ICIT 2015 The 7th International Conference on Information Technology
doi:10.15849/icit.2015.0033 © ICIT 2015 (http://icit.zuj.edu.jo/ICIT15)

Quantum Information Technology: Novel Way for Increase of Sensory Systems Capability

Paata J. Kervalishvili

Department of Engineering Physics, Georgian Technical University, Tbilisi, Georgia

Abstract – **In the last decade quantum information theory and technology evolve and show their great potential. There are a set of problems for which it's more efficient and even not possible with classical communication to solve than with quantum equivalent. The best known example is Quantum Key Distribution (QKD), though there are quantum non-locality (entanglement), quantum teleportation, communication complexity and many more. The quantum information technologies permit by using quantum representation of data, to collect much bigger, more varied and precise information, as well as quantum data bank creation, which can be effectively treated by usage of relevant quantum algorithms. For creation of quantum databases, two methods will be dealt with: One is based on quantum numbers usage for processing various parametrical values (attributes of data bank); next, the database will be presented as its quantum model. On the basis of quantum information technology approach the new methods of possible improvement of nano micro sensory systems effectiveness is discussing in the recent paper. Multiparametral and multifunctional nature of sensors and their networks was taking into account. Nano micro sensor systems integrate and interface multiple core technologies and related devices to implement a variety of functions. They can be implemented through scalable homogeneous, or heterogeneous hardware integration technologies, in order to advance the miniaturisation, functionality and reliability of the sensor, processor, actuator and communication functions. Power autonomy (consumption and supply) is a common issue. In the medium term, there is growing industrial interest to integrate nanosensors in smart (intelligent) microsystems, mainly due to an increase in sensitivity, device simplification and associated cost reduction.**

Keywords – quantum information, sesensory systems, swarm intelligence, qubit, data collection and processing

I. INTRODUCTION

Monitoring natural uncertain environment parameters is a complex task of great importance in many areas. The origin of the difficulty lies in the environment's dynamism, arguably representative of real world problems, which consists of a number of peaks of changing width and height and in diffuse processes [1,2].

For technological monitoring of environmental safety which should be conditioned by the large scale spatially distributed homogeneous or heterogeneous environment with dynamic diffusion processes the multi mobile sensor systems and reconfigurable wireless networks of distributed autonomous devices which can sense or monitor physical or environmental conditions cooperatively are very sufficient. Intelligent sensors and sensor networks have an important impact in meeting environmental challenges. Agents interact (communicate, coordinate, negotiate) with each other, and with their environment. Usually, in a multi-agent system, interaction dynamics between an agent and its environment lead to emergent structure or emergent functionality [3].

There are many applications for non-stationary problems in the sense that the global optimum value and the shape of fitness function landscape (by the moving peaks) may change with time. The task for the adaptive optimization algorithm in these environments is to find optimal results quickly after the change in environment is detected.

Conceptually speaking, monitoring can be realized by continuously collecting sensory data from a distributed network of stationary or mobile Intelligent Sensor Agents deployed in the field. The architecture of such system for environment monitoring may consist of both sensors (for complex environment monitoring) and mobile Intelligent Sensor Agents, a wireless communication network [4].

Integrated sensory system is possible to treat as an information channel between the environment and the automated monitoring and mapping distributions. The development of a new range of sensor materials, effective sensors and sensory systems (networks) united in artificial intelligence techniques can achieve the necessary capabilities to provide quantitative information as well as alarm functions. Sensor networks consisted of a small number of sensor nodes that were wired to a central processing station. Sensor networks have a variety of applications. Examples include environmental monitoring – which involves physical or environmental conditions, habitat monitoring (determining the plant and animal species' population and behavior), seismic detection, military surveillance, inventory tracking, smart spaces, etc. In fact, due to the pervasive nature of micro-sensors, sensor networks have the potential to revolutionize the very way we understand and construct complex physical systems [5].

However, nowadays, the focus is more on wireless, distributed, sensing nodes. Multiple roles can be

This paper was prepared in the framework of the EU projects: SENSERA and SECURE R21

distinguished: Sensors – measure physical phenomena, sources of measurement data; Base stations – analyze and post-process data, sinks for measurement data. Actuators – perform actuation in response to received data; Processing elements – pre-processing of transmitted data.

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental condition, and to cooperatively pass their data through the network to a main location. The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. On the other hand, we can distinguish also two kinds of nodes: Aggregator and Device or Sensor/Actuator.

Area monitoring is a common application of WSNs. In area monitoring, the WSN is deployed over a sensor field where some phenomenon is to be monitored. When the sensors detect the event being monitored, the event is reported to one of the base stations, which then takes appropriate action. Sensor nodes can be imagined as small computers, extremely basic in terms of their interfaces and their components.

The base stations are one or more distinguished components of the WSN with much more computational, energy and communication resources. They act as a gateway between sensor nodes and the end user as they typically forward data from the WSN on to a server. The algorithmic approach to modeling, simulating and analyzing WSNs differentiates itself from the protocol approach by the fact that the idealized mathematical models used are more general and easier to analyze.

To better support high quality monitoring, we propose to enhance the sensor network with mobile swarms. A ”swarm” is a group of nodes which are physically close to each other and usually share the same mobility pattern [6].

Swarm intelligence is an exciting new research field still in its infancy compared to other paradigms in artificial intelligence. Particle swarm optimization algorithms (PSO) have gained popularity in recent years. PSO is a population-based method, a variant of evolutionary algorithms with moving towards the target rather than evolution, through the search space. In PSO algorithm, the problem solution emerges from the interactions among many simple individual agents called particles [7].

The movements of the particles around in the search-space are guided by their own best known position in the search-space as well as by the entire swarm's best known position. The improvement of positions is a necessary condition to guide the movements of the swarm. The gradient of fitness or cost function, which must be optimized, is not known. The goal is to find a solution in the search-space, which would mean is the global optimum. The process is repeated and by doing so it is hoped, but not guaranteed, that a satisfactory solution will eventually be discovered.

II APPROACH TO QUANTUM INFORMATION TECHNOLOGY METHODS

Nowadays information processing is fundamentally studied with classical approaches; the latest improvements in this direction use existing explorations and no significant breakthroughs are observed. The explanation of such difficulties lies under the natural limitations to which we are already close enough. Our progress barely satisfies our needs, for we are reaching the edge of existing paradigms; consequently, we seek for novel approaches of information processing. Information processing methods based on quantum mechanical phenomenon is believed to be closer to nature, which promises to open a whole new world of opportunities. Moreover, emerging technologies use nano and sub-nano scales, where quantum mechanics comes into play, and we can't ignore its influence on the computing process and we see information processing based on quantum approaches as the future of information science [8,9].

The main actor in quantum system – the main unit for saving information- is called quantum bit or qubit. Qubit exists simultaneously in two states, and there is certain probability to measure qubit in classical state 0 or 1. After measurement, we lose the superposition and from all possible states we get just 0 or just 1. To take advantage of this property, we must operate on the qubits as long as needed and measure them only at the end because operating saves the superposition. We have restrictions on the types of operations; every operation should be reversible (intuitively it's easy to understand that quantum operations are reversible because there is no lost of information and we always can go back, reverse the process), but measurement is irreversible and all irreversible operations collapse the superposition. Furthermore, no cloning theorem tells that every particle in the universe has its own unique state. We can't fake it (nature seems to forbid making an exact copy of something). We can't hide the information a particle contains; it's somehow represented into its unique quantum state, so this can be used to detect false. It's awful if we would think about spreading information, but from the security point of view it gives novel opportunities [10].

The outline of this problem includes: a) Quantum computation (QC) – quantum bit (qubit) and entanglement; – problems in experimental realization of QC; b) Spin-based QC – nuclear spin and electron spin in semiconductors as qubits. A challenging problem is to use the reach world of correlations in quantum systems in a controllable manner to process information [11].

A quantum particle with two steady state levels can be used as a quantum bit $\equiv$ *qubit*

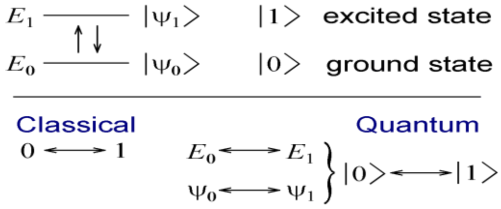

E_1 $|\psi_1\rangle$ $|1\rangle$ excited state
E_0 $|\psi_0\rangle$ $|0\rangle$ ground state
Classical
$0 \longleftrightarrow 1$
Quantum
$E_0 \longleftrightarrow E_1$
$\psi_0 \longleftrightarrow \psi_1$
$|0\rangle \longleftrightarrow |1\rangle$

Fig.1. Examples:
- ground and excited states of an atom;
- vertical or horizontal polarization of a single photon;
- superconducting and normal state; - spin 1/2 particles in a magnetic field.

Classical bit can represent at the moment either 0 or 1. Most general qubit state is a superposition of two basic states:

$$|\psi_1\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\alpha^2 + \beta^2 = 1$$

For two bits there are four possibilities: 00, 01, 10, 11. In contrast, two qubits are in general in a state of a form

$$|\psi_2\rangle = a|00\rangle + b|01\rangle + c|10\rangle + d|11\rangle$$

$$a^2 + b^2 + c^2 + d^2 = 1$$

Qubits in this state display a degree of correlations impossible in classical physics. This phenomenon is called entanglement and is a crucial property for the success of quantum computing.

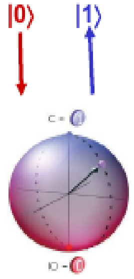


Fig.2. The general state of N qubits is specified by a 2^N- dimensional complex vector.

The main requirements for the implementation of a quantum computation are:

1. A scalable physical system with well characterized qubits: Two-level systems - spin 1/2 particle in a magnet field where one is ground and excited states of an atom, the second – superconducting and normal state.

2. Long relevant decoherence times: at least 10^4-10^5 times longer than the gate operation time.

This is necessary for successful application of the quantum correction procedure

3. The ability to initialize qubits to a ground state, such as $|000\ldots\rangle$: registers should be initialized before the start of computation.

4. A “universal” set of quantum gates: two-qubit interactions: CNOT (control not) or SWAP gates (universal quantum gates).

5. A qubit-specific measurement capability: the result of computation must be read out.

Among many suggestions for realizing the basic unit for Quantum Computation, the most exciting avenue is using spin-1/2 particles (electrons, some nuclei) embedded into a semiconductor device which allows to utilize the tremendous resources of silicon based industry for scalable fabrication technology [12].

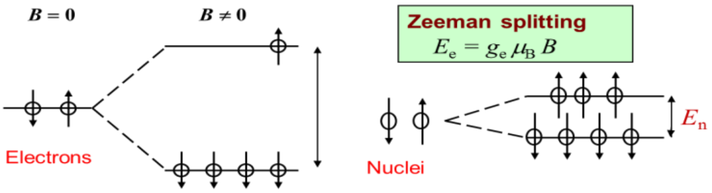


Fig.3.Candidate for a qubit needs phase coherence during quantum com

In the last decades our perception of the world has changed. We are more involved in distant and shared tasks, and it's natural to seek new ways to improve communication. As quantum information theory evolves and shows its great potential, why not try and take these advantages and make communication better.

Quantum communication refers to a process of transferring qubits from Point A to Point B at distance. There are a set of problems for which it's more efficient and even not possible with classical communication to solve than with quantum equivalent. The best known example is QKD, though there are quantum non-locality (entanglement), quantum teleportation, communication complexity and many more [13].

Quantum communication relies on some phenomenon like entanglement which gives plenty of opportunities, but at the same time it's very tricky. When Einstein first saw this phenomenon (EPR – Einstein-Podolsky-Rosen paradox), he said that it was incompleteness of quantum mechanics. For today, we know more about this phenomenon; still we have a lot to explore in this direction Present knowledge lets us define entanglement as a property of quantum system when two or more objects are linked together (their quantum states) and you can't refer to one without referring to the others, so if you measure one, others are determined as well. If we define communication in qubit terms, every qubit has its own channel to transmit state, but sometimes it happens so that two or more qubits are entangled and share the channel which means they communicate between each other. The result of communication is the “immediate” transmission of one of the qubit’s state to others [14].

The medium that provides the communication is unknown for today. It can be said that it is some sort of field. It is important, that this field fills the space and even more - the communication is not based on light speed, which means either the distance does not reflect on the communication time or it reflects less.

Still, we try to use what we know about entanglement, and we came up with a strange communication scenario which we call quantum teleportation. But if you look closer, it’s nothing that special.

Quantum teleportation is a great proof of entanglement’s power. Quantum teleportation is a process when an object’s quantum state dissolves here and reappears at a distance without ever existing at any intermediate location. Process can be executed as a three step sequence (Fig.4).

First an entangled pair of qubits are prepared and distributed, then the sender performs a so called Bell-State-Measurement (BSM) between entangled qubit and qubit to be teleported and sends measurement result to receiver via classical channel. Note that BSM provides nothing about the teleported qubit's state, but contains something about how the two are related (entangled and teleported qubits), and this information is infinitely smaller than classical description of teleported qubit's state. At the end, based on BSM results, the receiver makes result-dependent unitary rotation to his/her system to recover qubit state. So as we use the classical channel to communicate, we are limited with the speed of light and physical implementation (with linear optics) of BSM is not as efficient as needed [15].

Communication complexity refers to the number of communications required to solve a distributed task. For example if A and B points (separated in distance) have their own input x and y and want to calculate some function f(x, y), what would be the minimal amount of information exchange (communication) for problem to be solved?

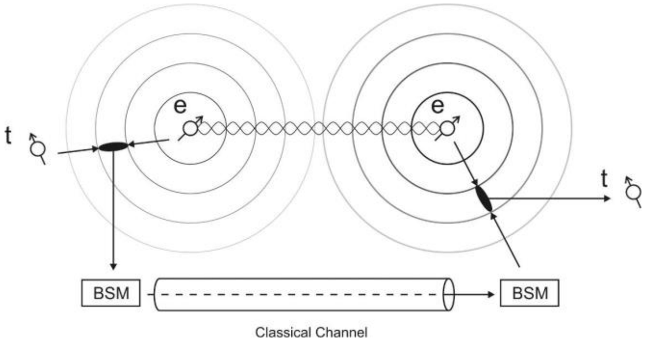


Fig. 4 Visual representation of teleportation: t – Qubit to be teleported; e – Entangled qubits; BSM – Bell-State-Measurement result.

Quantum superposition phenomenon plays a significant role in Quantum Algorithms. There are also some limitations but generally quantum algorithms are more advanced than classical ones. The most important advantage is the possibility to maintain all of the states simultaneously during the process. Theoretically it gives us the exponential power of quantum computer, but for today there are many technical and principal problems, which limit us to implement quantum algorithms [16].

III QUANTUM TECHNOLOGY METHOD OF SENSORY SYSTEMS DATA COLLECTION AND PROCESSING

Environment condition data collection process usually is managed by the different methods and devices (which determine the types of data) are used [17]. These methods might be divided as:

1. Standard measurement methods – sensors and sensory systems which are measuring the various physical and chemical parameters; data bank is inflated / significantly increased by these common and other standard data .
2. Semantic description (estimated texts) – collection of information represents the unstructured data coming from sensory systems. For their valuable use semantic analysis is necessary as well as the structuring of data knowledge taking from estimated texts and performing another range of tasks.
3. Description by multimedia sensory systems (photo and video clamping, audio recording) – the process is mainly dedicated to image recognition and may have a large range of complexity (Fig.5)

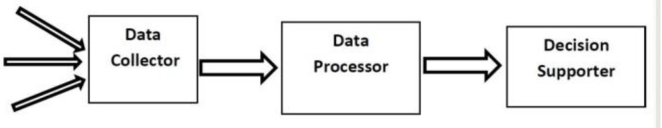


Fig.5. General scheme of the modeling process

Let us stay at the first method. In predicting the consequences of certain actions or events, various models play a crucial role. The key of simulation of the model for any purpose is determination of its tasks and targets.

Data collection is one of the most important parts of the model successful functioning. Quantum approach for optimization of the use of databases can give to us at least two positive effects: 1. The compact representation of the database; 2. The possibilities to reduce the processing time.

It is well known in computer science the representation of the three main types of data: real-valued, integer or Boolean. These types reset all data that belongs to the type of class one (Classes of data type): primitive data types (machine data types, Boolean type, numeric types); composite types (enumerations, string and text types); other types (pointers and references, functional data types, abstract data types; utility types).

Primitive or composite data types are used in the models describing the data of disaster types. This depends on two main factors: 1. Data source and 2. Model representation of type Boolean (logical), an integrated, causal, and the others.

Any type and scale of the disaster we can imagine, as it is a big system. One characteristic of this kind of systems that are used to describe the condition of many and varied attributes and, in addition, may consist of many smaller ones define the subsystems. For example, if the object of our study is earthquake, earthquake could lead to flood or landslides [18]. Therefore, we have at least two different and mutually dependent systems, which at the same time could be described by a separate model.

The parameters of each of this kind system are divided into descriptive qualitative parameters (include only content definitions), quantitative parameters (include only discrete or continuous quantitative parameters) and mixed parameters (include quantitative and qualitative parameters all together). In the real situation when disaster is mixture of different systems of parameters it is very important to use a method where all types of data are in the form of inference and therefore there are no information loss and all these can be used in a single model. Let us represent a generalized notion of the catastrophe. To observe the different disasters jointly because of the reason of their high individuality is not always possible [19].

Let us admit that we have S a big system, and its describing parameters are:

$$x_i \in \{P\} \cup \{C\} \cup \{A\}, i = 1, \dots, N ,$$

the abundance of (where N is the description of the parameters of the points, {P} - Primitive data type, {C} - Composite data type, {A} - Abstract data type) model is essential to reducing the effectiveness of the same type. Type depends of the chosen model. In our case, all parameters are reset to the quantum dimension of the quantum value.

We can perform the transformation process in two stages: 1. Unification of logical presentation of data from the census; 2. the quantum representation of parameters.

In the first step, for each parameter there is a discrete set of values, which contains much of numeric values [20], contextually described in non-overlap range. The question is; how many different values can be fixed when we describe the S system, which was adopted by the International grading system describing or defining the level of threats. This number can be different for each parameter. As a result, we get the allowable values for each parameter draws x_i domain:

$$x_i \in \{x_i^1, x_i^2, \dots, x_i^{n_1}\},$$

where n_i is equal to x_i a number of different meanings .

In case that we have the S system description in the generalized form we could say that the description of the observed x_i is the main option or not. In some cases, different it is important first to analyze the existence of zero in the option. In this case the quantum x_i performance is used.

Assume that x_i is a quantum imagination of the system, which can be represented as $|x_i\rangle$ and the state of a quantum system $|x_i\rangle$ is a vector in a complex vector space (Fig.6). If the state of a quantum system $|x_i\rangle$ is a vector in a complex vector space and the set of vectors $\{|n_i\rangle\}$, $n_i = 0, \dots, N-1$ (where N may be ∞) has an orthonormal basis, for this space we can always express

$$|X_i\rangle = \sum_n c_n^i |n_i\rangle$$

for some complex coefficients c_n^i, where $\sum_n |c_n^i|^2 = 1$.

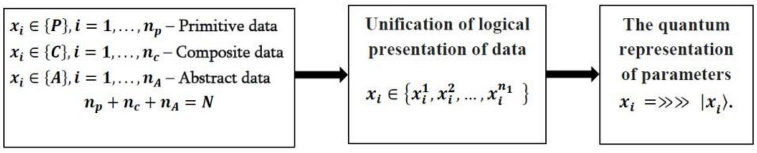

$x_i \in \{P\}, i = 1, \dots, n_p$ – Primitive data
$x_i \in \{C\}, i = 1, \dots, n_c$ – Composite data
$x_i \in \{A\}, i = 1, \dots, n_A$ – Abstract data
$n_p + n_c + n_A = N$
Unification of logical presentation of data
$x_i \in \{x_i^1, x_i^2, \dots, x_i^{n_1}\}$
The quantum representation of parameters
x_i =»»» $|x_i\rangle$.

Fig.5. The data transformation process.

According to the parameters of each presentation of each x_i $x_i^j, j = 1, \dots, n_i$ meaning we can write: c_j^i ratio. This form will be modified according to our data base for further processing [21].

In the point of view of data processing, we see two approaches: 1. Quantum information processing classical quantum algorithm (mainly meant to search), and 2. Data processing system S is used to describe and convey it by the quantum concepts.

Grover's algorithm for quantum calculations is one of the most important tool, which helps to describe not well defined N=2^n elements in the database (a database handle disasters) of a particular element search. This algorithm makes possible to compute the many unsolved problem of classical calculations [22]. Using classical methods in the theory of probability, we can say that for any m element inspection the probability that a request for records with equal m/N. It is clear that the database needs to be $O(N)$ =2^n for the necessary elements to look for. Using the Grover's algorithm the necessary number of requests (steps) is $O(\sqrt{N})$ =$O(2^{\frac{n}{2}})$

In our case, we may give to the task such formalization: S is used to describe the system of $N=2^n$ From the each of the values S_1, S_2,… S_n, there is a unique situation, which

doi:10.15849/icit.2015.0033 © ICIT 2015 (http://icit.zuj.edu.jo/ICIT15)

satisfies the condition: $f(s_u)=1$ is only one element $s \in A$, and $f(s)=0$ for all other elements. We can make such a formulation of the problem, because we have already reduced our options to quantum face.

As mentioned above, we use the S parameters for description of the $x_{i,} i = 1, \dots, N$. In concrete case presentation these parameters reducing to the quantum face. Suppose we have a different system in *K S* Description. Each description we can write as quantum implications:Where

$$|\widetilde{x_1}\rangle \& |\widetilde{x_2}\rangle \& \dots \& \overline{|x_N\rangle}$$

$$|\widetilde{x_i}\rangle = \begin{cases} |x_i\rangle \; \textit{description of the S system ;} \\ \overline{|x_i\rangle} \; \textit{no description of the S system.} \end{cases}$$

Therefore we have *K* implicants. Write a realization in dysfunctional normal form: $\bigvee |\widetilde{x_1}\rangle \& |\widetilde{x_2}\rangle \& \dots \& \overline{|x_N\rangle}$

If we minimize this form following the method which it is shown in [23], as result we will receive S system describing quantum concept in a generalized form. This description is compact and contains only those parameters that are most important to a particular kind of system evaluation. Its use will enable to evaluate the system not only by quantitative parameters, but options of all of them.

Quantum algorithms (especially Shor's) prove that quantum approaches are more flexible than classical in complex environments like the sensory network (when process goes exponentially). So we can say that our tool-set of information processing (brain) must be minimum quantum, as far as we know, because Devo (development evolution) have chosen us as leading creatures.

Shor's algorithm have suppressed any hope that encryption base on discrete logarithm (factoring large numbers) can be resistant against quantum computing, so we have to replace asymmetric encryption algorithms with novel quantum approaches. Though it was proved that symmetric algorithms perform quite well in quantum environments, similar approaches do not give effective use in quantum asymmetric world. Instead of pure asymmetric key distribution there are some thoughts about quantum asymmetric cryptography using entangled key pairs. This approach effectively uses the physical security of channel, so to estimate private key with high probability eavesdropper needs large amount of public keys. The disadvantage of this approach is the need of trusted issuer of keys, who generates private and public key pair and sends it to authenticated users securely [24].

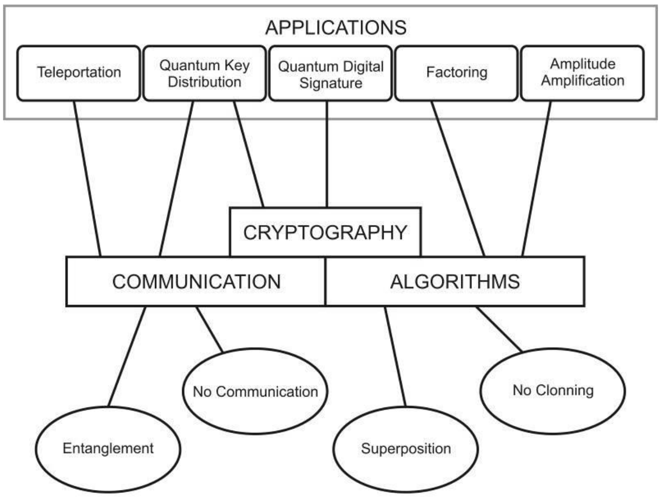
Suppose eavesdropper reads quantum state in channel without collapsing superposition. QKD uses quantum channel to negotiate the key, after that encrypted data is sent via the classical public channel. The security of this method will become vulnerable if quantum reading without losing superposition is possible. The next advancement of attack on quantum channel is to get the information with about the same probability as the receiver. One of the known attack modes includes man-in-the-middle attack at any point in QKD. The reliability of QKD is based on encoding the information in non-orthogonal states. Quantum indeterminacy means that these states cannot be measured without disturbing the original state. However, if we read superposition without collapsing it, then we would be in the same state as actor A, thus if man-in-the-middle attack continues, we can get the key generated using QKD.

If we assume that reading qubit is possible with certain (high) probability and the eavesdropper can easily access information sent by quantum channel, the need of different approach arises. One protection against such attack is the use of entangled qubit pairs as key. The sender generates entangled registers (sequence of qubits) and sends one of them via quantum channel. The eavesdropper can successfully read this information but after the receiver receives it, sender operates the entangled register on his/her side and in that way sets a key, which is also accessible to the receiver but is unknown for the eavesdropper. After that, encryption and decryption happens with entangled keys. If we assume that entanglement could not be intruded by a third-party, then this scheme is unconditionally secure.

Let's take n-bit qubit and apply some algorithm on it. After performing the main algorithm quantum register is in superposition of all possible states. The goal is to find the solution, that is one of the $N = 2^n$ states. Let's take the simple model to describe amplitude amplification. The best example should be uniform superposition that contains every possible state with the same amplitudes (coefficients) and the sum of the squares of amplitudes is 1. The solution we are interested in is one of them, but if we measure the register, the probability of getting solution is 1/N. We could try again and again, but which one would be a solution is unknown, so we can't effectively find the answer without changing the coefficients. This is the case where amplitude amplification comes into play. We use the "oracle", which changes only the solution's amplitude. Applying oracle on qubit result in the change only in the solution's amplitude; specifically, it gets a minus sign, so the probabilities (square of amplitudes) remain unchanged. After that the amplitudes are inverted against the mean of amplitudes; consequently the solution's amplitude is raised and the other amplitudes are lowered. The reason this happens is that only the solution has negative amplitude which is less than the mean, and all remaining amplitudes are more than the mean. The above described steps make one iteration of Grover's algorithm [24]. When we apply Grover's algorithm, we change the amplitudes iteratively, so that on every iteration the amplitude of solution is changed. This process is periodic. Not every iteration will raise the amplitude. To be more specific, within

$$r \approx \frac{\pi}{4}\sqrt{N}$$

steps the amplitude is increased, but on r+1 step, amplitude begins to decrease. This means that we need r iterations to get maximum possible amplitude effectively. The complexity is sub-linear and is O($N^{1/2}$) which is better to simply repeat the main algorithm several times and analyze measured results to "guess" which result is solution. There is one interesting detail about the oracle. Oracle is represented as a matrix which contains "1"-s on the diagonal except one element which is related to the solution and is "-1" and all other elements are "0". In the real world, we don't know where that "-1" is, because if we knew, we also would know the solution itself. The oracle hides the solution in itself; we just can use it to increase the probability of measurement.



Finally, it's worth mentioning, that finding the quantum solution is more effective if the states are unstructured and unsorted because in sorted cases there are no significant differences between classical and quantum algorithms. So, Grover's algorithm is used for searching the solution that is already mixed in the superposition of quantum register; more generally it's useful for searching one particular element in an unsorted, unstructured set. This algorithm is also expanded to search for multiple solutions in the superposition, but this is beyond our scope [25].

Applications we have reviewed, we think are ready for mainstream after implementing the quantum computer. The approaches that lie under these applications use quantum properties (Fig.5).

Fig. 5 Quantum Approaches and its applications.

Cryptography has always been an important part of information theory. A lot has been done in classical cryptography. Two main types of algorithms are known – symmetric and asymmetric. Symmetric algorithms are widely used for securing communication between two parties (e.g. A and B) and asymmetric are used for digital signatures. Both of them have their advantages and disadvantages, but we will discuss classical cryptography only in order to explain quantum cryptography. Security in classical cryptography was based on the exponential number of computational calculations, which was not achievable in real time, needed to decrypt encrypted message. As we have seen, quantum computing offers us exponentially more computing power than classical analogy. Due to that, many algorithms which were thought to need years to break the key, need no more than minutes with the help of quantum computation. But that will be done after the quantum computer is built. Until quantum cryptography can help these problems, it solves classical cryptography's weak issues. Quantum cryptography is mainly known for quantum key distribution (QKD) which solves the weakest point of classical symmetric algorithms- key distribution [26]. Despite this fact, integration in classical cryptography is essential because QKD only generates and distributes keys over two parties which then can use this key with any classical encryption algorithms.

The idea of QKD algorithm is the following:

We begin with the first stage, the transmission of the photons, which is the physical representation of qubits, from A to B. Afterward the communication switches to the public channel. There, the first phase is the shifting phase, where A and B negotiate which bits are used and which bits are discarded. To avoid a man-in-the-middle attack by C, this message exchange must be authenticated. After agreeing on the bits and being sure that C has not modified messages by using an authentication scheme, A and B go on to the reconciliation phase or error correction phase. Due to the fact that quantum channel is not a noiseless channel, A and B do not share the same identical string. There is a small portion of errors in B's string, which are corrected in this phase. Again, C has the possibility to modify messages during this phase to his/her interest. Therefore, A and B must authenticate this phase. Passing reconciliation, A and B share a string, which is identical with a very high probability. But this string cannot be used as a key yet. C's information about the string must be considered.

As we can see QKD is limited in distance, because in the first part we send qubits via quantum channel. Due to this fact, no cloning theorem and no repeaters can be used as in classical communication. This type of algorithm is unconditionally secure if several simple conditions are met:

1. Eavesdropper cannot access A's and B's encoding and decoding devices
2. The random number generators used by A and B must be trusted and truly random (for example a Quantum random number generator)

3. The classical communication channel must be authenticated using an unconditionally secure authentication scheme

Despite this fact QKD has been broken, but not because of the algorithm but due to the non ideal behavior of the present-day quantum cryptographic hardware [27].

As for asymmetric algorithms some theoretical advancement is present. Nothing has been done in practice because asymmetric quantum algorithms require quantum technology beyond today's advancements.

Quantum digital signature algorithm is already available.

Quantum digital signature shares a lot with classical analogy. Requirements for good and usable signature schemes for classical and as well as for quantum are underlined:

1. The scheme has to provide security against tampering by: - The sender after the message was signed; -The receiver; - A third party
2. Creating a signed message has to be easy
3. Every recipient has to get the same answer, when testing the message for validity

Differences between classical and quantum signatures are based on quantum information nature.

IV Conclusion

This work was motivated by the idea of developing the high effective sensory systems monitoring of environmental pollution, particularly in nuclear power engineering, which can be realized by continuously collecting sensory data from a wireless mobile sensor network deployed in the field [28]. The relevance of problems is particularly pointed out by the environmental dynamism of the shape of fitness function landscape, which consists of a number of peaks of changing width and height and in diffuse processes. We have discussed the quantum algorithms as effective tools for the adaptive control of the mobile sensory system .

We also discussed the quantum approach of sensory data collection and processing using some quantum information technology methods and tools.

Present knowledge lets us define entanglement as a property of quantum system when two or more objects are linked together (their quantum states) and you can't refer to one without referring to the others, so if you measure one, others are determined as well. More than that, no matter how far they are (physical separation), measurement occurs instantly, faster than the speed of light. It's like an instant communication which would be great, so that we could reduce the dependency on distance, but unfortunately lack of knowledge does not allow us to realize its potential. Inside the quantum world, entanglement is some sort of communication because the separated states depend on each other or have a connection.

Taking into account the quantum and multi parametrical nature of information for its clear and precise modeling it is possible and effective to combine two methods, where one is based on quantum numbers usage for performing of different parametrical values (transferring logical numbers to quantum numbers), and second - to creation of the data base (quantum date base) which should be presented as its quantum model. These approaches jointly with quantum search algorithms and quantum query algorithms are opening the new ways for creation of novel technologies for modeling and creation of novel high effective sensory systems and networks.

References

[1] M.Roza, J.Voogd, D.Sebalj, "The Generic Methodology for Verification and Validation to support acceptance of models, simulations and data". The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology October 2013 10: pp. 347-365

[2] P. Kervalishvili, B. Meparishvili. "Synergy, entropy and sustainable development". Georgia Chemical Journal, vol.10, N 4, 2010, 169-173.

[3] P. Kervalishvili, B. Meparishvili, G. Janelidze. "Adaptive control of mobile information system". NATO Science series, IOS press, v.93, 2012, 100-108.

[4] Luís M. L. Oliveira and Joel J. P. C. Rodrigues ."Wireless Sensor Networks: A Survey on Environmental Monitoring," Journal of Communications. Vol. 6, no. 2, April 2011.

[5] Wilson, D.M. S. Hoyt, J. Janata, K. Booksh, and L. Obando, "Chemical Sensors for Portable, Handheld Field Instruments." *IEEE Senso rs J.*, Vol. 1, No. 4, 2001, 256-274

[6] K. E. Parsopoulos, M. N. Vrahatis. "Particle Swarm Optimization and intelligence: Advances and Applications." Published in the United States of America by Information Science Reference. Hershey, New York ISBN 978-1-61520-666-7, 2009.

[7] Y. H. Shi, and R.C. Eberhart, "Empirical Study of Particle Swarm Optimisation," Proceedings of the Congress on Evolutionary Computation, (Washington D.C. USA), IEEE Service Centre, Piscataway, NJ, 1995, 1945-1949.

[8] P. Kervalishvili. "Philosophy of quantum information science". NATO Science series, IOS press, v.93, 2012, 55-73.

[9] P. Kervalishvili. *"Quantum Information Science*: Some Novel Views." In Book *Computer Science Technology* an Applications. Nova Science Publishers, Boston, USA, ISBN: 978-161324-870-6, 2011.

[10] Alexander Holevo. *"Quantum Informatics."* Science World (Scientific American - Rus.), No7. 2008.

[11] Paata J. Kervalishvili. "Development of Quantum Information Technology based on nuclear spin qubits". The Eighth Japanese-Mediterranean Workshop on Applied Electromagnetic Engineering for Magnetic, Superconducting, Multifunctional and Nanomaterials

(JAPMED'8), book of abstracts NCSR Demokritos, 24-26 of June, 2013, Athens, Greece.

[12] B. Kane, "Si-based nuclear-spin quantum computer", Nature 393, 1998, 133.

[13] A. Liang, V Scarani., J. G. Rarity, J. L. O'brien, 2010. Reference Frame "Independent Quantum Key Distribution". Centre of Quantum Photonics, University of Bristol, U.K. Centre of Quantum Technologies and Department of Physics, National University of Singapore, Singapore, arXiv:1003.1050v1

[14] C. H. Bennett. "Notes on the History of Reversible Computation". IBM J. Res. Dev. Vol. 44. No ½, Jan.-March. 2000.

[15] Nicolas Gisin,and Rob Thew, "*Quantum Communication"*, Group of Applied Physics, University of Geneva, Switzerland, arXiv:quant-ph/0703255v1 2008.

[16] D. A. Meyer. "Physical Quantum Algorithms". UCSD preprint, 2001.

[17] D. Estrin, L. Girod, G. Pottie, M. Srivastava, "Instrumenting the world with wireless sensor networks." In Proceedings of the International Conference on Acoustics, Speech and Signal Processing (ICASSP 2001), Salt Lake City, Utah, May 2001.

[18] D. Pfeifer, J.Valvano, A.Gerstlauer. "SimConnect and SimTalk for distributed cyber-physical system simulation". SIMULATION, October 2013 89: 1254-1271.

[19] Paata Kervalishvili, Manana Khachidze. "Quantum Information Technology and Modeling of Disasters – A Prospective View". Presentation at the NATO Advance Research Workshop – ARW, Improving Disaster Resilience and Mitigation - New Means and Tools, Trends Jassy Romania, November,6-8 2013.

[20]Kazuo Iwama. "Quantum Search Algorithms for Database Query Processing". ERATO Quantum Computation and Information Project. September 6-8, 2001, Tokyo, Japan.qci.is.s.u-tokyo.ac.jp/qci/eqis/Iwama.ps

[21] Sudip Roy, Lucja Kot, Christoph Koch. "Quantum Databases". CIDR, 2013.

[22] Archuadze M., Besiashvili G., Khachidze M. and Kervalishvili P. "Knowledge Engineering: Quantum Approach", published in Philosophy and Synergy of information: Sustainability and Security, Publication is supported by: The NATO Science for Peace and Security programme Sub-Series E: Human and Societal Dynamic-, , vol.93 ISSN 1874-6268, 2012 pp.175-185.

[23] M.Khachidze, M.Archuadze ,G.Besiashvili "The Method of Concept Formation for Semantic Search". 7th International Conference on Application of Information and Communication Technologies., Baku, Azerbaijan, 23-25 October 2013.

[24] P. W Shor. "Algorithms for Quantum Computation: Discrete Logarithms and Factoring."in S. Goldwasser, ed., Proceedings of the 35th Symposium on Foundations of Computer Science, Santa Fe, NM, 20{22 November, Los Alamitos, CA: IEEE Computer Society Press 124{134, 1994.

[25] L. K. Grover, "A Fast Quantummechanical Algorithm for Database Search". in Proceedings of the 28th Annual ACM Symposium on the Theory of Computing, Philadelphia, PA, (New York: ACM 1996) 212{219, 1996.

[26] Fei Gao, Qiao-Yan Wen, Su-Juan Qin, Fu-Chen Zhu. "Quantum Asymmetric Cryptography with Symmetric keys", arXiv:0809.3408v2,2008

[27] L. Lydersen, J. Skaar. 2010. "Security of Quantum Key Distribution with Bit and Basi Dependent Detector Flaw.|" Norwegian University of Science and Technology, Trondheim, Norway, University Graduate Center, Kjeller, Norway, arXiv:0807.0767v4

[28] Paata J. Kervalishvili and Tamara M. Berberashvili. "Quantum Effects Based Nanosensory Systems". Black Sea Energy Resource Development and Hydrogen Energy Problems. NATO Science for Peace and Security Series-C; Environmental Security. Springer. 2013, pp.359-372.