Study on Actual Developments in the Field of Quantum Computing in Terms of Cyber Security and Physical Systems

Maria-Daniela IANCU
National Institute for Research & Development in Informatics - ICI Bucharest
daniela.iancu@ici.ro

Abstract: This paper deals with the concept of quantum computer, which describes the quantum algorithms, areas of use and weaknesses or strengths of quantum computing, cyber security and quantum circuits.

Keywords: Qubit, Quantum Algorithm, Combinatorics, Big Date, Artificial Intelligence, Quantum Computer, Cyber Security, Photonic Tubes, Qubit Matrix

INTRODUCTION

In the early 1980’s, the first theories emerged that indicated the possibility of performing quantum calculations. In 1985, the physicist David Deutsch published the article „Quantum theory, the Church-Turing principle and the universal quantum computer”, in which he described the first universal quantum computer. The famous American scientist Peter Shor defined the algorithm that bears his name, i.e. Shor algorithm. He proposed a system for correcting quantum computational errors.

In 1995, Benjamin Schumacher proposed the term „qubit”. Next, we have Lov Grover who invented the data search algorithm, the Grover algorithm. This is a probabilistic algorithm, and in 1997, the first practical experiments were performed to implement all the calculations. The first secure communication experiment using quantum encryption was successfully performed at a distance of 23 km and the first quantum teleportation of a photon was performed.

In 1998, Isaac Chuang and Mark Kubinec developed the first 2 qubit quantum computer, and in 2005 the first qbyte was created. The term quantum refers to quantum, a number that characterizes the energy level of a particle.

Machines that use the properties of quantum physics to store data and perform calculations...
that would take a very long time are called quantum computers.

This is a great advantage in completing tasks that even the most advanced computers could not solve. In classical computers, encoding is based on bits, respectively 0 and 1, and in quantum computers we have quantum bits or qubits. This basic unit of quantum memory was created with the help of physical systems such as the electron or spin. These quantum bits are connected by the phenomenon called quantum crossover, which results in the simultaneous representation of different things.

For example, to see a clear difference between a classical computer and a quantum computer, we take eight bits to represent any number between 0 and 300, but if we take eight qubits we could represent all the numbers at the same time. So we can assume that it would be possible to represent the atoms in the universe with the help of a few hundred qubits (Atzori, M. et al., 2018).

IBM has released the newest quantum chip measuring 127 quantum bits, but their goal is to create a 433-qubit quantum processor called the „Eagle” chip, and the next step is a 1,121-bit chip. „Condor” quantum. Figure 1 illustrates a chip made by IBM, the one we have referred to above (Chow & Gambetta, 2021).

![Quantum Processor -127 quantum bits](Chow & Gambetta, 2021)

In 2019, Google reported a quantum advantage with the help of manufactured qubits and superconducting loops. The problems solved were of an artificial nature, for real problems such as the simulation of drug molecules or various materials we need very powerful computers. For example, Australia believes that the 1,000 qubit chip would pay off.

The researchers opted for a hexagonal network with two or three neighbors to allow the qubits to interact with each other in order to solve engineering problems. They relied on the history of 3D architecture.

The processing power of a quantum circuit depends on several factors, such as strength and speed to be able to complete the calculation, overcoming random fluctuations. For quantum computers, the troubleshooting part is difficult, because the laws of physics do not allow the use of the necessary methods of error handling. In the future, other approaches to the construction of quantum computers may be
considered, which will benefit from the smallest possible errors.

One of the teams developing this process made a logical qubit, which consists of 13 quantum bits of trapped ions, and another team using 21 superconducting qubits obtained a similar rate. This result is important in order to correct errors.

In order to improve the signal-to-noise ratio, we try to detail the noise, and then extract it.

In order to have a functional quantum computer, we need to keep an object in an overlapping state as long as it is necessary in order to carry out the processes and achieve the objectives.

For example, in the following figure we have the first quantum computer that works with a 100 quantum bit processor.

![Quantum Computer](image)

*Fig.2: Quantum Computer (Ball, 2021)*

We need devices that can protect quantum states from decoherence, making them easier to navigate. These challenges are approached from various angles in order to find better ways.

There are mathematical researchers who believe that there are various obstacles that are virtually impossible to overcome. They could help by speeding up data processing, developing better forecasting patterns, and balancing more accurate alternatives. They could also help solve optimization problems, such as portfolio management risk, and of fraud. Cyber security is an ideal use case for quantum computing solutions, as cryptology is a very complex discipline.

### ALGORITHMS

In the last period of the last century, various theories of quantum mechanics began to appear to develop quantum algorithms. One of the oldest discoveries and also a very good justification for quantum calculus to date is Shor's algorithm for factoring integers into prime numbers.

In many cases, Shor's algorithm can be considered a starting point. Equally important are Grover’s quantum search algorithms. These algorithms were developed in the 1990s. Since then, several algorithms have been developed. Quantum computing has the potential to disrupt security by using these types of algorithms.
Quantum security solutions can destroy complex encryption systems, such as RSA encryption. RSA encryption is commonly used to protect sensitive data and online communications. Many organizations use RSA encryption to protect data that is sent over the Internet. For example, crypto-agile technologies and secure quantum cryptography are now being proved to enable a seamless, convenient, and cost-effective transition to new cryptographic standards to protect key customer assets.

In order for the algorithms to run in the most efficient and controlled way possible, the quantum computer performs quantum calculations and at the same time manipulates the data and states of the qubits.

The idea of developing a quantum computer has just emerged, and its components contain dozens of quantum bits. A real challenge in this area is the fault tolerance and scalability part. As a result, quantum operations performed by a quantum computer will be performed in an insecure manner because its components are insecure. Researchers in the field are working hard to build the best computer possible.

From an experimental point of view, the scientists obtained consistent results, results that went in parallel with the theoretical notions. The whole process has undergone a continuous evolution, methods have been developed for the manipulation and detection of quantum objects. For example, photons or electrons are part of the object of research. These lead to quantum physical implementations of the quantum process.

The information is classified according to the memory unit used, respectively bit or qubit. If we use bit we can have the value zero or one, and qubit is used in quantum calculation. The qubit is provided on two levels, i.e. it can be in a linear combination. This is called an overlap phenomenon.

In the following figure we can see the difference between the classical and the quantum bit in a binary system.

![Fig.3: Classical bit and quantum bit (qubit) (ERP News, 2019)](image-url)
An algorithm is a step-by-step procedure for performing a calculation, or a sequence of instructions for solving a problem, in which each step can be performed on a computer. Therefore, an algorithm is a quantum algorithm when it can be performed on a quantum computer. In principle, it is possible to run all the classical algorithms on a quantum computer. The term quantum algorithm applies to algorithms in which at least one of the steps is distinctly "quantum", using overlap or another method.

With the help of technology development, various processes could be performed, which require a lot of processing power. For example, there have been trips to the moon, satellites have been set up, etc., but there are still tasks that traditional computers are struggling with.

A rather important problem is combinatorics, because it involves finding an arrangement of elements that grows exponentially. Computers have to repeat each permutation to find the best result. Quantum computers show a reduction in the cost of solving combinatorial problems.

In the field of quantum mechanics, the state of objects depends on notions of probability, which means that data is stored and recorded differently by non-binary qubits rendering the multiplicity of states in the quantum environment. Even physicists are studying this study of the subatomic universe.

**CYBER SECURITY**

The combinator was essential for encrypting information. Al-Khalil’s eighth-century cryptographic message book looked at permutations and word combinations.

Nowadays combinatorial calculations are the basis of encryption, which is difficult to manage. A new industry is emerging that is helping companies solve cybersecurity issues. To make the best predictions we need the help of quantum calculus, which opens new gates in artificial intelligence, such as the facial recognition algorithm. (Lu, 2020)

Currently, the software is quite limited to allow a significant increase in quantum machine learning with faster AI.

Quantum computers can identify the problems of a manufacturing process that have led to malfunctioning incidents. For example, in the production process of the microchip.

Quantum computers rely on the same physical rules as atoms to manipulate information. Quantum computers are based on fragile qubits, short for quantum bits, which are useful only when they are in a delicate quantum state. Any external disturbances, such as heat, light, or vibration, inevitably take these qubits out of their quantum state and turn them into ordinary bits. (Gil, 2020)

Quantum communication has improved the security of communication between two separate media, the photon crossover. To secure the information we need advanced encryption and interference detection capability, which is to the benefit of consumers. This process also has a side effect of involving quantum communication on the parties involved, which is based on the infiltration of intelligence into the systems of other participants. The whole process is in a continuous development.

The quantum process encompasses a wide range of technologies, which means that we need high security. All this has an impact on the power of decryption and other data processing capabilities. The following image is representative of the cybersecurity chapter, in terms of encryption and decryption key.

*Fig.4: Cyber Security*  
(Intacs Corporation, 2016)
Imperfections in the manufacture and control of the qubit still lead to errors in quantum logic operations, currently at the level of a few percent. This level of hardware error is unacceptable for large-scale algorithms, and hardware imperfections are unlikely to be reduced to an acceptable level at any time. Borrowing from classical information, quantum error correction (QEC) and errors.

The theoretical development of QEC and FTQC in recent years has focused on building codes that are adaptable to physical hardware projects and raising the fault-tolerant threshold to an experimental level over the next decade. The topological model of QEC has proven to be more promising compared to many other long-term techniques and now forms the effective basis of all modern quantum computing architectures. (Devitt & Nemoto, 2012)

Each of these hardware models uses a different physical system that defines the qubit, and all allow for a wide range of physical operating speeds, physical component sizes, and associated ancillary technology, such as cryogenic cooling and ultra-high vacuum. The architectures that are based on the topological model have in common that the realization of an algorithm is, in fact, independent of quantum hardware. This method of calculation is very abstract compared to classical computer science. One of the most bizarre aspects of this model is that the physical hardware does not actually perform any real calculations. The hardware is responsible for producing a very large three-dimensional network of qubits that are all tied together to form a single quantum, massive, universal state. This quantum state forms the workbench of computation, and information is created, processed, and read by strategically manipulating this massive quantum state.

Even though quantum technologies are at the beginning of the road in terms of development, they have brought added value in the industrial area, through various social and technical trends. This research has been and is quite important for the academia.

This area of development has managed to reach high points of interest and funding, although the technical direction is not very clear. We are currently working on universal quantum computers, which are based on gate-based quantum algorithms and run parallel to quantum annealing technologies.

**QUBITS**

One of the earliest demonstrations of the quantum computer was in 1995 using captured ion qubits based on extended auxiliary hardware. Although they encountered various difficulties in their expansion, they were successful on a small scale. Superconducting qubits or artificial atoms.

Macroscopic electronic circuits that show quantized energy levels are called superconducting qubits. They can be applied in quantum calculus and quantum annealing.

These large amounts of artificial qubits or atoms are becoming more difficult to operate because we have to consider the interaction between each other and the unique matrix.

A major competitor to spin qubits is silicon. They are recognized for their stability.

We also have photonic qubits that are at an early stage in terms of research. They are based on a single unit of light. These are a real challenge, because they are harder to locate and manipulate.

Another area is that of topological qubits that are based on topological symmetry and see the improvement of the error correction process and are at an early point in the research.

The power of quantum computing derives from algorithmic methods that exploit the availability of quantum overlap and entanglement to perform calculations that are insoluble with classical devices. To date, several types of hardware have been developed, with the greatest efforts being made for trapped ions, photons, superconducting approaches, quantum dots, and neutral atoms. Although all approaches have strengths and weaknesses and are in various stages of development, the challenge of creating a practical design that can be scaled to one million or more qubits has not
yet been met with any of the existing platforms. The solution is to build error correction circuits that operate on logical qubits, each composed of many physical qubits, which will allow logical error rates with orders of magnitude much smaller than physical error rates. Although error correction is remarkably effective for conventional computing devices - Hamming codes detect and correct errors while requiring only about 10% overload in physical bits - quantum error correction is costly. New approaches to error correction are being subject of intense research, with a promising direction being the development of codes that are optimized to suppress the dominant error mechanism in a given physical platform.

However, with physical error rates of 10^-4, a plausible target for current qubit systems, the overload required to achieve logical error rates of 10^-10 can be measured in thousands of physical qubits. Thus, a quantum computer capable of performing deep calculations on hundreds of logical qubits could require one million physical qubits (Saffman, 2019).

Here is an example of the chart for physical qubit error rate.

![Physical error rate chart](Tanaka, U. & Kondo, M., 2021)

One consequence of the cost of quantum error correction is that any viable approach to large-scale quantum computing must combine high-fidelity quantum logic operations with the ability to integrate large numbers of physical qubits. From this perspective, neutral atomic qubits look particularly promising, as they have already demonstrated control of more qubits than any other platform, with recent experiments in 1D, 2D and 3D geometries showing control of up to 50 atomic qubits.

Large qubit matrices can be prepared in 1D, 2D or 3D geometries. The number of proximal qubits increases with dimensionality, which is advantageous for the implementation of error correction code words and indicates a preference for 2D or 3D matrix (Planat, M. & UI Haq, R. 2017).

From a fundamental perspective, the prospects for scaling neutral atomic systems are particularly promising due to the ratio between coherent and incoherent coupling rates. Neutral atomic qubits are encoded in hyperfine fundamental states for which coherence times of the order of 10 s have been demonstrated. The coherent coupling that allows quantum logic operations is activated by stimulated atoms at high Rydberg states with the principal quantum number close to 100. The ratio between the desired coherent coupling and the residual incoherent phase shift establishes a merit figure that allows scalability. To our knowledge, only captured ions can claim a similar g / γ ratio, but without a direct path to control thousands of qubits in a single processing unit.
RAM/ Q PRAM MODEL

The concept of RAM or an analog of the classical parallel RAM model would be useful for algorithm design. We introduce the parallel quantum RAM model (Q PRAM) which, in addition to any step of the circuit model, allows simultaneous queries to a shared quantum RAM. This allows us to design new quantum algorithms for parallel search in databases and the problems of distinguishing elements and finding collisions (Devitt & Nemoto, 2012).

We can show that if we use a more realistic idea, from a physical point of view, we have to gain in reversible sorting through more efficient circuit models. And at the same time we can present the implementation of the model (Q PRAM) with the help of a quantum circuit on a physical device, in which qubit iterations would be restricted. All this leads to a more efficient way to access the memory of a quantum computer. As a result, quantum memory can be shared between several processors.

A single qubit is a memory site. In order to be able to implement quantum algorithms as efficiently as possible, we need trapped ions that use optical cavities and nitrogen centres. All this emerges from the experiments made in the vacant centres. To allow the connectivity of a hypercube we need long-range qubits. For example, the bitonic sorting network is a much more efficient sorting network for emulating quantum circuits.

If we use a classical algorithm we can have quite high costs, in which the storage components have a lower cost than the computational components, which results in a total parallelism that is unrealistic and requires a reassessment of the process.

In the future, a quantum passive memory can be built that tolerates errors, and the costs will be much lower. Schemes for this process require full parallelism, regardless of the purpose.

There is a particular type of qubit, which is called molecular spin qubit and carries information, i.e. electronic spin. Previous studies have shown that interactions such as qubit-qubit require error correction. There are nuclear spins, which are part of the molecular spin qubit category and have longer coherence times. However, gates can slow down due to poor interaction. The architecture was tested in gates of one qubit and two qubits (Kramer, 2018).

Each qubit was coded separately in a single gate using their electronic „switch”, they also induced the reversible crossover that uses a gate controlled by two qubits with a phase change.

They are able to activate and deactivate the interaction between qubits with the help of paramagnetic resonance pulses in a uniform environment, unlike classical NMR schemes.

This phenomenon has been demonstrated by quantum simulation over time of a spin equal to 1 in the quantum tunnel. In the implementation of this experiment, the calculation for each sequence of gates was used, as well as the evolution of the time which was divided into smaller steps.

At present, qubits are built with the help of current computer technology and at the same time it is authorized / conventional. For example, qubits were made from organometallic molecules. Which suggests that these complex networks of molecules, looking like metal frames or organic frames, could lead to quantum computers. These qubit molecules are vanadium complexes. The unpaired electron of the transition metal is the unit that carries the information.

From a quantum point of view, the other part of the molecule retains its latent state.

The qubit-based processor must be kept at low temperatures to avoid damaging the superconducting circuits.

All problems of decoherence start from the nuclear spin, and the magnetic bar with microscopic dimensions can be called nuclear rotation. So, this nuclear spin helps to wrap the vanadium centre, more precisely it covers it with oxygen atoms, etc.

It is important to know that a processor that consists of a series of quantum bits must function as a single system, because we will never see a qubit that simulates large molecules that interact.
As it was mentioned in the previous sections, combinatorics is a central topic in this field. Certain types of engineering, such as biological or chemical, involve the manipulation of molecules and the interaction of subatomic particles. All this leads to the concept of quantum mechanics. With the complexity of the molecules, the number of their configurations increases exponentially, which results in a combinatorial calculation. For example, chemical simulations of chemical reactions have been successfully performed using quantum computers, from which we can deduce that the next step may be much more complex, in terms of the configurations of molecules that are quite difficult to model.

With the evolution of simulations in terms of the potential of quantum computing, the part of quantum encryption also develops. The combinatorial calculation also appears in the financial field in order to establish the prices of the complex assets. To simulate market movements, we need certain projections that are made using the Monte Carlo simulation, which uses derivative instruments. It is important to keep in mind that quantum algorithms increase the speed of financial calculation.

With the help of quantum calculation, it was possible to highlight the research areas that were prioritized, and the companies were divided into three categories of work in terms of software, hardware and combined.

Based on the notions presented above, we observe the numerous fields of use of the quantum computer and the possible cracks of the algorithms.

**REFERENCE LIST**


