l_1, ..., l_r, but she must retain the total-length variable for continued encoding. Since the total-length variable is entangled with each branch of the encoded state, decoding cannot be completed by Bob without use of this information. In other words, Alice must disentangle her system from the encoded message before decoding may be completed.

Decoding

With the length information of each signal and the received qubits, Bob can start the decoding process before the whole transmission is complete provided that he does not perform any measurement at this moment.

Problem of Quantum Key Distribution (QKD)

In the contemporary cryptography the essential problem is not how to hide the message, as it was in the past. The focus is how to protect (hide) the key. Key is secret information that is used to encrypt the message. After encryption, its result (ciphertext) is sent through the transmission media (communication channel). The encryption key should be (as much as possible) random, known only to communicating parties (Alice and Bob) and should be reused with frequency rate which is large enough for the required level of secrecy (that rate could be changed in real time, depending on communication scenario). That will give secret communication system (cryptosystem).

The one time pad (based on Vernam cipher) offers unconditional security [9]. The main drawback of this method is that all the parties exchanging secret information should be aware of a secret sequence of random numbers, i.e. a key, which is of the same length as the text to be encrypted and which is to be used only once. These keys are normally exchanged by physical means (for instance by way of a CD – Rom). By doing so, the security problem is created and difficulties may arise. Should this happen, a security problem is relocated from the message to the key and is known as the key distribution problem [3].

Since often there are no practical ways of distribution of large symmetric keys, majority of today's cryptographic protocols rely onto the public (asymmetric) distribution of keys . They could be seriously compromised (as it has been shown in the chapter 3) once the quantum computer is invented [20].

The system for quantum key distribution (QKD) may well sort out this problem. QKD technology enables an adequate regeneration of cryptographic keys and provides the proper way to secure key distribution between remote locations. In the figure 2 there is a diagram of the functioning of QKD system from one point to another, in which QKD system increases the seurity of useful information exchange. In this scenario, MagiQ-QPN [15] represents an additional hardware part used to generate and distribute the keys in a way the encryption of communication channel is performed. That additional hardware is given by optical fiber and truly random number generator.

The security performance (due to this fiber) achieved is significant and is approved with RoI (return on investment), since the additonal cost of fitting that fiber in current infrastructure is negligible comparing to potential losses and security problems that would arrise without the fiber.

On the other hand, truly random number generator (TRNG) is based on quantum logic, which is not compatible to the classical logic (on which is based pseudo-random number generator (PRG)). As an important consequence, the correlation between generated output bits from that TRNG will be ideal (zero), which is not possible with PRG generated bits. This is important for obtaining higher level of security.

The protection against breakage of the keys

Majority of the cryptosystems rarely reuse their cryptographic keys, very often less than once a year, which is the case with systems which require the physical exchange of keys (such as those using cryptographic boxes). The situation is even worse with symmetric cryptosystems that use private key (due to the impossible task of updating the keys and maintaining a number of these). It happens rarely that refreshment of cryptographic keys results in a higher rate of key expansion (the length of encrypted data/ the length of the key). That ratio should be as less as possible as far as the security is concerned. Even if the key is compromised (when the frequency of the key reusage is high) the quantity of information that the eavesdropper will get will be small.

On the other side, encryption protocols using public keys (asymmetric cryptography) require great computer power in order to achieve a considerable speed of the key generation. These protocols are going to be compromised with the advance in either mathematical algorithms or with the increase of computer power that can be exploited by an adversary.

When the key is endangered, the information which is transferred by way of communication link is vulnerable as long as the cryptographic key on that link is not regenerated. In systems in which the rate of reusage of the keys is very low (or zero), the decrypted key enables the eavesdropper (Eve) a complete access to the useful information.

The solution provided by MagiQ – QPN enables the continous refreshment of keys and by doing so the security of communication channel is improved in many ways. It should be strongly emphasised that the mentioned ratio between useful data and the corresponding key is not as large as in the case of symmetric cryptosystem. In this manner, the decrypted key in the system of MagiQ-QPN can be used to decode a small segment of information being exchanged, and thus the cryptographic key in the system is refreshed at least once per second, which is noticiable frequency of key reusage, due to the fact that this is the first commercial application ever of QKD. Not only does MagiQ-QPN provide protection against cryptographic external attacks, but it also improves the physical security of the system in terms of its internal cryptographic threats (i.e. man in the middle attack, which is current problem to QKD). This is achieved thanks to the fertile combination between classical (RSA or Vernam) and quantum cryptosystem QKD. In this symbiosis RSA can serve for the secret key exchange, QKD for solving the key distribution problem and Vernam for the encryption of useful message. As an alternative solution (which is more up-to-date) we can use quantum authentication of classical messages [1] to obtain fully QKD and after that to apply Vernam cipher. In that way, both problems of key-sharing and key establishment should be overcomed.

Secure key exchange

The security of quantum cryptography rests in the absolute potential of key exchange – quantum key distribution. By sending the key coded on the level of only one photon, quantum mechanics guarantees that if the eavesdropper intercepts the photon, he must perform the measurement on it (this is the only way for him to get the knowledge about unknown quantum state). This irreversibly changes the information coded on that particular photon and communicating parties are able to detect the eavesdropper. Therefore, the eavesdropper can neither copy that photon, nor he can read the encrypted information on it, without changing it (by no-cloning theorem (direct consequence of Heisenberg uncertainty principle and its qualitative meaning) and its experimental verification) [22] .

The encryption of data becomes indisputably secure by transsmition of quantum keys through optical fiber and truly random number generators.

For the first time, MagiQ-QPN [15] solves the problems of distribution and protection of keys, which has been implausible for centuries. The key formation in real time, which is offered by MagiQ-QPN, as well as the quantum distribution of these keys makes the cryptographic system the safest one up to now, offering the most economical key management. The useful information (encrypted message-ciphertext) can be transmitted through an optical fiber after the secret key has been established (us-

ing the same fiber). The key length and the frequency of the key reusage in this system could be adjusted to the optical channel band-width, so that communication system could support the higher useful data rate (we are sparing communication resources of the fiber and the whole communication system). Due to that fact, we obtain communication system with better average performance (better spectrum efficiency), comparing to the communication system which is not using mentioned Magic-QPN setup. Also, according to given definition of communication complexity (chapter2), our system is more efficient (we can, by using Magic QKD system easily obtain the same bit error rate (BER) as in the classical case with spending smaller number of communicating bits or bandwidth at the same time).

By using MagiQ-QPN, the two sides (Alice and Bob) communicate via photons (on physical level) which are generated, sent and detected independently. That method of information processing guarantees that an eavesdropper will be either left without information (if he wants to copy unkown quantum state) or will be uncovered by the eventually obtained partial information, (if he performs the measurement and disturbs the state which is unknown to him) . This will be described in more detail in the forthcoming chapters.

Once a secure distribution of keys has been established, one can use (indisputedly secure) code Vernam [9] which provides absolute security. This has a huge advantage as it eliminates the risk built in the systems based on the security of current commercial cryptographic solutions (which are based on the computational complexity and which have been proven to lose their security due to unpredicted development in hardware and algorithms).

Superposition

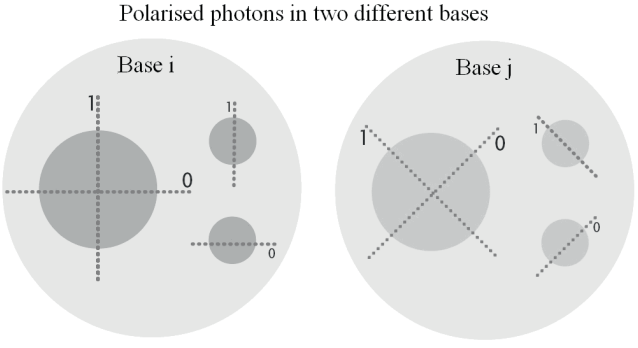
Classical information is encrypted in a binary (digital) form, i.e. in the form of zero and one, in electrical and optical systems. Quantum bit is unique as it encrypts two possible classical information states into a single coherent state of superposition. The formation of photon encoded qubits, or a coherent superposition of classical states is made possible by application of a number of techniques out of which all are mathematically equivalent. For instance, qubits can be formed by photon polarization, in time domain or in spacial domain. For QKD applications, the most enduring and most easily applicable photonic qubit transmission is in a time domain. An example of one QKD system which uses photon polarization for the encryption of qubits will be provided, since it can be applied very easily, and it provides a good insight into high level of security .

The encryption of photons

An optical channel requires a sender and a receiver (normally called Alice and Bob), and a fiber in which individually encrypted photons are transmitted. In this system, Alice can transmit photons in one of the two polarizational basis, which is shown in figure 1. Polarizational basis i encodes the photons to O degrees (which represents a binary zero, though this selection is debatable and Alice and Bob have to agree on it) and 90 degrees (which is a binary one). Polarizational basis j encodes the photons onto 45 degrees (which is a binary zero), and on 135 degrees (which is a binary one). The encoding is the matter of convention, previously established by Alice and Bob.

Alice uses a generator of random numbers (TRNG 1, figure 2) for making a random string of bits, with equal number of 0 and 1. Another generator of random numbers (TRNG2), is used to select the polarization basis (*i* or *j*) with the equal probability. After that individual photons encrypted in the appropriate way are sent through the fiber.

Figure 1. Polarization basis for encoding of photons in QKD systems



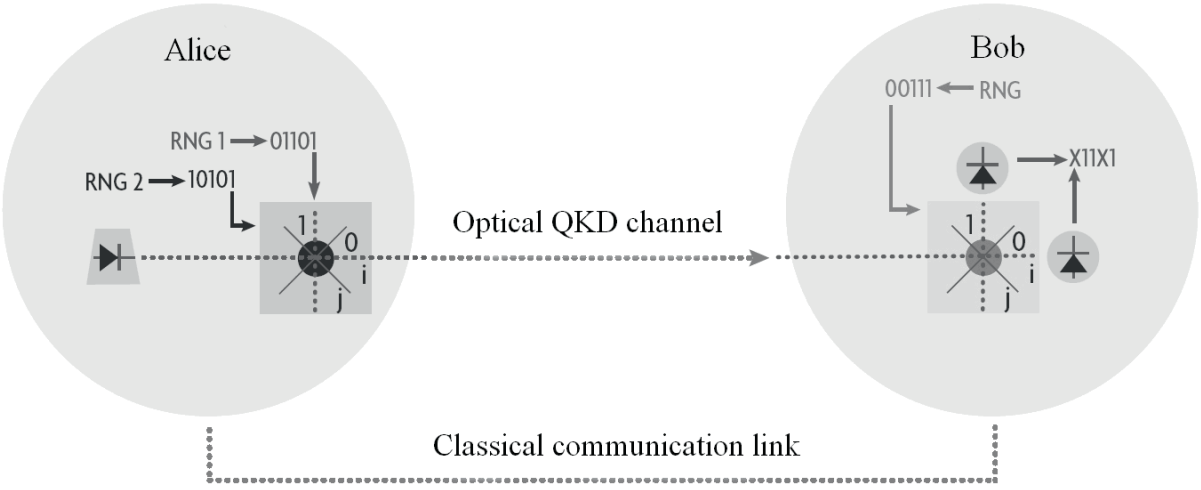
For instance, if the sequence of random numbers obtained by the generator RNG 1 = 01101, and the

sequence of random numbers obtained by the generator RNG 2 = 10101, then Alice sends five photons of the polarization as follows: 45, 90, 135,0 and 135 degrees by that order.

Photon detection

At the other end of the system, Bob receives the photons and measures their polarization. The receiver can be configured in a way that it differentiates polarization basis i and j as well as the appropriate photons polarized to 0 and 90 degrees (i base) and 45 and 135 degrees (j base).

Figure 2. Diagram of QKD system



As it is shown in figure 2, Bob uses a generator of random numbers and selects a base of reception (i or j). The laws of quantum mechanics dictate that Bob cannot properly measure the photons which are not adjusted according to the measurement base. For instance, if Alice sends the photons to the base i, and Bob has configured his receiver to measure the photons in the base j, then the receiver has equal chance to measure both 0 and 1 and the measurement result will be random. Bob then secretly saves the information about the received key and about the measurement base he used.

When the key transmission is finished, Bob reads which basis he has used to measure photons and uses classical (public) communication channel to announce it. Alice then communicates to Bob through the public channel to agree upon which corresponding basis are the same. Finally, Alice and Bob reject the bits measured in the opposite basis. That is statistically the half of the total number of transmitted (received) photons (bits), whereas the remaining bits which correpond to correct basis forms are the so called sifted key. After that, remaining steps are completely classical.

Error estimation

If sides are using a QKD protocol over a noisy channel, this situation turns into an advantage for an eavesdropper. Because at any time slot, if both sides use same type of filter for sending (reading) process and they do not have the same qubit value this can be due to not only existence of an eavesdropper but also to physical noise of transmission medium. This situation prepares a suitable environment for attacks on QKD systems over physical channel's noise.

To avoid such attacks, both sides determine an error threshold value "Rmax"(bit rate) when they are sure that there is no eavesdropping on transmission medium. Then after each QKD session, they compare (sacrifice) some bits of their raw keys in order to calculate a transmission error percentage "R". In that way, for R > Rmax case they can be sure about the existence of an eavesdropper and the protocol is restarted. It also must be stated that for QKD systems Rmax threshold value must be ideally chosen in a way that it is not smaller than the percentage of photons of which polarisations are spoiled due to transmission channel's or hardware's noise and not big enough to allow eavesdropping attempts [21]. An improper choice can lead to revelation of secret data or false alerts. This

ideal threshold value will keep on decreasing as physical noise of today's transmission lines and hardwares decreases and eventually it will be so hard to eavesdrop on QKD systems by hiding behind physical noise.

Key reconciliation

Even for R ≤ Rmax case, there can be erroneous bits in uncompared parts of keys. In this situation sides apply an error minimization step called "Key Reconciliation". This step includes these sub-steps:

1. Sending and receiving sides reorders their bit sequences by a common permutation function on which they agreed over public channel. In this way they distribute erroneous bits uniformly.
2. Bit sequences are divided into blocks of k bits. To reduce the possibility of more than one erroneous bit's existence in each block, k must be chosen ideally.
3. For each block, sending and receiving sides calculates a parity value and announces it. Last bit of each block of which parity value is annonunced, is deleted.
4. Both sides divide each matching block with different parity values into subblocks
5. and compare parity values of these sub-blocks in order to find erroneous bits [6]. This method is like "Binary Search". Last bit of each sub-block of which parity value is annonunced is also deleted.
6. There can be more than one erroneous bit in any block, for this reason first 4 sub-steps are reapplied by increasing k.
7. In order to detect remaining erroneous bits, both sides calculate the parity value of half of their bit sequences by announcing bit indices. If those values are *still* different then sides start "Binary Search" method in fourth substep again.

Privacy amplification

Privacy Amplification is the fourth step which is applied to minimize the number of bits that an eavesdropper knows in the final key [21]. Sending and receiving sides applies a shrinking method to their bit sequences in a way that eavesdropper can not apply properly to his/her bit sequence.

Let's assume that we have a bit sequence of *n* bits after application of first 3 steps. And also let's assume that eavesdropper knows m (m is a value derived from Rmax) bits of this final bit sequence. Then a number of *n-m-s* (s is a constantly chosen security parameter) sub-blocks is extracted from final bit sequence without revealing its contents and union of these subblocks's parity values form the final key. By this way number of bits that an eavesdropper may know is reduced to 2 – s / ln 2 and length of final key since start of QKD session is reduced to *n-m-s* bits.

Detection of eavesdroppers

One technique for performing attacks for Eve on the key between Alice and Bob is the use of transmitter and receiver similar to those which Alice and Bob use. Thus the interception is masked. When the eavesdropper Eve tries to intercept the message, it plants an error in the system, because it cannot know which base Alice will use for encrypting the photons [4]. In this scenario (figure 3), Eve detects the transmitted photons in the same way as Bob- by random choice of a measuring base. It uses also truly random number generator (TRNG). Even under very strong assumptions for Eve, (she has the same devices as Alice and Bob, has big computational power and the access to all critical points of the channel (excluding the emmision system from Alice and the detection system from Bob, which are the basic assumptions of quantum cryptography), Magic-QPN provides unconditional (information-theoretical) security, which is the strongest known type of secure communication [19].

Since Eve is forced to randomly select a basis, she will put an error into the transmitted photons. Alice and Bob verify the integrity of a quantum channel by detecting randomly chosen subset of the key and they check the rate of errors using a public communication channel. The presence of an eavesdropper is easily detected by uncovering the increase in the error rate by at least 25%. More information quantity Eve gains, it creates proportionally more disturbance. Therefore, the probability that Eve will be detected by Alice and Bob will be higher. This is true for any kind of attack (including entanglement-based attack).

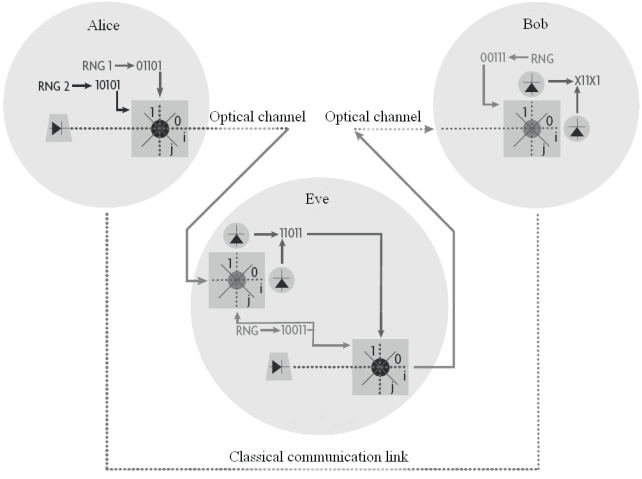
Beside eavesdropper, the main factor which contributes to bit losses in communication channel and to QBER at detection side is noise (in our case-optical). It is well established fact in quantum information theory

that (if the level of noise in the channel is reasonable) the noisy channel could be approximated with the noiseless (at the price of slightly higher BER). Noise has ambigous role in quantum cryptography. On one side, it is very frequent problem for Alice and Bob to discriminate between noise and the eavesdropper. This fact the eavesdropper can use to remain undetected. On the other side, noise prevents eavesdropper to read perfectly from noisy channel [1]. Beside that, noise can help key establishment phase (5.6.2. and 5.6.3.) in a way that it increases secret key space (the secret key rate).

Finally, it can be stated that mentioned Magic-QPN system satisfies all conditions for successful contemporary cryptosystems:

1. It is immune to any known mathematical algorithm
2. It has relatively high rate of key-reusage (integrity)
3. It is able to detect adversary with high probability, due to no-cloning theorem (availability)
4. The length of the secret key should be long enough comparing to the length of the message (confidentiality)
5. It will catch up with trends in technology (lack of perfect single-photon sources Magic-QPN compensates with the frequency of key reusage and its ability to perform error correction and privacy amplification in real time).

Figure 3. Diagram of Magic-QPN QKD system with the eavesdropper



Conclusion

The objectives of this paper are the following:

- Interpretation of the quantum theory of information,
- Description of a quantum coding scheme,
- Complete analysis of BB84 quantum protocol,
- Implementation of the complex communication system in real scenario.

Complexity is one of the main themes in information study and that makes the role of complexity theory important for research of information entities.

Quantum cryptography, which demonstrates the use of complexity, currently represents the greatest achievement of the quantum information technology. On the other hand, it is thought that the quantum information theory stands for the generalization of classical information theory, with significant improvements it has made in the areas of the current application of the information theory, and with applications in areas which are completely new for the classical theory of information.

This publication presents critical review of physical processes on which information technology of the future could be based. It explains the importance of complexity theory in telecommunication. Futhermore, this paper points out the advantages that quantum properties have over classical ones for information processing tasks [21]. The paper considered the way how to implement these advantages in existing telecommunication infrastructure, showing in illustrative manner the first commercial implementation of quantum key distribution [15].

This paper also ellaborates on several themes of analysis of information. The information structure of quantum information unit (qubit) is well introduced along with the introduction of quantum mechanics and with the statement of generalisation of problems from classical towards quantum information theory. Communication complexity is defined in inductive manner (through examples), with conclusion that quantum algorithms offer (for specific, narrow class of problems) exponential advantage comparing to classical algorithms. From the point of view of finding an optimal code, quantum Huffman code emerged as a natural choice, with significantly better complexity-theoretical bounds than corresponding classical. Finally, last chapter shows that combination between classical and quantum cryptosystem

provides higher level of security, keeping the same BER and obtaining higher bit rate for useful data at the price of adding only one optical fiber. Therefore, the publication has its contribution as a recommendation how the communication systems can improve both security and average performance (speed), at the price of negligible efficiency cost [21].

The information transmission methodology used in this paper is based on single-qubit transfer and no-cloning theorem [21].On the other side, actuall information technologies require enatnglement-based quantum cryptography. Therefore, there is a need for better laboratory conditions in our region, which would enable coherence between theoretical and experimental results and development of the prospective area of quantum cryptography.

Authorship statement

Author(s) confirms that the above named article is an original work, did not previously published or is currently under consideration for any other publication.

Conflicts of interest

We declare that we have no conflicts of interest.

References

[1] Assis, F., Stojanovic, A., Mateus, P. & et al. (2012). *"Improving classical authentication over quantum channel"* ISI journal Entropy.

[2] Barnum, H., Fuchs, C.A., Jozsa, R. & et al. (1996). *Phys. Rev.* A 54, 4707.

[3] Bennett, C.H. & Brassard, G. (1984). "*Quantum Cryptography: Public key distribution and coin tossing",* in Proceedings of the IEEE International Conference on Computers, Systems, and SignalProcessing ,Bangalore, p. 175.

[4] Bennet, C. & Brassard, G. (1989). *The dawn of a new era for quantum cryptography: the experimental prototype is working.*

[5] Cleve, R. & Divincenzo, D.P. (1996). *Phys. Rev.* A54, 2636.

[6] Cover, T.M. & Thomas, J.A. (1991). *Elements of Information Theory* (Wiley, New York).

[7] De Wolf, R. (2001). *Quantum Computing and Communication,* Complexity PhD thesis.

[8] Deutch, D. (1985). *Quantum theory, the church-turing principle and the universal quantum computer*.

[9] Kobayashi, H., Le Gall, F., Nishimura, H. & et al. (2010). *Perfect quantum network communication protocol based on classical network coding*, IEEE conference.

[10] Jozsa, R.J. (1994). Mod. Opt. 41, 2315.

[11] Jozsa, R. & Schumacher, B. (1994). J. Mod. Opt. 41, 2343.

[12] Kremer, I. (1995). *Quantum Communication,* Master Thesis.

[13] Kushilevitz, E. & Nisan, N. (1995). *Communication Complexity.*

[14] Magic Technologies. (2004). *Quantum Information Solutions for real world.*

[15] Papadimitriou, C., Dasgupta, S. & Vazirani, U. (2006). *Algorithms* McGraw-Hill, September.

[16] Schumacher, B. (1995). Phys. Rev. A51, 2738.

[17] Schumacher, B. (1994). Presentation at Santa Fe Institute.

[18] Shannon, C. (1948). Mathematical Theory of Communication. *Bell System Technical Journal.* 27 (3): 379–423.

[19] Shor, P.W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring" *Proc. 35th Annual Symposium on the Foundations of Computer Science*, p. 124 Edited by S. Goldwasser (IEEE Computer Society Press, Los Alamitos, CA.

[20] Stojanovic, A. (2009). The impact of quantum phenomena on complexity of communication systems MSc thesis, faculty of electrical engineering, Belgrade.

[21] Wootters, W.K. & Zurek, W.H. (1982). *Nature* 299 802.

[22] Yao, A.C.C. (1979). Some complexity questions related to distributive computing. In Proceedings of 11th ACM STOC, pages 209–213.

Internet source

[23] http://en.wikipedia.org/wiki/One-time_pad.

Submitted: November 19, 2012.
Accepted: May 16, 2013.