Ca' Foscari
University
of Venice

Single Cycle Degree programme

in Computer Science

Final Thesis

The impact of post-quantum cryptography on cloud computing

Supervisor
Ch. Prof. Flaminia Luccio

Graduand
Teili Makasheva
Matriculation Number 893308

Academic Year
2023 / 2024

Contents

Introduction

Cloud computing is an innovative technology that integrates IT resources across various hardware platforms and provides users with access through the Internet. The concept of "cloud computing" can be traced back to the 1960s when John McCarthy envisioned computer computations performed using "public utilities". While cloud computing might appear as a relatively new phenomenon, its history dates back to the early 1950s with the advent of mainframes, which allowed multiple users to access a central computer. The ideology of cloud computing gained significant popularity in 2007 due to the rapid development of communication channels and the exponentially growing need for businesses and individuals to scale their information systems.

The transformation of cloud computing into a mainstream technology is attributed to its ability to offer scalable, cost-effective, and flexible IT solutions. It allows organizations to avoid substantial upfront investments in IT infrastructure, leading to reduced capital expenditures and enhanced operational efficiency. Moreover, the pay-as-you-go model of cloud computing provides businesses with the ability to dynamically adjust their resource usage based on current demands, thus ensuring optimal utilization of resources.

In the contemporary era, cloud computing has become an integral part of the IT landscape, supporting various deployment models such as public, private, and hybrid clouds. Each of these models offers distinct advantages and caters to different needs and security requirements. Public clouds provide cost efficiency and scalability, private clouds offer enhanced security and control, and hybrid clouds combine the benefits of both public and private clouds, offering a strategic balance.

As cloud computing continues to evolve, it faces several challenges, particularly in the realm of security. Ensuring data integrity, confidentiality, and availability in cloud environments is crucial. Additionally, the emergence of quantum computing poses a new set of challenges and opportunities for cloud data security. Quantum computers, with their exponential computational power, can potentially break many of the cryptographic algorithms currently in use. This has led to increased interest in developing quantum-resistant cryptographic protocols to safeguard data in the post-quantum era.

The development of quantum computers and advancements in quantum computing pose an unprecedented threat to current data protection methods. State, professional, and commercial secrets, financial and personal data—all these could quickly lose their confidentiality once an attacker gains access to powerful quantum computers. Modern cryptographic systems, particularly those based on asymmetric encryption like RSA, rely on the computational difficulty of problems like factoring large integers. However, Peter Shor's algorithm, developed in 1994, demonstrated that quantum computers could solve these problems efficiently, thereby rendering many classical cryptographic systems vulnerable.

In response to the quantum threat, researchers have turned to post-quantum cryptography (PQC), which involves developing cryptographic algorithms that are resistant to attacks from quantum computers. PQC is based on hard mathematical problems that are believed to be unsolvable even for quantum computers. Some of the most promising approaches in post-quantum cryptography include lattice-based cryptography, hash-based cryptography, code-based cryptography,

multivariate polynomial cryptography, and isogeny-based cryptography.

This thesis explores recent developments and methods in cloud data security, particularly from a post-quantum perspective. It delves into the principles of quantum computing, examines various quantum algorithms, and evaluates the potential impact of quantum computing on cloud data security. Furthermore, it reviews existing post-quantum cryptographic approaches and identifies candidates for new standards in the field, highlighting their strengths and weaknesses.

Through this comprehensive analysis, the thesis aims to provide insights into the future of cloud data security and the measures necessary to protect sensitive information against emerging threats. As cloud computing continues to play a pivotal role in modern IT infrastructure, ensuring robust security mechanisms is paramount to maintaining trust and reliability in cloud services.

This investigation not only addresses the technical aspects of implementing post-quantum cryptographic solutions but also considers the practical implications for businesses and end-users. By understanding the challenges and opportunities presented by quantum computing, stakeholders can better prepare for a secure and resilient digital future.

The thesis is structured as follows: Chapter 1 provides an overview of the historical context and evolution of cloud computing and post-quantum cryptography, describing their key achievements in the form of an overview. Chapter 2 discusses the fundamental principles of quantum computing, their computing power, and the threats they pose to modern cryptographic systems. The principles of quantum algorithms are also presented and the obstacles to creating an error-free quantum system are shown. Chapter 3 examines various post-quantum cryptographic approaches and evaluates their strengths and weaknesses. Quantum post-quantum cryptographic approaches are also compared. Chapter 4 defines cloud computing and discusses the technologies that are used there, the practical implications of implementing these cryptographic methods in cloud environments and the current state of standardization work assesses. Chapter 5 discusses the methodology used for selecting scientific papers for research and provides a detailed descriptions of the selected scientific papers. Finally, it compares research papers, highlights their similarities, differences, and effectiveness. Moreover it presents the conclusions drawn from the study of these initial papers. The conclusions include a summary of the findings and implementation strategies for securing cloud computing in the post-quantum era.

1 Quantum Computing

In the field of information processing, the competition between quantum and classical computing is growing more and more distinctly. Forthwith, this competition has intensified due to the inability to solve a certain class of computational problems on classical computers, due to the lack of effective algorithms. Concurrently, quantum computing (QC), using the paradoxes of quantum mechanics, allows us to solve these problems.

The concept of quantum computing originated in the 1980s in the works of D. Deutsch, Y. I. Manin and R. Feynman [44]. The initial idea was that it is more efficient to simulate quantum physical and chemical systems on a computer, which also has a quantum nature. Modern quantum technologies can support completely new computational algorithms (quantum algorithms) based on the principles of quantum mechanics. For the development of quantum mechanics, it is necessary to solve specific quantum problems, which, with the exception of the simplest, modern classical computers can solve in a time exceeding the mechanical resource of the entire universe. Quantum computers are needed to solve alike problems.

Definition 1. [10] "***Quantum computers*** *are computing devices whose power increases exponentially due to the use of the principles of quantum mechanics in their operations. They use phenomena of quantum mechanics (quantum superposition, quantum entanglement) to transmit and process data. The basic unit of information in quantum computing is the* ***qubit (quantum bit)***."

Definition 2. [11] "***Quantum superposition*** *is a fundamental principle of quantum mechanics, according to which, if states are acceptable for some quantum system, then any linear combination of them is acceptable. The state is called a* ***superposition of states*** *(the principle of superposition of states)*."

The principle of superposition of states conveys: if a system can be in different states, then it is capable of being in states that result from the simultaneous "superposition" of two or more states from this set.

Definition 3. [12] "***Quantum entanglement*** *is a quantum mechanical phenomenon in which the quantum states of two or more objects turn out to be interdependent.*"

This means that when two or more objects become entangled, their quantum states are linked in such a way that the state of one object cannot be described independently of the state of the other objects. Essentially, any change to the state of one entangled object will instantly affect the state of the other entangled objects, regardless of the distance between them. This interdependence creates a situation where the measurement of one entangled particle's properties (such as spin, position, or momentum) will immediately influence the properties of the other entangled particles, leading to correlations that cannot be explained by classical physics.

Computational elements of quantum computers - qubits are built on the basis of quantum objects: ions, cooled atoms or photons capable of being in a superposition of several states. An atom, electron, or photon may be in a state in which its properties are undefined. For example, particles can have two energies at the same time. These quantum states are extremely fragile. Elements of classical computers can store only one bit: 1 or 0. Qubits can be in a superposition of

two states, that is, they encode both a logical unit and a zero at the same time, also any combination of 0 or 1. This allows quantum computers to perform many calculations simultaneously, in one clock cycle. Quantum computers are able to cope with tasks that would take classical computers billions of years to solve. In particular, they can be used to model the behavior of complex quantum systems. The capabilities of quantum computers depend on the number of qubits. Only a few tens of qubits can give such a gain in computing power, which is unattainable for classical computers.

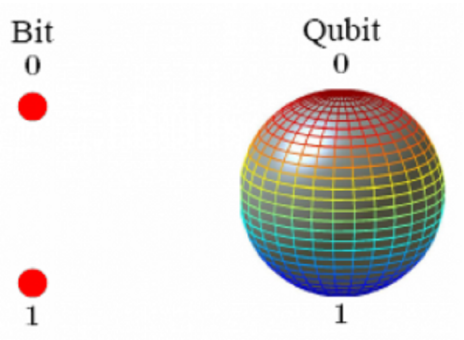

Figure 1: The general scheme of qubit

Figure 1 shows, as a comparison, how elements are stored in bits in classical computers in the form of signals and how this happens in quantum computers in the form of qubits [32]. Due to the fact that qubits are in several states at once and are interconnected, quantum machines can simultaneously sort through all the solutions at once - unlike conventional computers, which sort through the options sequentially and rather slowly.

Quantum computers exist in reality, but so far they are at an early stage of development. The largest technological corporations, including Google, IBM, Microsoft, are now trying to create a universal quantum computer. The first working model of a quantum computer was presented by scientists from MIT Media Lab in 1997. The two-qubit system worked on the principles of nuclear magnetic resonance (the same one used in MRI machines). The model was able to solve quite complex problems using the Deutsch–Jozsa algorithm (more information about this algorithm can be found Section 1.3.2) [46].

Presently, many companies and research institutes have Quantum computers. A few well-known models are:

- *IBM: Osprey* - 433 superconducting qubits that perform computing operations with 99% accuracy in 10 nanoseconds during the IBM Quantum Summit 2022. IBM claims that the number processing capabilities of this machine are far superior to those of any traditional computer, arguing that an ordinary computer will need more bits than atoms in the known universe to represent the state on the Osprey processor. By the end of 2023, the IBM Quantum System Two was released. This modular system will become the basis of the company's quantum supercomputers, accommodating several processors with communication channels between them. All these are steps towards IBM's plans to create a quantum system with more than 4,000 cubes by 2025 [47].

- *Google: Sycamore* - 53 superconducting qubits. The accuracy of calculations is higher - 99.9%, but the speed is slightly lower - 25 nanoseconds. In 2019, Sycamore completed a task in 200 seconds, which, as Google claimed in an article in the journal Nature, a modern supercomputer would take 10,000 years to complete. Thus, Google announced that it had achieved quantum supremacy. To estimate the time it would take for a classical supercomputer, Google ran parts of the quantum circuit simulation on IBM's Summit supercomputer, one of the most powerful classical supercomputers in the world. IBM later objected, saying that in a classic system such as Summit, the task would take only 2.5 days to complete. For such a statement, Google has been subjected to reasoned criticism [14].

- *Intel: Tunnel Falls* - 12 qubits, which show high accuracy - 99%, but relatively low speed - 100 nanoseconds. Intel has announced the release of the Tunnel Falls 12-qubit silicon chip and its availability to quantum researchers. Using Tunnel Falls, scientists can immediately start experimenting and calculating, instead of trying to make their own devices. As a result, a wider range of research becomes possible, including the study of the basics of qubits and quantum dots and the development of new methods for working with devices with multiple qubits. Tunnel Falls is manufactured on 300 mm wafers at the Intel D1 factory. The 12-qubit device uses the most advanced industrial production capabilities of Intel transistors. Intel is systematically working to improve the performance of Tunnel Falls and integrate it into its full quantum stack using the Intel Quantum SDK. In addition, Intel is already developing its next-generation quantum chip based on Tunnel Falls, it is expected to be released in 2024. In the future, Intel plans to collaborate with additional research institutes around the world to create a quantum ecosystem [48].

- *Xanadu: Borealis* - 24 photon qubits, the highest speed is 200 picoseconds, but the accuracy is 98%. Canadian developer Xanadu has demonstrated the benefits of quantum computing with Borealis, the first photonic quantum computer that provides full programmability of all its gateways. To demonstrate what a quantum computer with 216 "compressed" qubits is capable of, Xanadu has made it available in the public Xanadu Cloud for everyone. It will also appear soon in the Amazon Bracket cloud service [49].

Table 1 shows the technical specifications of various well-known quantum computers, including the number of qubits, accuracy, and speed.

Table 1: Summary of well-Known Quantum Computers

Company	**Model**	**Qubits**	**Accuracy**	**Speed**
IBM	Osprey	433	99%	10 ns
Google	Sycamore	53	99.9%	25 ns
Intel	Tunnel Falls	12	99%	100 ns
Xanadu	Borealis	24	98%	200 ps

Table 2 shows the key features of these quantum computers, highlighting their unique capabilities and development plans.

Table 2: Key Features of Quantum Computers

Company	Key Features
IBM	Superior processing, Quantum System Two, 4,000+ qubits by 2025
Google	Quantum supremacy, task in 200s vs 10,000 years for a supercomputer
Intel	Available to researchers, advanced production, next-gen chip in 2024
Xanadu	Full programmability, Xanadu Cloud, Amazon Bracket

1.1 Principles of quantum computing

Quantum computing is based on several fundamental principles of quantum mechanics. Here are some of the key principles that underlie quantum computing.

Superposition. Superposition states that, like waves in classical physics, two or more quantum states can be added together, and the result will be another valid quantum state. Conversely, each quantum state can be represented as the sum of two or more other separate states. This superposition of qubits gives quantum computers their inherent parallelism, allowing them to process millions of operations simultaneously.

Entanglement. Quantum entanglement occurs when two systems are connected so closely that knowing about one of them gives us immediate knowledge about the other, no matter how far apart they are. Quantum processors allow us to draw conclusions about one particle by measuring another. For example, they can be used to determine that if one qubit rotates up, then the other will always rotate down, and vice versa. Quantum entanglement allows quantum computers to solve complex problems faster.

When the quantum state is measured, the wave function collapses, and we can measure the state as zero or one. In this known or deterministic state, the qubit acts like a classical bit. Entanglement is the ability of qubits to relate their state to other qubits.

Decoherence. Decoherence is the loss of a quantum state in a qubit. Environmental factors such as radiation can cause the quantum state of qubits to collapse. A major engineering task in creating a quantum computer is the development of various functions that try to delay the decoherence of state, for example, the creation of special structures that shield qubits from external fields.

1.2 Components of a quantum computer

Quantum computers have hardware and software similar to a classical computer. They are composed of the following main components [45].

The quantum data plane. The quantum data plane is an efficient engine of a quantum computer that ensures the operation of its core. It includes physical qubits and structures to provide them. An important element is to maintain

strict isolation of qubits from the environment, which creates specific architectural constraints for connection and operation. Not every qubit can interact directly with others, so calculations must be adapted to these limitations.

Unlike classical computers, where control and data are integrated into one device and use the same technology, managing the quantum data layer requires a separate approach and technology. The control information for qubits is transmitted using various media: electrical wires, optical or microwave radiation. This maintains a high specificity and accuracy of exposure to the desired qubits without affecting others. As the number of qubits increases, it becomes more difficult to maintain this specificity.

The quality of the quantum data plane is determined by the error rate, the connectivity between the qubits, the coherence time of the qubits and the number of qubits in the module. Each of these parameters affects the efficiency of the quantum data layer.

Control and measurement plane. The control and measurement plane transforms digital commands from the control processor, which determine the necessary quantum actions, into analog control signals required for performing operations with qubits in the quantum data plane. It also transforms analog measurement results of units in the data plane into classical binary data processed by the control processor.

Any flaws in the isolation of these signals (called signal crosstalk) can lead to weak control signals for the qubits that otherwise would not be affected during the operation, which can lead to small errors in the state of the qubits. The shielding of control signals is complicated by the fact that they must pass through a device that isolates the quantum plane from the environment using vacuum, cooling, or both. This requirement limits the possible isolation methods.

Opportunely, both errors in the manufacture of qubits and crosstalk in signals are systematic and slowly change depending on the mechanical configuration of the system. The impact of these slowly changing errors can be reduced by using special control pulses that reduce the dependence of the qubit on these factors, and periodic calibration of the system to minimize the impact. Since each control signal can potentially affect any other control signal, the number of measurements and calculations required to achieve such calibration more than doubles with an increase in the number of qubits in the system.

The type of control signals of the quality control system depends on the qubit technology used. For example, systems using trapped ion qubits typically use microwave or optical signals (forms of electromagnetic radiation) transmitted through free space or waveguides and delivered to the location of the qubits. Superconducting qubit systems are controlled by microwave and low-frequency electrical signals, which are transmitted through wires penetrating the cooling device to reach the qubits inside the controlled environment.

In conclusion, the speed of a quantum computer is always limited by the time required to create the precise control signals required to perform quantum operations.

The plane of the management processor and the hosting processor. The control processor plane implements a quantum algorithm or sequence of operations. The hosting processor interacts with the quantum software and provides

a digital signal or a classical sequence of bits to the control and measurement plane. The control processor plane determines and activates a sequence of operations with quantum elements and measurements (which are then performed by the control and measurement unit at the quantum data level). These operating sequences implement the program provided by the main processor to implement the quantum algorithm. Programs must be adapted to the specific capabilities of the quantum level using a set of software tools.

Significant classical information processing is required to calculate the quantum operations required to correct errors based on the results of measuring the syndrome, and the time required for this processing can slow down the operation of a quantum computer. These additional costs are minimized if error correction operations can be calculated in a time comparable to quantum operations and measurements. As the size of the machine increases, this computational task becomes more and more complex, and it is likely that the control processor panel will consist of many interconnected processing elements to handle the computational load.

Building a control processor panel for large quantum machines is a complex task that is an active area of research. One approach involves splitting the panel into two parts. The first part is a classic processor that "runs" a quantum program. The second part is a scalable user hardware unit that interacts directly with the control processor panel and combines higher-level "instructions" received from the main controller with measurements of the syndrome to calculate the following operations that need to be performed with qubits. It is important to create scalable user hardware that can work fast enough and scale depending on the size of the machine, as well as develop the right high-level abstraction of commands.

The control processor panel operates at a low level of abstraction: it converts compiled code into commands for the control and measurement layer. The user usually does not interact with the control processor panel directly (or should not understand it). Instead, the user interacts with the host computer, which is connected to the control processor panel and speeds up the execution of some applications. This architecture approach is widely used in modern computers, where "accelerators" are used to speed up work for various tasks.

Quantum Software. Quantum software implements unique quantum algorithms using quantum circuits. A quantum circuit is a computational procedure that defines a series of logical quantum operations on basic qubits. Developers can use various software creation tools and libraries to encode quantum algorithms [45].

1.3 Quantum algorithms

The quantum computers work with the help of quantum algorithms capable of solving problems that are mathematically difficult for classical computers. Such algorithms establish the order of information processing on a quantum processor, and also use quantum superposition and entanglement to solve problems faster than the classical analogue.

The design flow of quantum algorithms is different from that of classical algorithms because the paradigm of quantum computer science requires a shift towards paradoxes and a "reformatting" of thinking because quantum mechanics

is inherently counterintuitive. Design flow of quantum algorithms must translate high-level quantum programs into efficient error-tolerant implementations on a variety of quantum environments. Moreover, it should contain programming languages, compilers, optimizers, simulators, debuggers, and other tools with well-defined interfaces and incorporated resistance to quantum error correction.

Quantum programming languages have already been developed for quantum computers. They are based on functional programming languages (Lisp, Erlang, Scala, Miranda, ML, Haskell) and realize quantum algorithms using vector and matrix algebra. In addition, on classical computers it is possible to solve simulation problems using frameworks of functional languages. However, it is impossible to realize real quantum algorithms with the help of such frameworks, because it would require huge computational resources to manipulate the necessary number of qubits and to apply unitary transformations to them. Such resources will not provide even supercomputers of exaflops performance, so we need quantum computers that will perform quantum operations at the physical analog level, which is much more efficient than a computational model on a classical computer [33].

The first algorithms for quantum computers, such as Deutsch's algorithm, were primarily of academic interest. Afterwards, American scientists Peter Shore and Lov Grover developed two different in essence, but very valuable from a practical point of view quantum algorithms [28]. Shor's algorithm convinced the world that quantum technologies had real applications and that the quantum computer threatened modern methods of cryptographic protection of information. The algorithms showed the ability to decrypt complex cryptographic algorithms, such as RSA, used to encrypt information. Grover's idea pointed to the fact that with the help of quanta it is possible to search unstructured data faster than with the help of classical technologies, and as it was later proved - with the maximum available in this task acceleration [27].

Admittedly, there are algorithms that are more applicable in reality. For instance, the Zalka-Wiesner algorithm will help create new medicines and new materials. Ambainis' algorithm is to analyze data, in a manner that images and texts. Another of the most notable inventions is the Harrow-Hassidim-Lloyd algorithm, which solves a system of linear equations on quantum computers [22]. This will significantly advance the processing of big data, the modeling of complex systems, and eventually may become another step towards the creation of strong artificial intelligence [29].

1.3.1 Deutsch's algorithm (1985)

Deutsch algorithm is a quantum algorithm proposed by D. Deutsch in 1985 [52], to solve the following problem. It is a function f, which takes 0 or 1 as an argument and also outputs 0 or 1 as a value. The function is set as a black box, i.e., it is possible to supply one of two values to the input and read only the output (the value of the function). It is required to understand, in the least number of calls to the function, whether the values of $f(0)$ and $f(1)$ coincide or differ.

To put it another way, we were given a black box with one of the four functions sewn inside. Our task is to understand which class the function inside the box belongs to. And all we can do is serve something to this black box at the entrance and see what happens at the exit.

This problem can be solved in a classical way (sending inputs and watching outputs) or quantum. In the first case, we will need two requests to our mailbox: we can see what it gives in response to an incoming 0 and 1, and then uniquely

determine the function itself and its type. The second solution is the implementation of the Deutsch algorithm. We are constructing a special quantum analogue for this black box, which is called a quantum oracle.

A quantum oracle is an analog of a black box that implements some functions, but receives quantum states at the input and outputs them at the output. In fact, a quantum oracle is a multi-qubit gate, which, as we already know, can be implemented using single-qubit and two-qubit operations. We send a specially prepared quantum state to the quantum oracle, then perform an additional quantum operation the Hadamard transformation. The Hadamard transform is a linear transformation used in signal processing and quantum computing. This operator performs the transformation of quantum states (qubits), creating a superposition of states, which is a key element of quantum algorithms.

Based on the result of measuring the resulting output state, we can understand which class (constant or balanced) the function inside the black box belongs to. The unambiguous answer can be found out in one pass, so we get an acceleration compared to the classical method.

Deutsch's algorithm was very important in the historical context. Deutsch showed that quantum computing helps solve problems faster than classical computers. The next important step was to generalize this algorithm to the case of functions of an arbitrary number of variables.

Deutsch's algorithm demonstrates a quantum advantage by completing the task in one call to the oracle function f, which is equivalent to the time complexity $O(1)$. In the classical case, two calls to the function f may be required, which is also a constant complexity [52].

1.3.2 Deutsch–Jozsa algorithm (1992)

Deutsch–Jozsa algorithm is a quantum algorithm proposed by David Deutsch and Richard Jozsa in 1992, which became one of the first quantum algorithms [13]. The algorithm is based on the phenomenon of quantum entanglement and the principle of superposition, due to which it demonstrates quantum superiority - significantly more efficient operation in comparison with well-known classical algorithms. The Deutsch algorithm (1985) that was mentioned before is the first version of this algorithm (Deutsch-Jozsa algorithm).

The problem solved by the Deutsch-Jozsa algorithm can be formulated as follows. Suppose there is a function $f(x)$ that can take as an argument x strings consisting of n bits each. A function can return 0 or 1. A function constant if it returns the same value for all arguments. A balanced function is a function that returns 0 or 1 on half of the input values. The task is to determine which function $f(x)$ is by making as few calls to it as possible. The classical theory of algorithms tells us that in the worst case it takes $2^{n-1}+1$ function calls to get a result. The Deutsch-Jozsa algorithm allows you to get a result by making just one function call, regardless of the number of bits included in the strings. To solve the problem, we need a circuit containing a multi-bit gate, which allows us to work with all input cubes at once, which ensures greater performance of the quantum algorithm. The Deutsch-Jozsa algorithm has demonstrated that quantum computing can solve problems that would require an exponential amount of computation in a single step. Thus, the total time complexity of the Deutsch–Jozsa quantum algorithm is also $O(1)$ [13].

1.3.3 Grover's Algorithm (1996)

The purpose of the algorithm is to search for an element in an unordered of size N database [28]. We can assume that we have a black box with a certain fixed number of inputs equal to N, among which there is only one to which the black box will say "yes", while it says "no" to the rest. The task is to find this element in the most optimal way in the classical and quantum case. It turns out that the quantum algorithm for solving such a problem gives an advantage - as they say, quadratic acceleration, because in this case, instead of the order of N queries that we need in the classical case, we will need only the root of N queries.

You can understand this as follows. If in the classics we would solve this problem by trying one option after another, then in the quantum case the algorithm is built in such a way that we create some quantum state containing all possible input options at once. Then we feed it to the black box (quantum oracle), and with the output we make some transformations. Then we re-submit the resulting state to the oracle and perform some transformations. After the root order of N iterations, the final dimension almost exactly gives the desired input.

The main steps of the algorithm:

1. *Initialization:* Begins with the preparation of qubits in the initial state. This state is then transformed into a superposition representing all possible list items at the same time.

2. *Oracle Application:* A special operation called oracle is used, which changes the state of the target element by marking it. This oracle acts as a black box that knows which element is the target and changes its phase to highlight it.

3. *Gain operator (diffusion):* After the oracle, an operation is applied that increases the probability of finding the target element. This operation redistributes probabilities so that the target element becomes more likely to be measured.

4. *Repetition of steps:* Oracle and diffusion steps are repeated several times. The number of repetitions is proportional to the square root of the number of items in the list and takes $O(\sqrt{N})$ iterations. Each repetition increases the probability of choosing the correct target element.

5. *Measurement:* At the end of the algorithm, the qubits are measured, and the result is likely to be the target element.

The generalization of Grover's algorithm is called the amplitude increase algorithm - that is, the fact that we do quantum transformations in such a way as to increase the probability of detecting the correct answer as a result of measurement. Quantum mechanics gives us the opportunity to "try" these black boxes by sending superpositions of all possible states to them. This is something that is "classically" difficult to imagine.

Grover's algorithm poses a threat to symmetric encryption. Also known as the quantum search algorithm, it allows you to speed up the unstructured search for input data for a given function. Quantum computers can use it to speed up cryptanalysis by going through all possible options to protect symmetrically encrypted information. However, unlike Shore's algorithm (which is discussed in more detail below in Section 1.3.4) the proposed acceleration is not exponential.

Simply put, increasing the length of the key used for encryption leads to an excessive increase in the cost of searching.

The classic linear search in an unsorted list requires $O(N)$ time, because in the worst case, it needs to check each element of the list. Due to the fact that the number of iterations of the oracle and diffusion steps is $O(\sqrt{N})$, therefore, the time complexity of the Grover's algorithm using quantum parallelism and superposition is $O(\sqrt{N})$ [19].

1.3.4 Shor's Algorithm (1994)

Work on a number of quantum algorithms, such as the Shor and Grover algorithm, was carried out in parallel and in the same direction, since the differences in the presentation times of the algorithms are 2 years. Ideologically, they were a development of the idea of the Deutsch algorithm presented earlier [54].

Peter Shore's algorithm is a quantum algorithm for decomposing numbers into prime factors, that is, factorization. The essence of the algorithm is to reduce the factorization problem to the search for the period of the function. If its period is known, then factorization is performed using the Euclid algorithm in polynomial time on a classical computer. Thus, Shor's algorithm includes two parts: classical and quantum. The quantum part searches for the period of the function, and the classical part first prepares this function, and then checks the period found by the quantum part. If the period is found correctly, then the problem will be solved.

Here are the main steps of the algorithm:

1. *Choosing a random number:* Start by choosing a random number a that is smaller than the number N that needs to be factorized.

2. *Checking for trivial divisors:* Check if a is not a trivial divisor of N. If a is divisible by N, then a is one of the multipliers, and the problem is solved. If not, go ahead.

3. *Using a quantum computer to search for a period:* At this stage, a quantum computer is used to find the period of the function, which takes a and raise to a degree it by calculating the remainder of the division by N. The goal is to find the shortest period at which the function returns to its initial value [15].

4. *Period parity check:* If the period is even, proceed to the next step. If odd, repeat the algorithm with a new random number a.

5. *Analysis of period values:* Use the found period to calculate the values that will help determine the multipliers of the number N. This step includes analyzing and verifying the values obtained in the previous step.

6. *Multiplier search:* The found values are used to find the divisors of N by calculating the largest common divisors with N. This allows you to get two numbers that are multipliers of N [23].

Shor's algorithm significantly speeds up the process of factoring numbers compared to classical methods, especially for large numbers. This is possible through the use of quantum computing to find the period of a function, which makes this algorithm a powerful tool for cryptography-related tasks. Thus, it poses a serious threat to public key cryptography based on these principles. All this has

generated great interest in quantum computing technologies as a potential tool for solving problems inaccessible to classical computers, and an incentive for the development of other technologies.

The total time complexity of the algorithm consists of the complexity of all stages:

1. *Choosing a random number:* This operation is performed in $O(\log N)$ time steps, since choosing a random number from a range of 1 to $N-1$ requires logarithmic time.

2. *Checking for trivial divisors:* The divisibility check is performed in $O(\log N)$ time.

3. *Using a quantum computer to search for a period:* This is the most difficult and important step. It involves preparing a superposition, performing a unitary operation representing a function $f(x) \equiv a^x \pmod{N}$, and applying the quantum Fourier transform (QFT). The quantum part has a time complexity $O((\log N)^3)$, since QFT is performed in $O((\log N)^2)$ time and exponentiation is performed in $O((\log N)^3)$.

4. *Period parity check:* Checking the parity of the period takes $O(1)$ time, since it is a simple check.

5. *Analysis of period values:* The analysis of values and the calculation of modular exponentials are performed in $O((\log N)^3)$ time.

6. *Multiplier search:* The calculation of the largest common divisor (GCD) is performed in $O((\log N)^2)$ time using Euclidean algorithm.

Now summarize all these complexities:

$$O(\log N) + O(\log N) + O((\log N)^3) + O(1) + O((\log N)^3) + O((\log N)^2)$$

Since $O((\log N)^3)$ is the largest term in this sum, it will dominate. The cumulative time complexity of Shor's algorithm has polynomial time complexity - $O((\log N)^3)$ [15], which makes it significantly more efficient than classical factorization methods with exponential complexity. This algorithm shows the potential of quantum computing to solve problems that are considered difficult for classical computers, and has important implications for cryptography.

The development of quantum and post-quantum cryptography is an important consequence of the invention of the Shore algorithm.

1.4 Obstacles to creating an error-free quantum system

It seems easy to create different algorithms for different tasks - and in theory there really are dozens, if not hundreds of them. But when it comes to practice and significant, exponential acceleration, the development of quantum algorithms runs into certain barriers. And therefore, the emergence of new quantum algorithms that can lead to radical changes.

The main difficulty is related to the fact that in the minds of mathematicians and theorists, algorithms work on an ideal computer. However, real quantum computers are not at all error-proof.

The obstacles come down to the fact that it is very difficult to create a powerful error-free quantum system:

- Quantum objects are very sensitive to the slightest changes in the environment: even minimal leakage of quantum information into the environment during the execution of the algorithm can lead to distortion of the final response. And this is despite the fact that the conditions for the stable operation of qubits in certain cases must be maintained very specific.

- Noise affects the calculation process due to the constant impact of errors, the number of operations that can be implemented in a quantum algorithm is now limited to several dozen, whereas thousands of operations are required to win when solving industrial problems.

- So far, it has not been possible to create the right number of error-free, that is, logical qubits. For example, to calculate the risks of a company operating in the securities market, at least 200 logical qubits are required, about 6 thousand to crack cryptography, and 7.5 thousand to predict the value of financial derivatives in real time [29]. For even more complex tasks like fast network hacking, bitcoin, or modeling new materials, you need from several tens to hundreds of millions. Whereas today quantum devices do not have more than a few error-proof qubits [45].

Quantum algorithms are already beginning to be implemented in actually functioning experimental devices, and quantum computing is a fairly advanced field of knowledge. Many of the best minds in the field of physics and computer science are involved in it, and the number of publications is growing day by day. New algorithms and ways of applying them to solving applied problems are being intensively created. Therefore, modernized and technological measures are needed to protect against attacks that will be carried out using quantum computing and quantum computers.

1.5 Quantum Cryptography

Quantum cryptography as a science originated in 1984, when the first quantum key distribution protocol, called BB84, was developed [50]. The main advantage of quantum cryptographic protocols over classical ones is a strict theoretical justification for their durability: if in classical cryptography, durability is usually reduced to assumptions about the computational capabilities of an eavesdropper, then in quantum cryptography an interceptor can take all actions permissible by the laws of nature, and still he will not have the opportunity to find out the secret key, while remaining unnoticed.

One of the key properties of quantum mechanics important for quantum cryptography is the collapse of the wave function. This means that when measuring a quantum system, its initial state changes. The important thing is that because of this, it is impossible to accurately distinguish one quantum state from another unless they are completely different. This property is used to ensure secrecy in quantum cryptography. If someone tries to eavesdrop on the transmitted quantum states, they inevitably introduce errors that can be detected on the receiving side. Legitimate users (who have the legal right to use the system and exchange secret information, for example, Alice and Bob) decide whether the secret key can be safely transferred based on the number of errors observed during reception. If the number of errors approaches a critical value (which depends on the protocol

used), the length of the secret key is reduced to zero, and key transfer becomes impossible.

This means that the most important characteristic of quantum cryptography protocols is an acceptable critical error on the receiving side, to which secret key distribution is possible: the larger it is, the more stable the quantum cryptography system is in relation to its own noise and eavesdropping attempts. The experimental implementation of quantum cryptography has encountered a number of technological difficulties, the most important of which is the difficulty of generating strictly single-photon quantum states.

In quantum cryptography, weak laser pulses are usually used, which are described by coherent quantum states. The laser radiation is distributed according to the number of photons according to the Poisson distribution. This means that, with a certain probability, each pulse can contain one, two or more photons.

Coherent quantum states are states of light created by a laser. In these states, light waves have certain phases and amplitudes, which makes them stable and predictable. Laser radiation with coherent states is distributed by the number of photons according to the Poisson distribution. This means that there may be a different number of photons in each pulse: sometimes one photon, sometimes two or more, but the probability of having more photons decreases.

In relation to quantum cryptography, this property is important because multiphoton states can be used by an interceptor for attacks. For example, an interceptor can delay some of the photons, and then, after receiving information from legitimate users, restore the necessary information from the delayed photons, which violates the security of data transmission.

This is important because if there are many photons in the pulse, the interceptor can delay some of them. Then, after receiving additional information from legitimate users, he can extract the necessary information from the delayed photons, which violates the security of quantum cryptography. Such an attack is called a photon number spliting attack or PNS attack (the full description of this attack is in section 1.5.3).

Developments in the field of countering the PNS attack have led to the emergence of a protocol with a modified (compared to BB84) configuration of states used by legitimate users. This configuration, although it provides a lower key generation rate, no longer allows the interceptor to obtain all the necessary information about the key, even if a part of the transmitted photons is successfully delayed in its quantum memory. The most well-known protocol resistant to a PNS attack is the SARG04 protocol, proposed in 2004 [51]. The analysis showed that the quantum key ceases to be secret only when the interceptor can block all pulses with one, two and three photons. This means that the quantum key can be transmitted over a longer distance than using the BB84 protocol, because the communication length depends on the average number of photons per pulse.

Thus, there is a concept of the critical transmission distance of the secret key. At this distance, the probability of pulses with a large number of photons is very low, and the stability of the protocol to photon number separation attacks (PNS attacks) is determined precisely by this critical distance [30].

1.5.1 BB84 Protocol

The purpose of the protocol is that, after execution, Alice and Bob both use the same key, with which they can encrypt messages with the inability of a third party to access them.

The protocol works as follows: Alice creates a set of qubits (for example, single photons) and prepares each of them in a random state. She chooses not only "0" or "1", but also prepares them in one of two bases: the z-basis or the x-basis. In the case of photons, the z-basis and x-basis mean the use of linearly polarized or circularly polarized light, and "0" and "1" mean horizontal or vertical, or right or left polarization. After that, Alice sends these qubits to Bob.

One of the ways to implement the first two steps of the algorithm: Alice prepares single photons and sends them to Bob. Photons are prepared in one of four states: light with circular polarization on the right or left, or light with horizontal/vertical linear polarization.

Bob then measures each qubit in a randomly selected basis. This, in particular, means that it can measure in the "wrong" basis, that is, not in the one in which Alice prepared the qubit.

After that, Bob tells Alice in which basis he measured each qubit. Alice tells him where he chose the correct basis. If the basis is correct, they get the same result and can use it as part of the key. For example, if Alice sent a "1" in the z-basis and Bob measured in the z-basis, he will also receive a "1". This result can be used in the key. If Bob chose the wrong basis, the result will be random and may differ from Alice's value. For example, if Alice sent "0" in the x-basis, and Bob measured in the z-basis, he is equally likely to receive "0" or "1". They cannot use such a result in the key, as it will not match. Thus, they create a common key using only those results where their bases match [31].

They can use all the numbers measured in the correct basis as a key. But if Eve intercepts the transmission and measures the qubits before sending them to Bob, she can change Bob's measurement results.

Therefore, for a part of the qubits (for example, half of them), Bob sends the results of his measurements, and Alice answers what they should be. If some values don't match, they may suspect that Eve was trying to intercept the qubits. Eve, like Bob, can only randomly choose a basis for measurements. If Eve chooses the "wrong" basis and Bob chooses the "right" one, Alice and Bob's results may not match, indicating interference.

If an attacker intercepts the qubits, it will be detected thanks to the principles of quantum mechanics. In quantum systems, any measurement changes the state of the qubit. Here's how it works:

- *Interception and measurement:* If an attacker intercepts qubits and tries to measure their state, he must choose a basis (z or x) to measure each qubit. Since the attacker does not know which basis Alice used, he will make a random choice.
- *State change:* If the attacker has chosen the correct basis for the measurement, he will receive the correct value ("0" or "1"). But if he chose the wrong basis, then his measurement will change the state of the qubit.
- *Sending qubits to Bob:* After the measurement, the attacker will send qubits to Bob. However, due to random changes in the state of the qubits caused by incorrect choice of the basis, some qubits will be changed.
- *Basis comparison:* After Bob receives the qubits, Alice and Bob publicly discuss which basis (z or x) they used for each qubit (without discussing the values of "0" or "1" themselves). They discard results where their bases do not match.

- *Detection of interference:* If the qubits were intercepted and measured by an attacker, then as a result of comparing the bases, Alice and Bob will find more inconsistencies than expected due to changes in the states of the qubits. This will indicate an interception attempt.

Alice and Bob will be able to detect interference attempts and take measures to ensure safety.

Example for BB84: Alice randomly prepares 10 qubits and sends them to Bob. Bob takes measurements randomly, getting some results, after which they both exchange their databases and discuss them, destroying the qubits that Bob measured on the wrong basis. On the half of the qubits that are fine, they also discuss the measurement results. If they get matching results, they use the measurement results as a key, which consists of the remaining uncollected qubits [31].

The BB84 protocol is the first and most studied protocol for quantum key distribution. Moreover, attempts at its technical implementation have encountered a number of technological difficulties, as a result of which Eve has the opportunity to conduct a new type of interception of information, impossible with the "strict" implementation of all the principles of the BB84 protocol. Since quantum cryptography aims to ensure secrecy in all possible actions of Eve, it has become necessary to develop protocols that can withstand Eve and at the current level of technology development.

Attack to the BB84 protocol. How can the photon separation operation be used to crack the BB84 protocol? Eva can find out the number of photons in each pulse without any consequences. The attack is structured as follows: if the pulse contains only one photon, Eve blocks it, otherwise she leaves one of the photons in her quantum memory (for its implementation it is enough to have a regular delay line), sending the rest to Bob through her more perfect channel (ideally through a channel at all without losses). After the operation of matching the bases, conducted through an open channel, Eva receives all the necessary information to reliably distinguish the photons available to her, which means she is able to find out the whole key without being detected. This makes the BB84 protocol completely unprotected against a PNS attack.

Simply, BB84 uses orthogonal states, which makes it vulnerable to PNS attacks. Eva can intercept multiphoton pulses and measure them, obtaining accurate information about the transmitted state.

1.5.2 B92 Protocol

The B92 protocol is close to BB84, but more flexible, and the ideas of which will be used in the future.

The B92 protocol is important for understanding the use of non-orthogonal states in quantum cryptography. It differs from the BB84 protocol, where the probability of error on the receiving side is 25% in the absence of interceptors [31]. In B92, this probability may vary depending on conditions such as the length and quality of the channel, which allows for higher data transfer rates in some cases.

Non-orthogonal states - in the context of quantum cryptography, this means that they cannot be clearly distinguished without errors, unlike orthogonal states, which can be distinguished with complete confidence. Examples: states 0 and 1

for a qubit. These states can be distinguished accurately and without errors and quantum, non-orthogonal, different states from each other $< \phi >$, $< \varphi >$, where the angle between them is not equal to 90 degrees. Such states cannot be distinguished without some probability of error. If an attacker tries to measure non-orthogonal states, he cannot determine exactly which state was sent, due to the superposition of states. This leads to errors in its measurements and signals legitimate participants (Alice and Bob) about a possible interception attempt.

The B92 protocol works as follows: Alice sends Bob one of two non-orthogonal quantum states. These states are not orthogonal, which means that their angle is different from 90 degrees. Bob makes a measurement that can give three results: two accurate and one inconclusive. Inconclusive results do not provide useful information and are discarded. After transmitting all the messages, Alice and Bob disclose some of their data for error checking. If errors exceed a certain threshold, the protocol is terminated. If the errors are less than the threshold, the rest of the data is used to create a secret key.

The closer the angle is to 90 degrees, the closer the protocol is to using orthogonal states, which increases the data transfer rate, but reduces the resistance to interception. At smaller angles, the probability of incompatible results is higher, which complicates the interception.

The B92 protocol offers flexibility in configuring data transmission parameters, which allows it to be adapted to the specific conditions of the communication channel. This makes it an important tool in quantum cryptography, especially in the context of the development of new protocols such as SARG04 and non-orthogonal versions of phase-time coding.

Attack on the B92 protocol. The attack on the B92 protocol turns out to be even simpler. It is possible even in the case of a strictly single-photon source, and for its implementation, only attenuation in the communication channel between Alice and Bob is sufficient. Eve can make the same measurement that Bob makes on her side. In the case of a joint outcome, Eve receives all the information about the transmitted signal, and can forward it to Bob without errors (again using a more advanced channel to compensate for losses). If the measurement gave an inappropriate outcome, then Eve simply blocks the impulse. With such an attack, Eve gets all the information without being detected. It should be noted that the formally described attack does not even fall under the definition of a PNS attack (see next Section 1.5.3), since it does not use the photon separation operation. This attack is possible not in the case of transmission of multiphoton laser pulses, but when using an imperfect communication channel with losses greater than a certain critical level. Thus, the B92 protocol turns out to be much more vulnerable to such eavesdropping [31].

1.5.3 PNS attack

In practical schemes of quantum cryptography, attenuated laser pulses are often used instead of a strictly single-photon source. This technical limitation is due to the fact that creating an ideal single-photon source is difficult and expensive. Attenuated laser pulses contain low light intensity, which increases the probability of transmitting a single photon, but does not exclude the possibility of transmitting several photons simultaneously. The Photon Number Splitting (PNS attack) is one of the main threats to such systems. Here how it works:

- *Multiphoton pulse detection:* An attacker (Eva) can determine which pulses contain multiple photons.
- *Blocking single-photon pulses:* Eva blocks pulses containing only one photon.
- *Multiphoton pulse processing:* For pulses with multiple photons, Sheva sends one photon to Bob and holds the rest, performing various actions with them to obtain information.

Eva can use a better communication channel to transmit photons. Eve can replace the quantum communication channel between Alice and Bob with her own channel, which has less attenuation. Ideally, Eve uses a lossless channel to send the remaining photons to Bob. This allows it to avoid detection, since photon losses in the channel are common and difficult to detect. If there is a significant proportion of multiphoton pulses on the source side and losses occur in the communication channel, Eva's actions may go unnoticed. This reduces the secrecy of the quantum cryptographic protocol, since Eva can intercept information without the risk of being detected [31].

1.5.4 Protocol 4+2

The "4+2" protocol was created to counteract the PNS attack. In this protocol, the states within each basis are made non-orthogonal, which prevents Eve from accurately determining the transmitted state. The 4+2 protocol can be considered a combination of the BB84 and B92 protocols. BB84 uses orthogonal states and two bases. B92 uses two non-orthogonal states. "4+2" combines elements of both protocols using four BB84 states and two additional non-orthogonal states.

Alice prepares and sends qubits using four states, as in BB84, and two additional non-orthogonal states. Bob measures these states by choosing bases randomly. If Eve intercepts and measures qubits, it will be difficult for her to determine the exact state due to the non-orthogonality. Her interference causes errors that Alice and Bob may notice when checking the data.

Thus, the "4+2" protocol increases the security of quantum communication, complicating the task for an attacker and improving the detection of interference attempts [30].

2 Post-Quantum Cryptography

The development of quantum computers and improvements of quantum computing pose an unprecedented threat to current data protection methods. State, professional and commercial secrets, financial and personal data - all these will lose their confidentiality quickly once an attacker gains access to powerful quantum computers. However, a new - post-quantum - cryptography is coming to the aid of classical cryptography.

Classical cryptography can use symmetric or asymmetric keys. In symmetric cryptography, only one key is used to encrypt and decrypt a message: the sender shares it with the recipient, who successfully uses it to read encrypted data. In asymmetric cryptography, there are two keys: public and private. The first key (public key) is needed to encrypt the data, the second key (private key) is needed to decrypt it. Despite the fact that both keys are connected by a mathematical function, access to data is impossible without a private key: neither personal computers nor supercomputers can cope with this task due to lack of computing power.

There are quantum algorithms that can potentially crack symmetric-key ciphers, it is a Grover's algorithm (which was discussed earlier in the Section 1.3.3). Grover's algorithm is the main quantum algorithm affecting symmetric-key cryptography and it demonstrates that quantum computers can significantly reduce the security of symmetric-key ciphers by providing quadratic acceleration in brute force attacks.

It is also possible to break the asymmetric cipher: an algorithm that can cope with this task was developed by scientist Peter Shore (which was discussed earlier in the Section 1.3.4). Realize this algorithm requres a quantum computer [54]. Unlike conventional devices based on semiconductor technology, the power of quantum ones grows exponentially. Therefore, their capabilities far surpass any tools that hackers use today.

Modern quantum computers are not yet powerful enough to crack systems based on asymmetric encryption. But since the early 2000s, such technological giants as IBM, Google, Intel have been working on the development of quantum computing, which brings us closer to a new type of cyberattacks. According to most experts, the first cases of such attacks may be recorded before 2030 [1].

This brings us to the concept of the quantum threat - the risk that attackers may already save sensitive data encrypted with asymmetric cryptography today in order to decrypt it in the future when the opportunity arises. It doesn't matter how hackers gain access to quantum devices - whether it's social engineering, a cloud-based quantum computing platform, or employment with a quantum computer development company. All that matters is that all the accumulated data relevant at that time will be decrypted and lead to colossal losses. Therefore, it is necessary to protect them today.

Such data with a long life cycle include personal data of customers of banks and other financial organizations, medical institutions and mobile operators, as well as information representing commercial and state secrets.

In response to the quantum threat, information security specialists began to develop new methods of protection. Solutions based on post-quantum algorithms have become the most optimal in terms of cost and speed of integration. Such algorithms are based on complex mathematical problems, whose solution with

quantum computers does not give a computational advantage. Persistence of post-quantum encryption is guaranteed by mathematical proofs of secrecy of each of the algorithms - all of them are verified by the world scientific mathematical community.

In particular, these are algorithms based on linear codes, lattice theory and hash functions. The first type (code-based) is based on the hypothesis that it is very difficult to decode a random linear code. The first algorithm of this type appeared back in 1978 - it was the McEliece system (full description of this algorithm given in Section 2.1.4), one of the first public key systems [20]. The McEliece cryptosystem is a public-key encryption algorithm that is based on coding theory, specifically the theory of error-correcting codes. At that time, attacks using a quantum computer were out of the question, but after the advent of Shor's algorithm, which could easily break the encryption used everywhere, cryptographers-researchers became interested in the McEliece algorithm again.

Another type of post-quantum cryptography schemes are algorithms based on lattice theory. Such schemes are well-studied and easily applied in practice, in particular, IBM uses them in its security applications. One of the most popular cryptographic tools, the hash function, is also used in post-quantum encryption. Hashing is the conversion of an arbitrary amount of data into a unique set of fixed-length characters, which is very difficult to decrypt. And post-quantum algorithms using a hash function make decoding a message impossible, at least by all known methods. A hash function can be the basis of an electronic signature.

Today, post-quantum cryptography is at the stage of standardization. In the USA, this process is overseen by the National Institute of Standards and Technology (NIST). Since 2016, on a competitive basis, experts have been selecting the most quantum-resistant and optimal algorithms that will form the basis of post-quantum encryption standards at the international level, the final choice is planned by 2023 [4].

2.1 Existing post-quantum approaches

Post-quantum cryptography currently includes the following main approaches: lattice-based cryptography, multivariate cryptography, hash-based cryptography, code-based cryptography, isogeny-based cryptography [6].

2.1.1 Lattice-based cryptography

Lattice-based cryptography is a method of cryptography that uses mathematical structures known as lattices to create ciphers. Lattices in mathematics are sets of points in a multidimensional space with certain properties.

This type of encryption is considered particularly promising because of its potential resistance to attacks by quantum computers, making it an important candidate for post-quantum cryptography. Regardless of traditional methods such as RSA, which are based on factorizing large numbers or computing discrete logarithms, the complexity of lattice problems makes them difficult to solve even for quantum computers.

Besides, encryption and signing, other interesting applications can be built on lattices (fully homomorphic encryption, attribute-based encryption and signing, code obfuscation, and others). Most lattice-based algorithms are apparent to understand, provide widely performance, and have the property of parallelizing computation.

At a more abstract level, the description of lattices resembles that of codes - both structures are a set of vectors of length n in some space, to which error vectors are added. However, unlike codes, where values are typically bounded by 0 or 1, lattices use much larger numbers in each entry, and errors can propagate further. The problems associated with lattice-based cryptographic constructions are finding the original vector if the vector is broken. Lattices offer more parameters than codes, allowing them to offer solutions better suited to specific situations, but also leaving more room for attacks. Lattice-based cryptography began to develop with the work of Adjani in 1998 [7]. Currently, there are both encryption and signature systems based on this technology.

Advantages of lattice-based cryptography:

- *Resistance to quantum attacks.* The main advantage of lattice-based cryptography is that it remains secure even when using quantum computers. Algorithms based on the problems of finding the shortest vectors in lattices do not have effective quantum algorithms for solving them.

- *Comparative performance.* Lattice cryptography offers algorithms whose performance is comparable to modern encryption algorithms. This allows it to be used in practical applications without significant loss of performance.

- *Versatility.* Lattice-based cryptography can be applied in various fields, including data encryption, electronic signatures, authentication protocols, and more. Its versatility makes this cryptography approach widely applicable.

The problems of lattice theory are the basis of the finalist algorithms of the NIST competition: CRYSTALS-Kyber, NTRU, CRYSTALS-DILITHIUM, SABER and FALCON, alternative finalist algorithms FrodoKEM and NTRU Prime [55].

The Kyber and FrodoKEM algorithms are two of the most promising approaches in lattice-based cryptography.

CRYSTALS-Kyber is a shared key scheme that uses modular arithmetic and polynomials to create a secure cryptosystem. It is known for its high efficiency and relatively small key sizes. Kyber is designed to be resistant to quantum attacks and has been optimized for performance, making it suitable for various practical applications, including secure communications and data encryption.

FrodoKEM is an algorithm based on the "noisy" version of the Learning with errors (LWE) problem [57]. Unlike other algorithms, FrodoKEM does not rely on structured noise, FrodoKEM uses unstructured noise, which increases its potential resistance to quantum attacks. This approach provides a higher level of security assurance, making FrodoKEM a promising candidate for post-quantum cryptography. Despite its relatively larger key sizes compared to other lattice-based schemes, FrodoKEM's design focuses on maximizing security against both classical and quantum adversaries.

The Kyber and FrodoKEM algorithms, according to research, demonstrate impressive resistance to potential quantum threats [6]. Their implementation may be the key to creating a new era of cybersecurity, where information will be reliably protected from even the most advanced quantum attacks.

NTRU is a family of lattice-based public key cryptosystems that rely on the hardness of certain polynomial problems in lattices. NTRU encryption and NTRU

signatures have been studied extensively and are known for their efficiency and strong security properties. NTRU-based schemes are particularly attractive due to their relatively small key sizes and fast cryptographic operations.

NTRU Prime is a variant of the original NTRU cryptosystem that aims to enhance security by avoiding potential vulnerabilities related to certain algebraic structures. It employs a different lattice structure and provides a high level of security against known attacks. NTRU Prime is designed to be efficient and secure, making it a viable option for post-quantum cryptographic applications.

The lattice-based cryptographic algorithms demonstrate impressive resistance to potential quantum threats. Their implementation may be key to creating a new era of cybersecurity, where information will be reliably protected from even the most advanced quantum attacks. These algorithms offer a promising path forward in the quest for post-quantum security, ensuring the confidentiality, integrity, and authenticity of data in the quantum computing age.

2.1.2 Multivariate cryptography

The reliability of this section of cryptography is based on the complexity of solving a system of multidimensional quadratic polynomials over a finite field. Algorithms have high speed and low requirements for computing resources, but the lengths of public keys are quite large. This branch includes cryptographic systems such as, the Rainbow scheme and Unbalanced Oil and Vinegar scheme [56]. Oil and Vinegar scheme is a cryptographic scheme designed to create digital signatures. Rainbow scheme is an improved version of the Oil and Vinegar scheme, proposed to improve safety and efficiency.

Over the past few decades, various attempts to build secure encryption schemes for multidimensional equations have faced significant challenges. Although several multivariate encryption schemes have been proposed, multivariate cryptography has historically been more successful as a signature approach rather than encryption. This is primarily due to the following reasons. Multidimensional encryption schemes generally suffer from inefficiencies, characterized by extremely large public keys and long decryption times. These attributes make them less practical for widespread use. On the other hand, multivariate signature schemes have shown more promise. They are often more efficient and have been the focus of much research and development, leading to more practical implementations.

In the ongoing NIST competition to standardize post-quantum cryptographic algorithms, multivariate signature schemes have shown notable success. Of the nineteen signature schemes submitted, seven were based on multivariate quadratic equations. Two of these seven schemes advanced to the third round of the competition, highlighting their potential and robustness. The Rainbow scheme was selected as one of the three finalists, while the GeMMS scheme was selected as an "alternate candidate". These schemes are characterised by a very small signature size 33 bytes, but require relatively large public keys 160 KB [6], like Rainbow but its signature sizes and security features make it a viable candidate for post-quantum digital signatures.

Multivariate signature schemes like Rainbow could become the basis for quantum secure digital signatures. Their reliance on the hardness of solving multivariate quadratic equations, which is believed to be resistant to quantum attacks, positions them as strong candidates for securing digital communications in the quantum era.

2.1.3 Hash-based cryptography

New classes of algorithms are required to protect information systems from quantum computer attacks. Among such classes of algorithms we consider electronic signature schemes based on cryptographic hash functions. A hash function is a function that maps an arbitrary amount of data into a fixed-length string in such a way that it is almost impossible to find the input that maps into specific outputs. Such schemes use the following approach: a one-time signature scheme is taken as a basis (only one message can be signed), then it is combined with a Merkle tree to obtain a multiple signature. Different variations of the described approach are possible to achieve higher efficiency.

The peculiarity of algorithms on hash functions is high confidence in their security. When constructing electronic signature schemes, proofs are used to reduce the security of the scheme to certain properties of cryptographic hash functions. This means that if the scheme is compromised, some of the properties will also be violated. It is important to note that the properties of cryptographic hash functions have been studied for many years, but if the hash function used in a particular protocol turns out to be insecure, it is sufficient to replace it with another one, the construction itself remaining unchanged.

With this approach, only a limited number of signatures can be generated on a single key. Also, the disadvantages of the system include the fact that the signer needs to record the exact number of messages already signed. An error in this entry will lead to system vulnerabilities.

Signature schemes based on hash functions: They combine a one-time signature scheme, such as a Lamport signature, with a Merkle tree structure. Since the key of a one-time signature scheme can safely sign only one message, it is practical to combine many such keys in one, larger structure. The Merkle tree structure is used for this. One of the features of hash-based signature schemes is that they can only securely sign a limited number of messages due to their use of one-time signature schemes. Leslie Lamport came up with hash function-based signatures in 1979. Signature schemes based on the XMSS and SPHINCS hash functions were introduced in 2011 and 2015, respectively. In 2022, NIST announced the standardization of SPHINCS+ as one of three algorithms for digital signatures. SPHINCS+ is an improved version of SPHINCS. NIST standardized hash-based cryptography based on the extended Merkle Signature Scheme (XMSS) and Leighton-Mikali signatures, which are applicable in different circumstances, in 2020 [6].

The NIST competition finalist was selected XMSS algorithm and the alternative SPHINCS+ algorithm are implemented in the PQLR SDK.

XMSS is a hash-based signature scheme that uses a Merkle tree structure to manage OTS key pairs. It provides strong security guarantees, including forward security and post-quantum resistance. XMSS is efficient in terms of key generation, signing, and verification.

Unlike XMSS, SPHINCS+ is stateless, meaning it does not require the management of state information between signatures, making it more practical for certain applications. SPHINCS+ combines a large number of OTS key pairs using a hyper-tree structure and multiple layers of hashing to ensure security and efficiency.

One-time signature schemes: They are used as building blocks for signature schemes based on hash functions. This one-time signature key can be used to

sign only one message securely. In practice, one-time signature schemes such as the Lamport-Diffie scheme and the Winternitz scheme are commonly used.

Combining many one-time key pairs: The central idea of hash function-based signature schemes is to combine a large number of one-time key pairs in a single structure to obtain a practical way to sign more than one message.

Hash-based signature schemes, leveraging one-time signatures and Merkle tree structures, offer robust security against quantum attacks. Schemes like XMAS and SPHINCS+ have demonstrated their potential in the NIST competition, with SPHINCS+ being standardized for future use. These schemes are characterized by their efficiency, strong security guarantees, and practical implementations, making them essential components of post-quantum cryptography.

2.1.4 Code-based cryptography

These include cryptographic systems based on error-correcting codes, such as the McEliece and Niederreiter encryption algorithms [8].

The advantages of this kind of systems are the speed of computation. The disadvantages are that the keys are prolonged.

Many code-based signature systems have been designed to produce short signatures by using very large key sizes. Systems based on binary Goppa codes are generally considered secure, while systems based on quasi-cyclic medium-density parity checks have been used by analysts for about a decade and are becoming increasingly secure.

The robustness of such algorithms is based on an assumption about the computational complexity of the task of decoding a random linear code. NIST finalist Classic McEliece algorithm and alternative finalists BIKE and HQC algorithms are based on this problem. These algorithms are relatively efficient, but have long key lengths. They are also quite conservative in terms of security. The efforts of cryptanalysts since 1978 have not been able to significantly reduce the number of operations required to break cryptographic systems based on error-correcting codes, provided that their parameters are chosen correctly.

McEliece is a public key cryptosystem based on the theory of algebraic coding and developed by Robert McEliece. This was the first scheme to use randomization in the encryption process. In general, the work of this cryptosystem can be divided into three main algorithms:

- an algorithm for random key generation, which gives public and private keys at the output;
- a random encryption algorithm that outputs a ciphertext;
- a deterministic decryption algorithm that outputs the original plaintext.

The algorithm has not been widely recognized, but at the same time it is a candidate for post-quantum cryptography, as it is resistant to attack using the Shore algorithm. The algorithm is based on the complexity of decoding full linear codes and uses binary Goppa codes. The public key is obtained by masking the selected code as a complete linear one.

So far, the McEliece cryptosystem with Goppa codes is not amenable to cryptanalysis. The cryptosystem has several advantages, for example over RSA. Encryption and decryption are faster, and as the key length increases, the degree of data protection increases. For a long time, it was believed that the McEliece cryptosystem was not being used properly for EDS. However, it turned out to be possible to build a scheme for EDS based on the Niederreiter cryptosystem (a modification of the McEliece cryptosystem).

BIKE is a code-based key encapsulation mechanism (KEM) that is designed to provide security against quantum attacks. BIKE stands for Bit Flipping Key Encapsulation, and it relies on the hardness of decoding random linear codes in the presence of errors.

HQC is another code-based key encapsulation mechanism (KEM) designed for post-quantum security. HQC stands for Hamming Quasi-Cyclic, and it uses codes that are designed to be resistant to quantum attacks.

Both BIKE and HQC, like the Classic McEliece algorithm, rely on the difficulty of decoding random linear codes, making them suitable candidates for post-quantum cryptography. However, BIKE and HQC offer different trade-offs in terms of key sizes, efficiency, and security properties.

2.1.5 Isogeny-based cryptography

These cryptographic systems rely on the isogeny properties of elliptic curve graphs over finite fields, in particular supersingular isogenic graphs to create cryptographic systems [8]. Isogeny-based cryptography applies the concept of isogenies between elliptic curves in finite fields. The isogeny problem is to find a relationship between two elliptic curves that are known to be isogenic.

The most well-received protocols of this direction are SIDH (Supersingular isogeny Diffie-Hellman) allows to exchange keys over an unsecured communication channel. Proposed in 2011 by L.De Feo, D.Jao , and J.Plut. It is a key exchange protocol similar to the Diffie-Hellman protocol, but in 2022 W.Castryck and T. Decru published a preprint of the work, which describes a polynomial attack on the SIKE cryptosystem (SIDH version), a candidate for NIST standardization [2]. One of the notable advantages of SIDH is its small key sizes compared to other post-quantum cryptographic schemes. When compression techniques are applied, SIDH has the smallest key length of all post-quantum key exchange protocols. Despite the small key sizes, SIDH has faced challenges related to computational efficiency. The operations involved in isogeny computations are more complex and slower compared to other cryptographic schemes.

The CSIDH (Commutative Supersingular Isogeny Diflie - Hellman) scheme is another key exchange protocol whose security is based on the difficulty of finding an isogeny between two supersingular curves. This scheme is resistant to the attack of Castryck-Decru. In addition, unlike the SIDH scheme, CSIDH uses the action of a commutative group, the CSIDH protocol was first described in 2018 by W.Castryck, T.Lange. In isogeny cryptosystems, despite the small key size, the slow speed of the circuits remains a smooth problem [2]. The Castryck-Decru attack removed from consideration the SIDH/SIKE scheme, which is the most promising from the point of view of practice, and all schemes for which isogeny values at torsion points were used to optimize. Therefore, the most important direction in the field of isogeny is the study of optimization issues of existing circuits.

This fact is its distinctive feature that guarantees perfect secrecy. Taking into account compression SIDH has the smallest key length of all post-quantum key exchange protocols. However, a full-fledged cryptosystem on isogeny has not been realized yet.

2.2 Difference between Post-quantum and Quantum Cryptography

Quantum cryptography is a field of cryptography that uses the principles of quantum mechanics to ensure the secure transmission of information. It is based on the use of quantum properties such as non-destructive measurement and quantum inequality to create protocols that provide continuous protection against interference and interception of information.

Post-quantum cryptography, on the other hand, encompasses new encryption methods and algorithms designed to protect information in an environment where quantum computers will become available and can effectively crack classical cryptographic algorithms. This field aims to create cryptographic protocols that remain resistant to attacks from both modern classical and future quantum computing systems.

Differences between post-quantum and quantum cryptography. The main differences between quantum and post-quantum cryptography can be summarized as follows:

Basic principles: Quantum cryptography uses the principles of quantum mechanics, such as quantum state, superposition, and measurement, to ensure the secure transmission of information. Post-quantum cryptography is based on classical principles of cryptography, but develops new methods and algorithms that remain resistant to attacks by quantum computers.

Goal: Quantum cryptography aims to create protocols and algorithms that protect information using quantum properties such as quantum trust and quantum uncertainty. Post-quantum cryptography strives to develop cryptographic methods that remain reliable even in conditions where quantum computers can effectively crack existing classical cryptographic algorithms.

Applied methods: Quantum cryptography includes protocols such as quantum key distribution, quantum teleportation, and quantum encryption. Post-quantum cryptography is developing new encryption algorithms that are based on mathematical problems that even quantum computers cannot solve efficiently.

Stage of development: Quantum cryptography is at the stage of active research and experimentation, and some of its protocols are already being applied in real systems. Post-quantum cryptography is also under active research, and the goal is to develop algorithms that will be ready for use when quantum computers become widespread.

Advantages of quantum cryptography.

Invulnerability to attacks using quantum computers: Quantum cryptosystems provide protection against attacks based on quantum computing, such as the Shore algorithm, which can crack modern cryptographic protocols.

Unconditional security of key transfer: The use of quantum keys for key exchange ensures that eavesdropping or interception of data is impossible without violating quantum mechanics.

Secrecy of transmitted information: The principles of quantum mechanics provide the possibility of covert information exchange, which makes quantum cryptography especially attractive for protecting confidential information.

Benefits of Post-quantum Cryptography: High degree of attack resistance: Post-quantum cryptography algorithms based on complex mathematical problems provide protection against quantum and classical attacks such as the Shore algorithm.

Efficiency and flexibility: Many post-quantum cryptography algorithms have high performance and can adapt to various use cases without significant security losses.

Relative independence from quantum technologies: Post-quantum cryptography is an alternative to quantum cryptography and does not require quantum computers for its implementation, which makes it more accessible and practical nowadays.

Thereby, although both cryptographic paradigms provide information security, quantum cryptography is predominantly based on quantum properties, while post-quantum cryptography uses complex mathematical problems to ensure security. Post-quantum cryptography and quantum cryptography both belong to modern fields of cryptography, but they solve different problems and use different principles.

Table 3 shows a comparison between quantum cryptography and post-quantum cryptography. Quantum cryptography is based on the principles of quantum mechanics, using properties of photons for secure key exchange and protocols like BB84 to utilize quantum uncertainty for security. It ensures security through state changes and offers unconditional security. By contrast, post-quantum cryptography addresses threats from quantum computers by developing new algorithms that are resistant to quantum attacks, securing data against potential decryption by quantum computers and differing from the principles of Quantum Cryptography.

Table 3: Comparison of Quantum Cryptography and Post-Quantum Cryptography

Quantum Cryptography	**Post-Quantum Cryptography**
Based on principles of quantum mechanics.	Based on classical cryptographic principles, designed to be secure against quantum attacks.
Uses quantum properties of physical objects, such as photons.	Develops algorithms resistant to quantum computer attacks.
Main protocols like BB84 use quantum uncertainty for security.	Main algorithms include lattice-based, code-based, hash-based, and isogeny-based cryptography.
Detection of intruders is possible because observation changes the quantum state.	Resistant to attacks such as Shor's algorithm which can factorize large numbers efficiently.
Aims to provide unconditional security based on quantum physics.	Aims to maintain security using mathematical problems hard for quantum computers.
Relies on quantum key distribution (QKD) for secure key exchange.	Relies on classical communication channels but with quantum-resistant encryption methods.
Sensitive to environmental disturbances and requires specialized hardware.	Can be implemented on existing digital infrastructure without special hardware.
Not yet widely deployed due to technological and practical limitations.	Actively researched and developed, with some algorithms already standardized by NIST.

Consequently, quantum cryptography provides unconditional security for data transmission using quantum properties, while post-quantum cryptography develops algorithms that are resistant to attacks based on quantum computers.

By way of contrast quantum and post-quantum cryptography have several common features. Both of them:

Based on quantum mechanics: Both forms of cryptography are based on the principles of quantum mechanics, such as the principle of superposition and measurement of states.

The purpose of ensuring security: Both quantum and post-quantum cryptography are aimed at ensuring the security of information transmission by developing cryptographic methods resistant to attacks of classical and quantum computing.

Application of quantum properties: Both forms of cryptography use quantum properties such as quantum keys and quantum superposition to create cryptographic protocols and algorithms.

Based on mathematics: Both fields of cryptography are closely related to mathematical concepts such as number theory, probability theory, and linear algebra for the development and analysis of cryptographic algorithms.

The evolution of methods: Post-quantum cryptography is the development of quantum cryptography and aims to create cryptographic methods that will be resistant to future attacks of quantum computing [34].

2.3 Candidates for the new post-quantum standard (NIST Standards Competition)

Since 2017, research processes in the field of synthesis and analysis of quantum-stable cryptographic schemes have received a new impetus thanks to the efforts of the National Institute of Standards and Technology of the USA (NIST), which organized an open international platform (competition) for submitting proposals on standardization and discussion of post-quantum cryptographic schemes.

Candidate algorithms submitted for the NIST competition implement the following mechanisms: key encapsulation and digital signature. Certain resistance requirements are imposed on these mechanisms, both theoretical (formally provable) and practical (several resistance levels have been determined relative to all known quantum and classical attacks). The practical applicability of the proposed algorithms is also an important criterion.

The algorithms undergo both internal expertise by NIST staff and open validation by cryptographic researchers from all over the world. The results of the examination are discussed both directly on the NIST website and on the public mailing list.

In 2017, the US National Institute of Standards and Technology announced the launch of a competition to create new post-quantum algorithms and standards to replace the old one. The acceptance of applications for participation in the NIST competition was completed on November 30, 2017. A total of 83 applications were submitted [3].

First Round. A total of 69 applications were accepted for the first round, 14 of them were withdrawn by the authors or hacked immediately. Including 49 public key encryption algorithms and 20 electronic signature schemes [3].

The main types of cryptographic schemes used in the algorithms participating in the NIST competition:

- complex problems of the theory of integer lattices (lattice-based cryptography);
- using error-correcting codes;
- digital signature schemes based on cryptographic hash functions (hash-based cryptography);
- systems of polynomials in many variables (multivariate cryptography);
- "exotic" problems such as the conjugate Search Problem, operations in Braid Groups, octonion algebra, Chebyshev polynomials, etc.

Since most symmetric encryption algorithms are relatively easy to modify so that they are resistant to attacks by quantum computers, emphasis has been placed on the development of public key cryptographic methods. In particular, attention is paid to the development of digital signatures and key encapsulation mechanisms.

Second Round. The results of the first round were announced on January 30, 2019. 26 candidates passed to the second round: 17 encryption and key distribution algorithms and 9 electronic signature schemes [24]. At the same time, NIST experts did not express a clear preference in choosing classes of promising

synthesis solutions. Only exotic schemes, which often turn out to be the least stable, were excluded from the list of participants. The three main criteria used to evaluate the candidates were: security, speed and memory resource utilization, algorithm characteristics, and nuances of implementations.

Security is the most important requirement. NIST plans to use the new post-quantum standard for a wide range of tasks. Candidates will be evaluated specifically on their ability to provide security in these cryptographic tasks.

Furthermore, one of the requirements for candidates was to provide information for generalization about known cryptanalytic attacks on the proposed schemes, and to assess the complexity of these attacks.

Efficiency of execution and the use of memory resources. These include: the size of the keys, the size of the signature; the time spent on generating keys and signatures; the time required to verify signatures, as well as the proportion of possible errors in the algorithms. Memory size requirements apply to both software and hardware.

Characteristics of algorithms and nuances of implementations consists in any specific capabilities of each algorithm, for example, in a good ability to work effectively on various platforms, or in the possibility of parallelizing calculations to achieve higher performance.

Third Round. In 22 July 2020, NIST announced the third round of the standardization process, which lasted 24 months. It included 15 algorithms (7 basic (first track) and 8 alternative (second track)) [9].

The first group of algorithms presented in the first track represents those that are currently considered the most promising and will be considered for standardization at the end of the third stage. Algorithms from the second group, presented in the second track, can still become part of the standard after the completion of the third stage. NIST suggests that some alternatives will also be considered in the fourth stage. This also means that in the future it may be possible to submit new signature schemes that will be reviewed again within the category of alternative candidates.

Table 4 provides a comprehensive overview of the ***7 basic algorithms*** that form the foundation of post-quantum cryptographic methods. These algorithms are categorized by type and further classified into Public Key Encryption/Key Encapsulation Mechanisms (PKE/KEM) and Signature schemes. The lattice-based category includes CRYSTALS-Cyber, TRY, and SOBER for PIKE/KEM, and CRYSTALS-Dilithium and FALCON for signatures. The code-based category features Classic McEliece for PIKE/KM, while the multivariate category includes Rainbow for signatures.

Table 4: 7 basic algorithms (first track)

Type	**PKE/KEM**	**Signature**
Lattice	CRYSTALS-Kyber, NTRU, SABER	CRYSTALS-Dilithium, FALCON
Code-based	Classic McEliece	
Multivariate		Rainbow

Table 5 provides a comprehensive overview of the ***8 alternative algorithms***

that constitute the second track of post-quantum cryptographic methods. These algorithms are categorized by type and further classified into Public Key Encryption/Key Encapsulation Mechanisms (PKE/KEM) and Signature schemes. The lattice-based category includes FrodoKEM and NTRU Prime for PKE/KEM. The code-based category features BIKE and HQC for PKE/KEM. The hash-based category includes SPHINCS+ for signatures, while the multivariate category includes GeMSS for signatures. The supersingular elliptic curve isogeny category features SITE for PKE/KEM, and the zero-knowledge proofs category includes Picnic for signatures.

Table 5: 8 alternative algorithms(second track)

Type	**PKE/KEM**	**Signature**
Lattice	FrodoKEM, NTRU Prime	
Code-based	BIKE, HQC	
Hash-based		SPHINCS+
Multivariate		GeMSS
Supersingular elliptic curve isogeny	SIKE	
Zero-knowledge proofs		Picnic

Winners and Fourth Round. On 5 July 2022, the third round of the NIST competition ended, and the final list of algorithms for standardization was announced. The selected algorithms include:

- digital signature schemes - CRYSTALS-Dilithium, Falcon, SPHINCS+;
- the scheme of secure key transfer - CRYSTALS-Cyber.

Table 6 presents ***the first group of winners announced by NIST*** for post-quantum cryptographic algorithms. These algorithms have been selected for their robustness and potential to secure data against quantum computer-based attacks. The table categorizes the winners by type and further classifies them into Public Key Encryption/Key Encapsulation Mechanisms (PKE/KEM) and Signature schemes. In the lattice-based category, CRYSTALS-Khyber has been selected for PKE/KEM, and CRYSTALS-Dilithium and FALCON for signatures. The hash-based category includes SPHINCS+ for signatures, recognizing its potential to provide secure cryptographic solutions in the post-quantum era.

Table 6: First group of winners

Type	**PKE/KEM**	**Signature**
Lattice	CRYSTALS-Kyber	CRYSTALS-Dilithium, FALCON
Hash-based		SPHINCS+

Additionally, the fourth round was announced to expand the set of algorithms for secure key transfer. Algorithms are considered as candidates: Classic McEliece, BIKE, HQC. This round aims to expand the set of algorithms for secure key transfer, addressing the need for robust cryptographic solutions in the

post-quantum era.

Table 7 provides an overview of the ***four candidates announced by NIST*** for the Standardization Round 4. The table lists the candidate algorithms by type and includes both code-based and supersingular elliptic curve isogeny approaches. The code-based category features BIKE, Classic McEliece, and HQC, while the supersingular elliptic curve isogeny category includes SIKE. These candidates represent potential additions to the post-quantum cryptographic standards, further enhancing the security of key transfer mechanisms.

Table 7: Four algorithms for extra round published by NIST

Type	**PKE/KEM**
Code-based	BIKE, Classic McEliece, HQC
Supersingular elliptic curve isogeny	SIKE

In addition to in July 2023, NIST published a list of digital signature schemes approved to participate in a new competition to choose the standardization of quantum-stable mechanisms.

The list includes 40 schemes (out of 50 submitted) based on various synthesis principles, including problems of lattice theory, coding, hash functions and others. The return is of interest for schemes based on revised isogeny problems of elliptic curves and systems of nonlinear equations, given that as a result of the first NIST competition, the schemes of these classes (SIKE, "Rainbow") were compromised.

Recall that the main reason for the additional round was the fact that the most effective winning schemes of the main stage (Dilithium crystals, Falcon) are based on lattice theory problems, and the third finalist - SPHINCS - is still inferior to them in performance.

As of August 2023, statistically significant data has already been obtained for each of us from the new generation (FuLeeca, KAZ-Sign, LESS, MEDS, Alteq).

Earlier, in August 2023, the following products were released: SPHiNCS+ (SLH-DSA, FIPS 205), Dilithium (ML-DSA, FIPS 204), Cyber (ML-KEM, FIPS 203).

By the very fact of its holding, the NIST competition had a significant impact on the development of methods for the synthesis and analysis of new quantum-stable cryptographic schemes. NIST experts and representatives of the international cryptographic community have analyzed more than 80 candidate algorithms over the past 3 rounds [9].

3 Cloud Computing

Cloud computing is an innovative technology that combines IT resources of various hardware platforms and provides the user with access to them via the Internet. The concept of "cloud computing" originated in 1960, when John McCarthy suggested that computer computing would be performed using "public utilities". Cloud computing may seem such a relatively new phenomenon. However, their history goes back to the early 1950s, when the advent of mainframes allowed multiple users to access a central computer. The ideology of cloud computing gained popularity in 2007 due to the brisk development of communication channels and the exponentially growing need for both business and private users to scale their information systems [21].

The National Institute of Standardization and Technology of the USA (NIST) has developed recommendations, where it gave a obviously definition of the term cloud computing. According to NIST:

Definition 4. [5] "***Cloud computing*** *is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*"

"Cloud" is a metaphor for a remote computing data center, access to which is provided after depositing pay-as-you-go funds (payment is made for the actual use of computing resources). The software is provided to the user as a service. In this case, the user does not care about the infrastructure, software and security of the cloud. Cloud technologies use computing power, hardware, and disk space located outside the office.

Cloud computing is made possible by a technology known as virtualization. Virtualization allows you to create virtual computers that exist only in digital format, but behave similarly to physical computers with their own hardware. The term "virtual machine" is used to refer to such virtual computers. When implemented correctly, virtual machines on the same host computer are isolated from each other, ensuring data security and privacy.

Virtual machines also make efficient use of hardware, allowing you to run multiple virtual "servers" on a single physical server. This makes data centers more scalable and able to serve more customers. Cloud providers can provide access to their servers to more customers at the same time, which reduces the cost of services. Cloud servers typically provide continuous availability by using backups of their services on multiple computers and in different regions. Users can access cloud services through a web browser or special applications by connecting to the cloud via the Internet from any device.

Figure 2 illustrates conceptual illustration of cloud computing, showing various components and services associated with it.

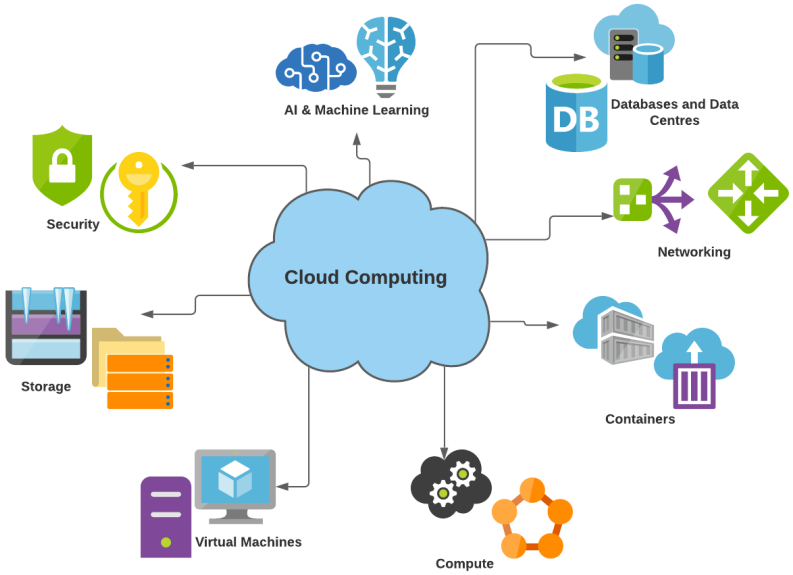

Figure 2: Conceptual illustration of cloud computing [42].

Cloud computing consists of three main components: front-end, back-end, and network. The cloud stores software that stores data on the server and provides access to it over the network. An front-end component is a user computer or client device that can access data in the cloud through specialized software for network or cloud computing.

The back-end part includes the server, the operating system, and the storage devices on which the data is hosted. These server components provide secure data storage and handle user requests.

The network component provides communication between devices connected to cloud computing, in accordance with the rules of the protocol. The network software uses middleware to ensure continuous communication between devices and computers through cloud computing.

Figure 3 illustrates the general scheme of cloud computing, including its main components.

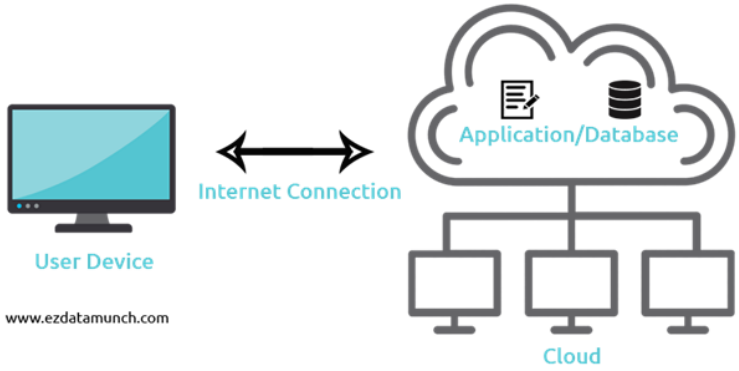

Figure 3: The scheme of cloud computing [37].

3.1 Characteristics and models of cloud computing

According to NIST definition, the cloud model supports high availability of services and is described by five major characteristics, three service delivery models and four deployment models.

3.1.1 Major characteristics

On-demand self-service. The consumer has the opportunity to access the computing resources provided unilaterally, as needed, automatically, without the need to interact with the employees of each service provider. The user can independently create, modify and delete virtual machines, data warehouses or other computing resources through the web interface of the cloud provider. For instance, a user can instantly create a new virtual server on Amazon Web Services (AWS) and start using it without having to contact technical support. The user can create a new virtual server in the cloud using the Microsoft Azure platform by selecting the necessary characteristics (for example, the number of processors, memory and operating system) and starting the deployment process in a few clicks.

Broad network access. Resources are accessible over the network and can be used using standard mechanisms that support various client platforms, including mobile devices, tablets, laptops and workstations. Cloud computing allows users to access their data and applications from anywhere in the world with internet access. For example, using Google Drive, a user can store their documents in the cloud and access them from any device connected to the Internet. Employees of the company can access cloud applications and data from anywhere with an Internet connection using the Salesforce web interface for customer relationship management (CRM) or the Office 365 platform for working with documents and email.

Resource pooling. Vendor computing resources are pooled to serve multiple users using a multi-tenant model in which different physical and virtual resources are dynamically assigned and reassigned depending on user needs. The user usually does not know the exact location of the resources, but can specify the

preferred data processing location at a higher level of abstraction. Cloud computing allows providers to pool computing resources from various physical servers to ensure scalability and fault tolerance. To give an example, VMware virtualization allows you to create virtual servers based on physical servers combined into a single computing environment. A cloud service provider can combine computing resources from multiple data centers to create a cloud infrastructure capable of serving global customers. For example, Amazon Web Services (AWS) combines servers from different regions to ensure high availability and fault tolerance.

Fast Elasticity. Resources can be quickly scaled up and down depending on the changing needs of users. The user has access to virtually unlimited resources that can be used as needed. Cloud computing provides flexibility and quick adaptation to changing business needs. In particular, if the load on a website suddenly increases, the cloud computing provider can automatically scale computing resources to ensure stable performance. An e-commerce website can automatically scale its infrastructure in the cloud during peak load during sales or holiday seasons to ensure fast order processing and avoid site disruptions.

Measurable Service. Cloud systems automatically monitor and optimize resource usage, providing the user with transparency and the ability to track and report on resource consumption at various levels of abstraction. Cloud computing provides transparency in the use of resources and payment for them. Namely, a user can track the amount of computing resources used in the cloud provider's control panel and receive detailed cost reports. A cloud computing user can track the amount of resources used (for example, processor time, storage capacity, and network traffic) and pay only for actual usage. For example, the Google Cloud Platform provides detailed resource usage reports for easy monitoring and cost analysis [5].

3.1.2 Deployment models

Public cloud. Public cloud is an infrastructure designed for free use by the general public. A public cloud can be owned, managed, and operated by commercial, scientific, and government organizations (or some combination thereof). The public cloud physically exists in the jurisdiction of the service provider owner. The public cloud is a computing service offered by third-party providers over the Internet. Unlike a private cloud, access to public cloud services is open to anyone who is interested in using or purchasing them. These services can be provided free of charge or available on request, with users paying only for the actual use of processor, storage, or bandwidth resources. Public clouds can significantly save enterprises the cost of purchasing, managing and maintaining on-premises infrastructure, since the cloud service provider is responsible for the entire infrastructure. They also provide the flexibility to scale DRAM memory and bandwidth, allowing businesses to easily expand their storage based on needs. Examples: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP). For instance, a startup can deploy its web platform on AWS, using virtual machines to host its website and database.

Private cloud. Private cloud is an infrastructure designed to be used by a single organization that includes several consumers (for example, departments

of one organization), possibly also by customers and contractors of this organization. A private cloud can be owned, managed and operated by both the organization itself and a third party (or some combination thereof), and it can physically exist both inside and outside the jurisdiction of the owner. A private cloud provides computing services through an internal OT infrastructure for use exclusively within a single organization. Also known as an enterprise cloud, it is usually managed by internal resources and remains inaccessible to third parties. Unlike the public cloud, private clouds have all the advantages such as flexibility, scalability and self-service capability, but at the same time provide an additional layer of control, security and personalization. They provide an increased level of security through the use of internal firewalls and hosting, which guarantees the confidentiality of the organization's data. However, the disadvantage of private clouds is the need for independent management and maintenance of data centers, which can require significant resources and efforts on the part of the organization. Examples: VMware vCloud, OpenStack. For instance, a large corporation may use a private cloud to store and process sensitive data such as financial records or intellectual property. Private cloud customers receive the main benefits of the public cloud, including self-service, scalability and adaptability, but also have the ability to additional control and configuration. In addition, private clouds can have a higher level of security and privacy because they are hosted on private networks that are inaccessible to public traffic.

Hybrid cloud. Hybrid cloud is a combination of two or more different cloud services. infrastructures (private, public or public) that remain unique objects, but are interconnected by standardized or private data transfer technologies and applications (for example, short-term use of public cloud resources for load balancing between clouds). The best of both cloud model provides flexibility in redistributing workloads between private and public clouds, depending on changing computing requirements and costs. At times of fluctuating demand for computing resources and data processing, the hybrid cloud allows companies to scale their on-premises infrastructure to the level of the public cloud to cope with increased workload, while protecting their data from third-party data centers. In the hybrid cloud computing model, companies pay only for resources that are used temporarily, instead of purchasing and maintaining resources that may remain unused for a long time. In this way, the hybrid cloud provides the benefits of a public cloud while minimizing security risks. Confidential services and applications can be stored in a secure private cloud, while public web servers and client endpoints can be hosted in a public cloud. Most popular third-party cloud service providers offer a hybrid cloud model that allows users to combine private and public clouds to meet their needs. This gives companies more flexibility when deploying an application that has special infrastructure requirements. Examples: IBM Cloud, Oracle Cloud. For instance, a large enterprise may use a private cloud to store sensitive data, and a public cloud to handle large amounts of traffic or temporary projects, such as launching a grocery site on sale.

Community cloud. Community cloud is a additional type of infrastructure designed for use by a specific community of consumers from organizations with common objectives (e.g., mission, security requirements, policies, and compliance with various requirements). A public cloud may be cooperatively owned, man-

aged, and operated by one or more of the community organizations or a third party (or some combination thereof), and it may physically exist both inside and outside the jurisdiction of the owner. The main difference between a hybrid cloud and a Community cloud is the use of multiple cloud computing capacities and data storage resources in a single architecture [5] .

Figure 4 shows the types of cloud computing based on two different models.

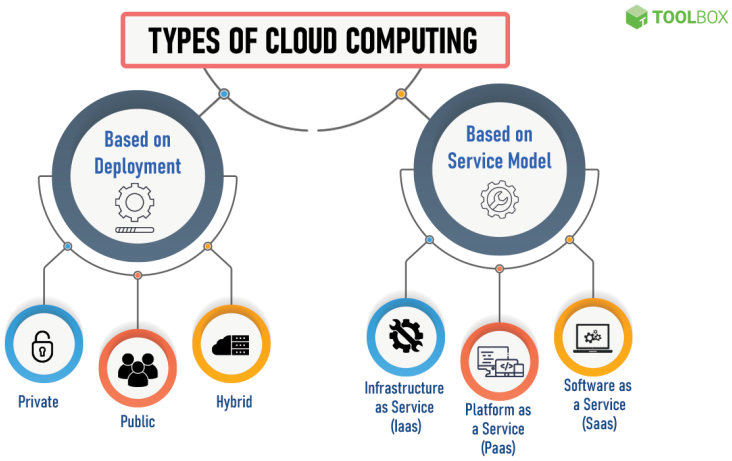

Figure 4: Type of of cloud computing [38].

3.1.3 Service models of service provision

Cloud Platform as a Service (PaaS). The consumer is provided with the means to deploy applications created by the consumer or purchased on the cloud infrastructure, developed using tools and programming languages supported by the provider [42]. The Platform as a Service (PaaS) solution is based on virtualization technology. PaaS solutions are a dynamically developing area of cloud computing, focused primarily on web developers. PaaS solutions simplify the development and deployment of scalable web applications and save programmers' labor costs. However, in return for additional convenience, developers should be willing to cede some of the low-level control of the system to a cloud provider.

PaaS provides customers with access to the development tools they need to create and control mobile and web applications. At the same time, customers do not need to invest in the creation or support of infrastructure. The cloud solution provider hosts infrastructure and middleware components, and the customer gets access to these services through a web browser. To improve performance, PaaS solutions must contain ready-made software components that enable developers to add new features to applications, including advanced technologies such as artificial intelligence (AI), chatbots, blockchain, and the Internet of Things (IoT). A well-chosen PaaS solution should also include solutions for analysts, end users, and IT administrators, including big data analytics, content management, database management, system management, and security [39].

Examples are, e.g.:

- Heroku: Heroku provides a platform for developing, deploying and scaling web applications using languages such as Ruby, Node.js and Python.

- Microsoft Azure App Service: This service offers a managed platform for the development and deployment of web applications, mobile applications and APIs.
- Google App Engine: Google App Engine allows developers to create and deploy scalable applications using Google infrastructure.

Cloud Infrastructure as a Service (IaaS). The consumer is provided with data processing, storage, networking and other basic computing resources on which the consumer can deploy and execute arbitrary software, including operating systems and applications. The consumer does not manage or control the cloud infrastructure itself, but can control operating systems, storage facilities, deployed applications and, possibly, have limited control over selected network components [25].

IaaS provides customers with on-demand access to infrastructure services over the Internet. The main advantage is that the cloud solution provider hosts infrastructure components that provide computing, data storage, and network bandwidth so that subscribers can perform their workloads in the cloud. A subscriber to a cloud solution provider is usually responsible for installing, configuring, securing, and maintaining any software in cloud native solutions, such as database, middleware, and application software.

Examples are, e.g.:

- Amazon Web Services (AWS): AWS provides a wide range of IaaS services, including Amazon EC2 (virtual servers) and Amazon S3 (data warehouse).
- Microsoft Azure: Azure offers virtual machines, Blob storage and many other services for infrastructure and application deployment.
- Google Cloud Platform (GCP): GCP includes Compute Engine (virtual machines), Cloud Storage and other services.

Cloud Software as a Service (SaaS). The consumer is provided with software tools - provider applications running on cloud infrastructure. Applications are accessible from various client devices through a thin client interface such as a browser. The consumer does not manage or control the cloud infrastructure itself on which the application is running, whether it is networks, servers, operating systems, storage systems or even some application-specific capabilities. In some cases, the consumer may be given the opportunity to access some user configuration settings [5].

SaaS is a software delivery model in which a cloud solution provider hosts the customer's applications. The customer gets access to these applications via the Internet. Instead of spending money on creating and maintaining its own computing infrastructure, the SaaS customer uses a subscription to the service, which is paid in proportion to the volume of use. For many companies, the SaaS model is optimal because it allows you to get started quickly using the latest innovative technologies. Automatic updates reduce the load on internal resources. Customers can scale services to support ever-changing workloads by adding and removing services and features according to business needs. The modern suite of cloud applications contains software for any business needs, such as customer satisfaction, customer relationship management, customer service,

enterprise resource planning, procurement, financial management, human capital management, human resources management, payroll, supply chain management, enterprise work planning and much more [21].

Examples are, e.g.:

- Google Workspace: Google Workspace provides a comprehensive set of cloud applications for organizations such as Gmail, Google Docs and Google Drive.
- Microsoft Office 365: Office 365 provides a wide range of office applications, including Word, Excel and PowerPoint, available over the Internet.
- Salesforce: Salesforce offers cloud-based CRM applications for sales, marketing and customer service management.

Figure 5 (diagram) in the form of a pyramid shows how the service models of a cloud service system are depicted.

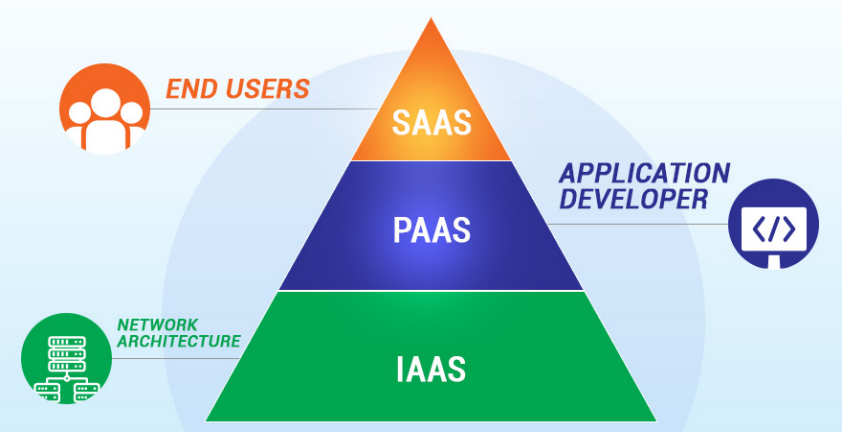

Figure 5: The general scheme of service models [43].

Figure 6 illustrates a service model with sample applications:

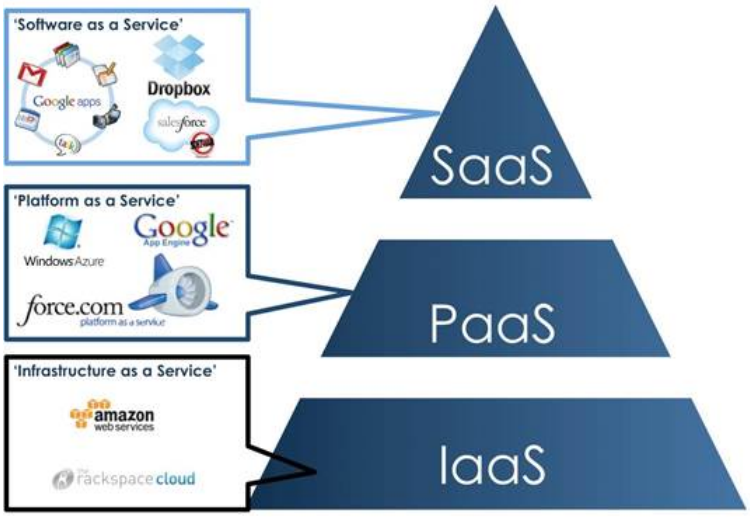

Figure 6: The general scheme of service models with examples [40].

The dynamic properties of cloud computing lay the foundation for new higher-level services. Figure 7 shows cloud computing services.

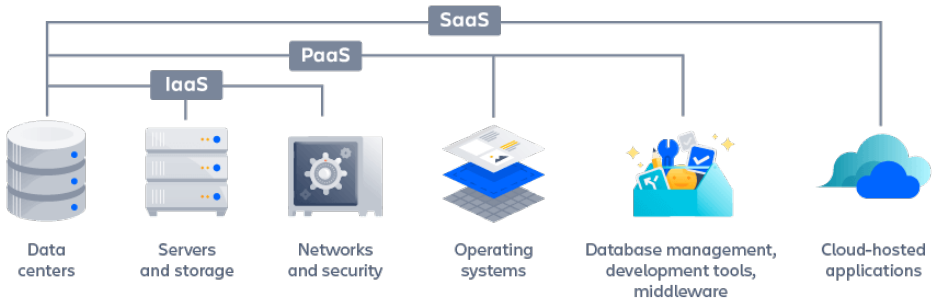

Figure 7: Type of of cloud computing [39].

3.2 Strengths and weaknesses of cloud computing

Cloud computing has a number of advantages over traditional computing methods, such as:

Cost reduction. Cloud computing allows you to reduce the cost of computing resources, since users pay only for the resources they use. Also, cloud computing allows companies to reduce capital costs by using cloud provider infrastructure instead of their own. For example, companies can avoid the cost of purchasing and maintaining servers, network hardware, and software if they use cloud services such as Amazon Web Services (AWS) or Microsoft Azure.

Increased efficiency. Cloud computing allows you to increase the efficiency of computing resources, because cloud service providers can optimize the use of these resources.

Scalability. Cloud services offer flexibility and scalability, allowing you to quickly adapt to changing business needs. For example, with increasing demand for a web application, you can easily scale it using cloud services to ensure high availability and performance.

Flexibility. Cloud computing offers a wide range of services and capabilities that can be customized to meet the specific needs of the company. For example, Google Cloud Platform provides various services, including computing power, data storage, databases, artificial intelligence and machine learning.

Global Availability. Cloud services are available worldwide, allowing companies to operate and expand globally. For example, Salesforce provides cloud-based CRM services that can be easily scaled and used between different offices and departments of the company around the world.

Furthermore, cloud computing has a number of issues that need to be considered, such as:

Internet addiction. Using cloud computing requires constant internet access. For example, if a network connection fails or a network failure occurs, access to cloud services may be limited or completely lost.

Security. Cloud computing can pose a security risk because user data is stored on remote servers. Storing data in the cloud can raise concerns about security and privacy. For example, data security incidents such as data leaks or hacker attacks on cloud provider servers can lead to serious consequences for a company.

Compliance issues. Some industry regulatory requirements may limit the ability to use cloud computing due to data security requirements or regulatory compliance. For example, organizations working with confidential medical information (PHI) or personal data may face restrictions in using cloud services due to HIPAA or GDPR requirements.

Provider dependency. Companies using cloud computing are becoming dependent on their cloud providers. For example, if a cloud service provider decides to change its pricing policy or terms of service, this may affect the company's business processes and costs.

Performance issues. Insufficient network or cloud provider server performance can lead to delays or problems accessing cloud applications or data. For example, if many users access a cloud service at the same time, this can lead to server overload and reduced performance.

Examples of the strengths and weaknesses of cloud computing may vary for different organizations and use cases. Therefore, it is important to carefully weigh all aspects before deciding on the transition to cloud computing [21].

3.3 Cloud computing in industry

Cloud computing is used in various fields of computer science, namely [41]:

IT and telecommunications. Cloud computing is widely used in the field of information technology and telecommunications to provide various IT services. For example, Amazon Web Services (AWS) provides virtual servers, data storage, and tools for application development and testing. Organizations can use cloud computing to manage their IT infrastructure without having to purchase and maintain their own hardware.

Finance and business. Cloud computing is used in business to increase efficiency and reduce costs. For example, cloud computing is used to store data, process transactions, and provide business applications. Financial institutions can use cloud computing to process transactions, analyze risks, provide online banking and other financial services. For example, Salesforce Financial Services Cloud provides cloud solutions for managing customer relationships and automating business processes in the financial sector.

Education. In the educational field, cloud computing is used to provide access to educational resources and applications from anywhere in the world. Cloud computing is used to create virtual labs and to store large datasets. For example, Google Workspace for Education provides cloud-based learning and collaboration tools for students and teachers.

Healthcare. Cloud computing is used in healthcare to store and process medical data, including electronic medical records, images, and test results. Cloud computing is used to create electronic medical records and to conduct medical research. For example, the Microsoft Azure platform provides cloud solutions for the development and deployment of medical applications and telemedicine services.

Research and Science. In the scientific field, cloud computing is used for analyzing and processing large amounts of data, modeling complex systems and simulating scientific experiments. For example, the Google Cloud Platform provides cloud resources for research and development of new technologies.

Production. In the manufacturing sector, cloud computing is used to monitor and manage production processes, optimize supply chains, and implement Internet of Things (IoT) systems to collect and analyze production data. For example, General Electric uses cloud technologies to manage its manufacturing operations and monitor the condition of its equipment.

Retail trade. In the retail sector, cloud computing is used to manage e-commerce, analyze purchase data, and provide personalized customer services. For example, Shopify provides cloud platforms for creating and managing online stores, and Adobe Commerce Cloud provides tools for managing customer relationships and executing marketing campaigns.

Cloud services such as AWS, Microsoft Azure, and Google Cloud provide tools for developing, testing applications, storing and processing data, also, analyzing information. In a general sense, cloud computing opens up new opportunities for the development of computer science and improving the work of IT specialists.

As a consequence, cloud computing is an important tool for IT professionals in the field of computer science. They provide extensive opportunities for creating, deploying and scaling applications, working with data and analyzing information.

4 Selection and analysis of scientific papers

In this chapter, we outline the methodology employed for the selection and analysis of scientific papers that form the basis of this research. The process involves several key steps to ensure a comprehensive and unbiased review of relevant literature. After identifying a group of relevant papers, each of them was analyzed based on its annotation, methodology, results and conclusions. A critical assessment of the reliability of the results was carried out. This included evaluating the study design, data collection methods, and statistical analysis used in the studies. The analysis also included the identification of common themes, trends and gaps in the existing literature. Special attention was paid to the proposed cryptographic algorithms and their effectiveness in post-quantum scenarios. In addition, any contradictory results or controversies in the literature were highlighted and discussed. Through careful selection and analysis of these scientific papers, this section provides a solid foundation for understanding the current state of research and identifying areas that require further study. The conclusions drawn from this literature review will serve as a guide for the subsequent phases of the research project, ensuring that the research is based on the most relevant and reliable scientific data.

4.1 Paper selection

Firstly, a systematic search was conducted using multiple academic databases such as IEEE Xplore, SpringerLink and Wiley Online Library. Keywords related to the research topic were carefully chosen to capture a wide range of studies. These keywords included specific terms relevant to the field, such as "quantum cryptography," "post-quantum cryptography," "cloud data security," "cryptographic algorithms," and "quantum computing."

4.1.1 Phase 1: Search strategy and database selection

To create a database of scientific papers, it is necessary to start with the selection of verified and reputable sources. The following electronic libraries were selected as preferred online resources:

1. IEEE Xplore is a digital library that provides access to full–text articles on electrical engineering, computer engineering and electronics published in journals, conference materials and IEEE and IET standards.
   `https://ieeexplore.ieee.org/Xplore/home.jsp`

2. SpringerLink is a platform that provides access to journals, books, protocols and reference materials on all scientific disciplines published by Springer.
   `https://link.springer.com/`

3. Wiley Online Library is a platform providing access to journal articles, books, and reference materials published by Wiley covering the natural, social, and human sciences.
   `https://onlinelibrary.wiley.com/`

Since the subject of our interest were articles covering two main areas: *post-quantum cryptography and cloud computing*, queries to search for such articles were generated using the logical operators "AND" and "OR". This provided

a more accurate search by name and a deeper understanding of our queries by search engines.

After reviewing all applications and evaluating the number of scientific papers found, at the second stage we proceed to determine the selection criteria.

The developers of the IEEE Xplore search engine recommend using the "*" symbol to improve the search and get more accurate results.

4.1.2 Phase 2: Selection criteria

After we will outline the selection criteria based on the following aspects:

- *Relevance:* Only those articles that directly related to the main issues and topics of the study were considered. The relevance of the article was determined on the basis of the sections "Abstract", "Introduction" and "conclusion".
- *Novelty:* In order to ensure the inclusion of the most relevant results, preference was given to articles published within the last five years. This criterion is crucial in rapidly developing fields such as cryptography and quantum computing.
- *Reliability:* The reliability of the articles was ensured by selecting only those that were published in peer-reviewed journals and conference proceedings with an authoritative reputation. This criterion helps to maintain the quality and reliability of research results.

The selection of scientific articles was carried out on the basis of a number of strict criteria designed to ensure the relevance, reliability and quality of the selected literature.

Inclusion Criteria:

1. *Papers from peer-reviewed sources.* Papers should be published on verified resources, that is, on verified or from common electronic library sites.
2. *Papers that specifically focus on post-quantum cryptography.* The works directly related to post-quantum cryptography are selected, taking into account the significant differences between quantum and post-quantum cryptography.
3. *Papers that specifically focus on cloud computing.* Preference is given to papers that cover both post-quantum cryptography and parallel cloud computing, as the dissertation research focuses on the integration of these two areas.
4. *Papers written in English and published up to 2024.*

Exclusion Criteria:

1. *Papers from not peer-reviewed sources.* Papers from unverified sources or electronic library sites that do not have sufficient academic reputation are excluded.

2. *Papers that specifically focus on quantum cryptography.* Due to the significant differences between quantum and post-quantum cryptography, works focused on quantum cryptography are not considered, as they consider other methods and means of protection.

3. *Papers that not specifically focus on cloud computing.* Publications focused on other areas, such as blockchain, artificial intelligence or web technologies are excluded, since these topics do not correspond to the focus of our research.

4. *Duplicated publications.*

4.1.3 Phase 3: Final papers selection

After the second stage of selection, based on predefined criteria, titles and keywords, we eliminated all duplicate articles and selected a total of 21 articles. After determining the group of relevant articles, a thorough analysis of each of them was carried out in step 3.

At the third stage, we studied the articles themselves in detail to determine their relevance to the subject of our research. We made a review of the annotation and introduction. The abstract of each papers was analyzed for its relevance, after which a detailed study of the introduction was conducted to evaluate the research plan of the methods used. Common themes, trends and patterns in the selected articles were identified and summarized. This generalization allowed us to get an idea of the current state of research, highlight significant achievements and identify gaps in the existing literature.

As a result of a more thorough analysis, at the third stage, 6 papers were selected that most fully correspond to the stated research topic.

Table 8 clearly shows all the stages of selection and the number of articles that have passed each stage.

Table 8: Number of papers obtained for each stage of the literature review.

Databases	Amount of papers		
	Phase 1	***Phase 2***	***Phase 3***
IEEE Xplore	76	17	6
Springer Link	108	4	0
Wiley Online Library	91	0	0
Total	275	21	6

This table illustrates the process of selecting scientific publications, starting with the initial search and ending with an in-depth analysis, which resulted in the selection of the most relevant articles for our research.

4.2 Descriptions of scientific papers

This section will provide a detailed description of each scientific paper for a more superior understanding of the work and make possible a more complete comparison between the studies. By carefully examining the algorithms (which have been described in general terms), the results and conclusions of each article, we aim to highlight their contributions to areas such as post-quantum cryptography and cloud computing, identify their unique approaches and evaluate their relative strengths and weaknesses collectively. This detailed analysis will not only clarify the significance of each stay, but also provide a clear basis for assessing their impact and interrelationship in the broader context of the scientific field.

4.2.1 First paper: *"Recent Developments and Methods of Cloud Data Security in Post-Quantum Perspective"*

First research paper was written by Shaik Mohammed Ilias and V.Ceronmani Sharmila from the Hindustan Institute of Technology and Science [58] examines modern methods and developments in the field of data protection in cloud systems, paying special attention to the prospects of post-quantum cryptography.

The authors emphasize that cloud technologies have changed the approach to the use of computing resources, providing opportunities to save money, eliminate data redundancy, scalability and compliance with regulatory requirements. However, these benefits come with significant security concerns. For example, with the development of quantum computers, traditional cryptographic methods are becoming vulnerable. Post-quantum cryptography aims to develop schemes that are resistant to both classical and quantum attacks. The paper provides examples of current developments in the field of post-quantum cryptography and hybrid systems. Projects and initiatives aimed at integrating post-quantum algorithms into existing security systems are described.

The authors identify the following scenario in which it is necessary to improve the methods of protecting cloud data, taking into account the possibilities of post-quantum cryptography. They consider the interaction of three key actors: the data owner, the cloud service provider (CSP), and the data user. With the growing use of cloud technologies and an increase in cyber attacks, reliable data protection is required. Clouds provide various forms of data storage: structured, unstructured and semi-structured. For each of these forms, there are specific security issues related to confidentiality, authenticity, integrity, authorization, non-repudiation and novelty of data. The authors discuss both external threats and internal attacks from CSP.

Paper also focused on lightweight cryptographic schemes, which are especially relevant for sensor networks. Various lightweight algorithms are given, such as lightweight homomorphic encryption, hybrid encryption, and searchable encryption. The article details the key characteristics of these methods. The authors outline that various methods of lightweight cryptography have different approaches to the structure, block size and key. They are used in different security scenarios. The authors also clearly showed in the paper different categories lightweight encryption schemes.

The authors divided the lightweight schemes into categories and presented them in Figure 8.

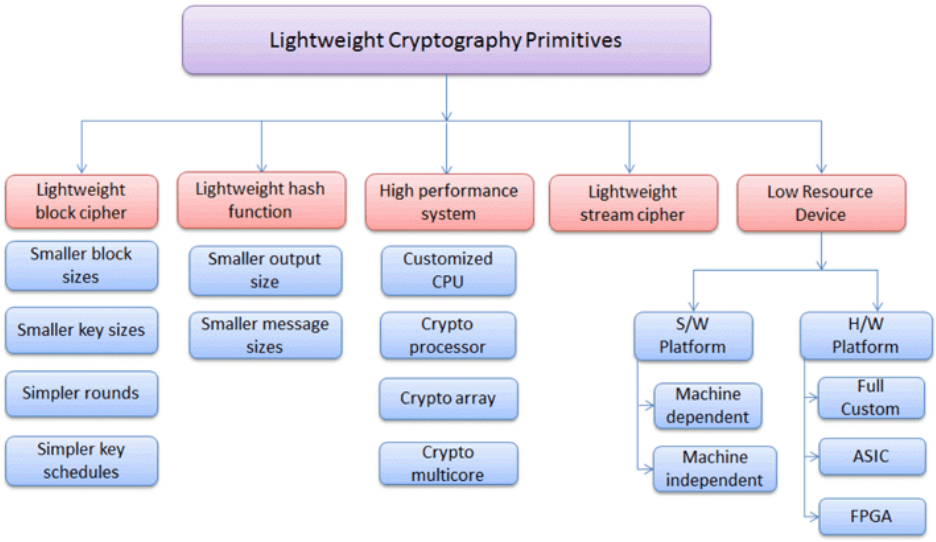

Figure 8: Different categories lightweight encryption schemes [58].

Authors reviewed modern hybrid cryptographic schemes designed to improve the security of cloud data and compared them with post-quantum methods that are still under processing. The following algorithms are presented in the work:

- Hybrid schemes: Include combinations of algorithms such as MD5 and Blowfish, RSA and AES, and others. Hybrid schemes offer a higher level of security compared to traditional methods.
- Methods for post-quantum security: Schemes such as Supersingular Diffie-Hellman Isogeny (ECDH), which provide security in the context of using quantum computers, are considered.

The authors highlight several important gaps in the paper: The need to optimize algorithms such as SIDH. Vulnerability of traditional cryptographic schemes to quantum attacks. Insufficient elaboration of hybrid approaches to ensure the security of cloud data.

In conclusion, this article represents an important contribution to the field of cloud data security, especially in the context of the growing threat of quantum computing. The authors offer an overview of current methods and indicate the need for further research to ensure reliable data protection in post-quantum cryptography. The article emphasizes the need to develop comprehensive approaches to data security that take into account the threats of the post-quantum era. The authors plan to develop a security system that would ensure data protection at rest, during transmission and during data analysis. Future research will focus on creating a platform that meets the needs of data owners, data users, and CSPs [58].

4.2.2 Second paper: *"Towards Cloud-based Infrastructure for Post-Quantum Cryptography Side-channel Attack Analysis"*

Authors of the next research paper Tristen Teague, Mayeesha Mahzabin, Alexander Nelson, David Andrews and Miaoqing Huang from the University of Arkansas

[59], explore the creation of a cloud infrastructure for analyzing side channel attacks (SCA) on post-quantum cryptographic (PQC) algorithms. The main goal of the work is to reduce barriers to SCA research in order to obtain safe and reliable PQC implementations faster.

Side-Channel Attack (SCA) is a method that attackers use to break into security systems without trying to crack the cipher itself. Instead, they observe the physical behavior of the device during operation. To put it another way even if the algorithm is mathematically protected, its physical implementation may leak information (for example, energy consumption, electromagnetic radiation), which may allow attackers to recover secret data. This highlights the need to protect not only the mathematical, but also the physical implementation of algorithms.

In this paper, authors described the idea of creating an open research infrastructure for analyzing side-channel attack on post-quantum cryptography algorithms. This includes:

- Development of tools for performing SCA analysis on various devices.
- Providing remote access for researchers through a web portal.
- Automation of the analysis process, including data collection, leak assessment and report generation.

In the article, the authors reported about the major components of this infrastructure. It consists of the following:

- *Client Interface:* Allows users to download implementations of cryptographic algorithms, create analysis tasks, manage the process and get results.
- *Server:* Processes tasks, manages resource allocation and data storage.
- *Sandbox computer:* Manages test benches and executes scripts for data collection and analysis.
- *Test benches:* Include oscilloscopes and Chip Whisperer devices for collecting data on energy consumption and electromagnetic emissions.

In this article, the authors analyzed side channel attacks (SCO) on post-quantum cryptographic (PC) algorithms and identified several analysis methodologies. In the paper, the methodology includes several key components and steps:

Leak Test (Test Vector Leakage Assessment - TVLA) is the main method of evaluating information leaks in this work. This method is used to identify information leaks by comparing two sets of measurements: a) a data set with fixed inputs (Tf): This set contains the fixed variables used for the cryptographic operation. b) a set of data with random inputs (Tr): This set contains the same variables as the fixed set, except for one random variable. TVLA calculates a single-sample t-test (Welch's t-test) for two sets of measurements to determine if there are significant differences between them. If the absolute value of the t-test exceeds the threshold value, this indicates a possible information leak.

Welch's single-sample t-test is a statistical test used to test the hypothesis that the averages of two samples are equal, especially when the variances of these samples are not equal. In the context of Side Channel Attack Analysis (SCA), this test is used to identify information leaks by comparing two sets of data [17].

They have identified several limitations in the methodology: Limited oscilloscope buffer size: Complete measurements of complex algorithms may be difficult due to the limited memory size of the oscilloscope.

Test vectors: Errors in the creation of test vectors are possible, which can lead to false conclusions about information leaks.

The analysis process was as follows:

Creating a task. The user downloads the algorithm implementation via the web interface and sets the analysis parameters (for example, device type, number of traces).

Data collection. A sandbox computer controls test benches, runs cryptographic operations on target devices, and collects data on energy consumption or electromagnetic radiation.

Data analysis. The collected data is transferred to a sandbox computer where TVLA is running to determine if there are information leaks. TVLA involves comparing datasets with fixed and random inputs.

Generating reports. The results of the analysis are generated in the form of a report, which is provided to the user via the web interface. The report includes graphs and text conclusions demonstrating the presence or absence of information leaks.

Moreover, authors provided the results of the analysis in the paper. They tested the CRYSTALS-Kyber algorithm on an FPGA and an STM32F4 microcontroller. Two versions of the algorithm have been developed and tested - unmasked and masked. TVLA showed that the unmasked version of the algorithm had leaks, whereas the masked version was leak-proof.

To sum up, the work represents a significant contribution to the field of post-quantum cryptography research and analysis of side-channel attacks. The proposed infrastructure allows researchers and industry to test and improve the security of cryptographic algorithms, which is especially important in the context of protecting critical infrastructure such as power grids. For the future works of the authors, it is planned to expand the infrastructure, including the addition of new platforms and the use of electromagnetic radiation analysis. It is also planned to fully automate the process - from uploading user data to providing analysis results [59].

4.2.3 Third paper: *"PQC Cloudization: Rapid Prototyping of Scalable NTT/INTT Architecture to Accelerate Kyber"*

A research paper from Microsoft is devoted to the creation of a scalable architecture of numerical theoretical transformation (NTT) to accelerate the CRYSTALS-Kyber algorithm [60]. The work is aimed at improving the security of cloud computing in the face of threats from quantum computers, and developing a scalable and high-performance architecture to accelerate the operation of Cyber, one of the key PQC algorithms, taking advantage of parallelism and cloud computing. In the article, the authors used the following technology and methodology: The numerical-theoretical transformation (NTT) is an algorithm used to speed up polynomial multiplication operations, especially in the context of lattice-based cryptographic algorithms [53]. NTT is used for efficient multiplication of polynomials in lattice cryptography. High-level Synthesis (HLS) this is a methodology for designing digital systems that allows you to describe hardware designs using high-level programming languages Used for rapid prototyping of hardware solutions [18]. HLS allows you to describe algorithms at a high level and automatically

generate optimized hardware code.

The NTT architecture is divided into three levels:

1. Butterfly Core Level. The architecture uses reconfigurable butterfly cores that support both Cooley-Tukey (CT) and Gentleman-Sande (GS) operations. This allows to use the same structure for NTT and IT. Cooley-Tukey is used to convert a polynomial from a time domain to a frequency domain. And Gentleman-Sande is used for reverse conversion from the frequency domain to the time domain. The Cooley-Tukey and Gentleman-Sande operations are key components in the implementation of the numerical-theoretical transformation (NTT) used in cryptographic algorithms. Their correct application allows to effectively speed up calculations and optimize the use of hardware resources. Butterfly cores include three registers for data input and two for output, which provides a delay of two cycles.

2. Stage Level. They are used to eliminate memory access restrictions during iterations of stages. This allows you to process several stages in parallel. The passage of all stages for a polynomial takes time proportional to the number of butterfly nuclei and the degree of the polynomial. For example, for degree 256 and 128 butterfly cores, one stage takes two cycles, and the entire NTT operation takes 14 cycles.

3. The Polynomial Level. The use of pipelines makes it possible to effectively use the architecture of stages by feeding polynomials to the last stage of the previous one. The performance of calculations at the polynomial level is determined by the number of butterfly cores and the parameters of the polynomial. For example, 64 or 128 butterfly cores are used for the Cyber parameter set.

The general architecture of Kyber: The NTT core - to speed up computing. The multiplier of the coefficients of a polynomial is used to perform multiplications of polynomials. Keccak-f [1600] - for cryptographic hash functions. Binomial Centered Distributor (CBD) - for generating random numbers. Rejection sampler and compression/decompression units - to ensure the efficiency and safety of operations.

The number of butterfly cores can be adjusted depending on the application requirements, ensuring a balance between performance and resources consumed.

Authors achieved the following results: the architecture achieved an acceleration of 11 times compared to existing solutions. NTT calculation for a polynomial of degree 256 takes only 14 cycles. Despite the high performance, the use of the HLS method leads to a significant increase in resource consumption compared to manual optimizations. The architecture requires about 4 times more resources compared to previous solutions, which is associated with the use of the HLS method.

As a final point paper represents an important step in the field of post-quantum cryptography, offering an efficient and scalable solution to accelerate the operation of key algorithms such as Kyber in cloud computing systems. The proposed architecture significantly improves the performance and security of post-quantum cryptographic algorithms, ensuring their effective deployment in cloud infrastructures. According to the authors, it is planned to investigate side-channel attacks and optimize other components to achieve efficiency comparable to manual RTL implementations [60].

4.2.4 Fourth paper: *"A Multi-Layered Hybrid Security Algorithm Based on Integrity for the Cloud Computing Environment"*

This research paper is devoted to the development of a hybrid security algorithm for cloud computing environments [61]. The paper examines the security problems of data stored in the cloud and proposes a solution based on a multi-layered hybrid algorithm that provides a high degree of data protection and integrity. In the sections also discussed existing research on improving data security in cloud computing. Various approaches were considered, including symmetric encryption (AES and DES), hybrid schemes based on combinations of RSA and AES, as well as information dispersion and hashing methods.

Advanced Encryption Standard (AES) is a symmetric encryption algorithm that has been designed to provide high security and efficiency [35]. AES is the data encryption standard recommended by NIST, and supports key lengths of 128/192/256 bits and data lengths of 128 bits. The algorithm includes 10/12/14 rounds of calculations depending on the length of the key.

Data Encryption Standard (DES) is a symmetric encryption algorithm that has been adopted as an encryption standard [36]. DES has been widely used for several decades, but is now considered obsolete due to the limited key length and vulnerabilities to various attacks. AES is superior to DES in terms of security and efficiency and is the recommended standard for modern encryption systems.

The proposed hybrid security algorithm is a multi-layered hybrid security algorithm (MLS). It was developed using several transformations to increase the level of security in post-quantum cryptography. The algorithm includes data encryption using AES, an information dispersion algorithm (IDA) to ensure data integrity, and hashing to verify data integrity.

The Information Dispersion Algorithm (IDA) is designed to efficiently disseminate information. It divides data into parts and distributes them, ensuring data recovery even if some parts are lost. Hashing is used to verify data integrity and prevent unauthorized changes. The implementation of this hybrid scheme is as follows:

Encoding procedure: The data is encrypted using improved AES. Encrypted data is divided into parts using IDA. Each piece of data is cached and the result is stored in the cloud. These processes ensure data integrity and availability. Figure 10 demonstrates encoding process for secure outsourcing.

Decoding procedure: Enables reverse encoding process for secure data recovery from the cloud. Data integrity verification is performed using hashing, and recovery is performed using IDA. Figure 11 demonstrates the Decoding procedure for secure data retrieval.

The Amazon EC2 and S3 platforms were used for the study. Execution time measurements were carried out for various operations: encryption, decryption, loading and unloading of data. AES showed the best performance compared to RSA and DES, however, ML-HSA was slightly inferior to AES due to a variety of transformations, but superior to RSA and DES. The decryption time is similar, AES was faster than ML-HSA, however ML-HSA provided a higher level of security. The loading and unloading time of ML-HSA was slightly slower than AES, but significantly faster than RSA and DES.

ML-HSA provides a higher level of security compared to traditional schemes, through the use of multiple transformations and hybrid approaches. The algorithm has been tested on AWS platforms and has shown high efficiency with

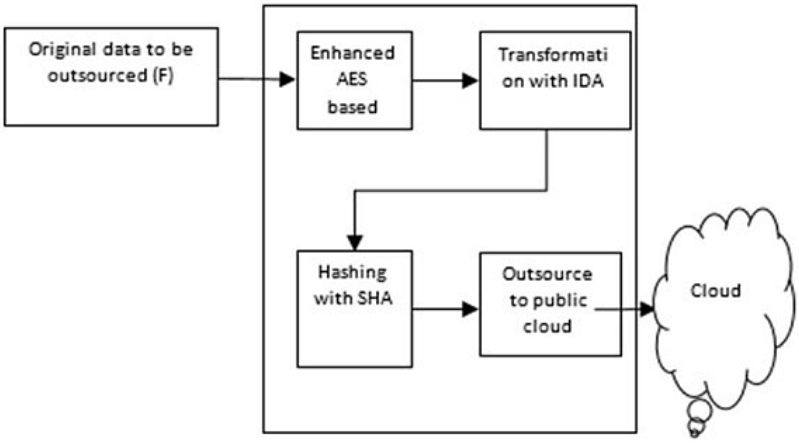

Figure 9: Encoding process [61].

reasonable overhead.

The article significantly enriches the security areas of cloud computing by introducing a new multi-layered hybrid security algorithm that combines encryption, information dispersion and hashing to ensure a high degree of data protection. The experimental results confirm the effectiveness and reliability of the proposed approach, making it a promising solution for cloud systems in post-quantum cryptography. As mentioned in the paper, it is planned to develop a hybrid key exchange scheme necessary to ensure security in multi-user cloud environments. The research will be aimed at further improving the algorithm to increase its efficiency and security in post-quantum cryptography [61].

4.2.5 Fifth paper: *"A Practical Approach to Quantum Resilient Cloud Usage obtaining Data Privacy"*

The paper examines approaches to ensuring data privacy in cloud computing environments in the context of quantum threats [62]. It proposes the use of post-quantum cryptography (PQC) and privacy-oriented technologies such as homomorphic encryption and secure multiparty computing (MPC). As mentioned in the article, homomorphic encryption allows you to perform calculations on encrypted data without decrypting it. Modern schemes include BGV, BFV and GSW. The fourth generation of homomorphic encryption (CKKS) supports secure multi-party computation.

In their paper, the authors propose the use of homomorphic encryption (HE) and secure multiparty computing (MPC) to ensure data security even against cloud providers, and also implement quantum-stable key exchange using lattice-based algorithms.

Secure multiparty computing allows multiple parties to perform computations jointly without revealing their input data. To provide quantum security, a lattice-based key exchange primitive (PQ-OT) is used.

The "dual cloud" model was used, including private and public clouds. The

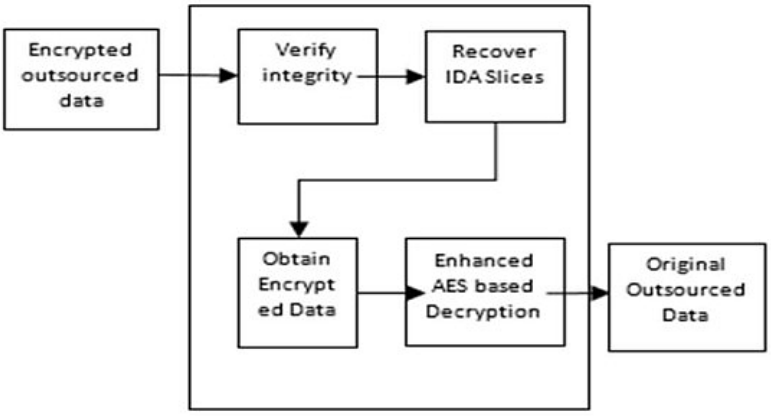

Figure 10: Decoding process [61].

private cloud creates all the necessary components to execute the GC (Garbled Circuits) protocol, while the public cloud performs the calculations. The GC protocol uses AES-256 encryption to secure computations.

The prototype uses the EMP library to implement MPC and PQ-OT for quantum-resistant key exchange. Testing was carried out on a local network with a typical speed of 1 Gbit/s for three scenarios: AES-128 encryption, addition and multiplication of 32-bit integers. Execution time, network traffic, and memory usage were measured for each scenario. The GC protocol has been optimized using the point and permute method, which reduces the number of messages between participants, improving performance and reducing costs. The prototype demonstrated the ability to ensure data privacy in the cloud using quantum-resistant techniques. The prototype showed that quantum-resistant methods can effectively ensure data privacy in cloud computing. The use of MPC and GC protocols provides a high degree of data protection.

According to the authors, further research into cryptographic flexibility (crypto-agility) and testing of various cryptographic schemes is planned. It is of interest to compare the current prototype with other methods, such as homomorphic encryption, to estimate costs and performance [62].

4.2.6 Sixth paper: *"Small Quantum-safe Design Approach for Long-term Safety in Cloud Environments"*

Last paper examines the need to create quantum-resistant cryptographic schemes for long-term data security in cloud environments [63]. The work is aimed at ensuring data security in the face of threats from quantum computing, offering the use of the Camellia block cipher.

Suggested approaches by the authors: 1) Introduction of a quantum-stable data storage architecture based on a block cipher. 2) Using the Feistel Camellia cipher to protect data in cloud storage. 3) Development of a common contribution to the creation of a quantum-secure repository for long-term data security.

A quantum-stable model for long-term security includes confidentiality, integrity, and authentication of data. To ensure data security, block ciphers with increased key sizes and the number of encryption rounds are used. The main

requirement for the model is that data encryption should be efficient enough so as not to cause a noticeable delay in data processing.

The proposed storage architecture includes a data synchronization mechanism, data encryption when stored in storage, and the use of quantum-secure methods to protect data. Encrypted data is synchronized with cloud systems via a secure connection.

The use of post-quantum schemes requires a large amount of computing resources, as the key sizes and the length of encrypted data increase. For long-term data security, it is recommended to use schemes with keys at least 256 bits long.

The input data is divided into blocks of 128 bits, which are encrypted using a secret key. The Camellia cipher supports keys of 128, 192 and 256 bits and uses the appropriate number of rounds of encryption. The encryption process involves splitting data into blocks, encrypting them using a block cipher, and generating encrypted files. The Camellia cipher uses networks of substitutions and permutations to ensure high cryptographic strength. The decryption process is the reverse of the encryption process and involves decrypting encrypted files using a secret key.

In the paper was discussed a scenario in which an attacker tries to hack a data warehouse using a quantum algorithm. The use of quantum algorithms such as Grover's algorithm to crack encryption is seen as a major threat.

As for the results, the performance of the Camellia cipher has been compared with AES for various data block sizes. The results showed that Camellia is slower than AES, but provides higher security due to the increased number of rounds of encryption. Quantum-secure schemes based on symmetric block encryption ensure long-term data security. It is recommended to use 256-bit keys to protect against quantum attacks.

To conclude, article proposes a general architecture for quantum-secure data storage using the Camellia block cipher. The developed approach is suitable for devices with limited resources, such as, IoT and sensor networks, and provides reliable data protection in cloud systems. Future research is planned in improving the functions of the rounds and the implementation of Camellia to improve safety. Further research will focus on the implementation of other PQC candidates and methods to ensure cryptographic flexibility (crypto-agility) [63].

4.3 Comparisons of all research papers

In this section, the key features will be described in detail, as well as a comparative analysis of the six previously reviewed articles. To do this, a table will be used in which the main parameters are presented in a structured way, allowing you to highlight the similarities and differences between them. This approach will allow for a more visual and systematic presentation of information, facilitating the process of understanding and further analysis. The table will include aspects such as research objectives, methodologies used, results, conclusions, as well as the practical significance and possible limitations of each of the articles.

4.3.1 The principal similarities

The similarities of all six scientific articles will be described as follows:

- ***Security topics in cloud computing.*** All six articles are devoted to data security issues in cloud computing environments. The authors strive

to ensure data protection both during transmission and storage. They consider various methods and approaches to protect data from various threats, including quantum computing.

- ***Focus on Post-Quantum Cryptography (PQC).*** All articles discuss the need to use post-quantum cryptographic algorithms to protect data from quantum attacks. In each article, various schemes and methods are proposed to ensure quantum-stable security.
- ***Hybrid Approaches.*** Most papers look at hybrid cryptographic schemes, combining various encryption methods to enhance security.
- ***The need for long-term security.*** The articles focus on the importance of long-term data security, given the rapid pace of development of quantum technologies.
- ***Data integrity and confidentiality.*** All papers emphasize the importance of ensuring the integrity and confidentiality of data in order to prevent unauthorized modification or access. Hashing and authentication methods are used to verify data integrity.
- ***Cryptographic Flexibility.*** The importance of developing flexible cryptographic systems that can adapt to new threats and changes in technology is emphasized. The necessity of regular updating of cryptographic schemes to maintain their resistance to new attacks is discussed.
- ***The need for quantum-stable solutions.*** All papers highlight the critical need to move to PQC to ensure data security in the face of future quantum threats.
- ***Hybrid and multi-layered approaches.*** In all articles, hybrid cryptographic schemes and multi-layered approaches to data security are considered as effective strategies for providing comprehensive protection.
- ***Practical application and testing.*** The importance of practical implementation and testing of the proposed solutions in real conditions is emphasized to assess their effectiveness and reliability.

In-depth analysis shows that all six articles have common goals and objectives aimed at ensuring data security in cloud computing using post-quantum cryptography. Key similarities include a focus on long-term security, the use of hybrid cryptographic techniques, and the development of infrastructure solutions for data protection. These works together form a comprehensive view of current research and approaches in the field of post-quantum cryptography, emphasizing the importance of preparing for quantum threats to ensure data security in the future.

4.3.2 The primary distinctions

As for the differences between these papers, they will be presented in the form of a table to provide a deeper understanding. The tabular format will allow a structured and visual comparison of various aspects of research, such as goals, methodologies, results, conclusions, as well as the practical significance and limitations of each of the articles. This approach will facilitate the analysis and

identification of the unique features of each work, contributing to a more comprehensive perception of their contribution to the relevant scientific fields. Table 9 demonstrate a comparing the distinctive features of 6 articles.

Table 9: Main differences of the articles

№	Target application area:	Approaches to the implementation of security	Used specific cryptographic algorithms and methods	Results
[58]	It is aimed at sensor networks and Internet of Things (IoT) devices, where lightweight and energy-efficient cryptographic schemes are important	Focuses on lightweight cryptographic schemes and hybrid methods to improve cloud data security	Lightweight cryptographic schemes, Hybrid schemes, Supersingular Isogeny Diffie-Hellman (SIDH)	It has been proven that lightweight cryptographic schemes and hybrid encryption methods can significantly improve data security in cloud computing environments in the era of post-quantum cryptography.
[59]	It focuses on the infrastructure for analyzing side-channel attacks, which is important for research and academic environments, as well as for developers of hardware and software solutions	Explores the creation of an infrastructure for analyzing side-channel attacks on PQC algorithms.	TVLA (Test Vector Leakage Assessment), CRYSTALS-Kyber, ChipWhisperer	An infrastructure has been created and tested to analyze side-channel attacks on post-quantum cryptographic algorithms and it allows you to effectively identify information leaks in cryptographic algorithms.
[60]	It is focused on accelerating cryptographic operations in cloud environments, which is important for high-performance computing and Big Data	It is focused on creating a scalable NTT architecture to accelerate the CRYSTALS-Kyber	Numerical-theoretical transformation (NTT), High-level Synthesis (HLS)	The scalable NTT architecture can significantly speed up the work of post-quantum cryptographic algorithms.

№	Target application area:	Approaches to the implementation of security	Used specific cryptographic algorithms and methods	Results
[61]	Ensures the integrity and confidentiality of data in corporate cloud storage, which is important for business applications and data management	It offers a multi-layered hybrid security algorithm that ensures data integrity.	AES (Advanced Encryption Standard), Information Dispersion Algorithm (IDA), Hashing	The multi-layered hybrid security algorithm has shown high efficiency in ensuring data integrity and confidentiality in cloud computing environments.
[62]	Considers the use of homomorphic encryption and secure multithreaded computing to ensure data privacy, which is important for financial applications and personal data protection	Considers the use of homomorphic encryption and Secure Multiparty Computation	Homomorphic encryption (HE), Secure Multiparty Computation (SMC)	The developed prototype using homomorphic encryption and secure multiparty computation shows significant potential in ensuring quantum-resistant security measures.
[63]	It is aimed at long-term data security in cloud storage, which is important for data archiving and mission-critical systems	Offers the use of the Camellia block cipher for long-term data security in cloud environments.	Camellia Block Cipher, Quantum-stable data storage architecture	The PQC candidate Camellia block cipher has proven highly effective in ensuring long-term data security in cloud environments.

4.4 Performance comparison of methods and algorithms

To create a comparative performance table of the algorithms presented in the six articles, it is necessary to identify key performance indicators for each of the proposed cryptographic methods. These indicators may include the time required to perform encryption and decryption operations, resource usage (memory, processor time), and efficiency at various data block sizes.

Table 10 provides a detailed comparison of the performance of various cryptographic algorithms as reported in different research papers. The table categorizes the algorithms by their encryption and decryption times, highlighting the specific conditions and platforms on which these performances were measured. This table serves as a valuable resource for understanding the comparative performance of these algorithms under various conditions and applications.

Notes to the table:

- RSA: As reported in Paper 1, RSA shows an encryption time of 12 ms and a decryption time of 15 ms. The algorithm is noted for its combination with AES to enhance security.
- CRYSTALS-Kyber: According to Papers 2 and 3, CRYSTALS-Kyber has an encryption time of 14 ms (measured in NTT loops). Paper 2 mentions testing on FPGA and STM32F4, using TVLA for information leak assessment. Paper 3 highlights an 11-fold performance improvement using NTT acceleration.
- NTT: Also discussed in Paper 3, NTT is used with Cooley-Tukey (CT) and Gentleman-Sande (GS) operations, showing an encryption time of 14 ms.
- AES: Paper 4 reports AES performance with encryption and decryption times of 1.5 ms and 1.2 ms respectively, tested on Amazon EC2 and S3 with key lengths of 128, 192, and 256 bits.
- AES-128: In Paper 5, AES-128 achieves a data rate of 0.678 Gbits/s for both encryption and decryption, used in a prototype with homomorphic encryption and secure multiparty computing (MPC).
- Homomorphic HE: Also from Paper 5, the performance of homomorphic encryption algorithms (BGV, GSW) depends on the specific operation being performed, with testing conducted using the EMP library.
- Camellia: As per Paper 6, Camellia demonstrates encryption and decryption times of 117 ms and 98 ms respectively for 128-bit keys. It is noted for its higher security compared to AES due to an increased number of rounds.

Table 10: Performance of Algorithms from Articles

Algorithm	**Research paper**	**Encryption time (ms)**	**Decryption time (ms)**	**Remark**
RSA	Paper 1	12	15	Combination with AES for increased security
CRYSTALS-Kyber	Paper 2	14 (NTT loops)	N/A	Testing on FPGA and STM32F4, using TVLA to assess information leaks
CRYSTALS-Kyber	Paper 3	14 (NTT loops)	N/A	Acceleration using NTT, an 11-fold improvement in performance is achieved
NTT	Paper 3	14 (NTT loops)	N/A	Using Cooley-Tukey (CT) and Gentleman-Sande (GS) operations
AES	Paper 4	1.5	1.2	Testing on Amazon EC2 and S3, keys 128/192/256 bits long
AES-128	Paper 5	0.678 (Gbits/s)	0.678 (Gbits/s)	Use in a prototype with homomorphic encryption and secure multiparty computing (MPC)
Homomorphic HE	Paper 5	Depends on the operation	Depends on the operation	Homomorphic encryption (BGV, GSW), testing using the EMP library
Camellia	Paper 6	117 (128 bits)	98 (128 bits)	Performance compared to AES, higher security due to increased number of rounds

The comparative performance table demonstrates various aspects and results of the application of cryptographic algorithms in the context of post-quantum data security in cloud computing environments. Key metrics include the execution time of encryption and decryption operations, as well as specific characteristics such as resource usage and bandwidth. This allows you to get a complete picture of the advantages and disadvantages of each approach in real-world applications.

The six articles reviewed provide a comprehensive analysis of various approaches to data security in cloud computing environments, especially in the context of quantum threats. The main focus is on post-quantum cryptography (PQC), which is necessary to protect data from quantum attacks. Each article offers unique solutions and methods adapted to specific scenarios and requirements. The main conclusions are as follows:

1. *Needing of Post-Quantum Cryptography:* all articles emphasize the importance of using PQC to ensure long-term data security, as traditional cryptographic schemes are vulnerable to quantum computers. Post-quantum cryptography protects the confidentiality and integrity of data even when using quantum attacks.
2. *A variety of methods and algorithms:* various cryptographic algorithms and methods are used, such as lightweight schemes, hybrid encryption, NTT, homomorphic encryption, secure multiparty computing (MPC) and block ciphers such as Camellia. Each article offers its own unique approach to solving the problem of data security in the context of quantum threats.
3. *Efficiency and productivity:* the proposed methods and algorithms show high efficiency and performance in various testing scenarios. Some solutions, such as NTT and the Camellia block cipher, demonstrate significant acceleration and performance improvements compared to traditional methods.
4. *Practical application and testing:* all articles include test results and experimental data confirming the viability and practical applicability of the proposed methods. Testing was carried out on various platforms, including cloud services (Amazon EC2 and S3), FPGAs, microcontrollers and standard systems.
5. *Long-term data security:* ensuring long-term data security is a key aspect of all proposed solutions. The use of block ciphers such as Camellia and other PQC algorithms guarantees data protection for decades.

The authors in their papers presented several recommendations and further researches. According to the authors, it is necessary to continue research and optimization of the proposed methods to increase their stability and productivity. Improving the functions of rounds and implementing other candidate PQCS can improve the safety and effectiveness of the proposed solutions. It is important to conduct a comparative analysis of various methods and algorithms to assess their costs and performance in real-world scenarios. Additional testing and comparison with other methods, such as homomorphic encryption and MPC, will help determine the most appropriate solutions for specific tasks. It is recommended to integrate the proposed methods into real cloud services and systems to ensure their practical applicability and effectiveness. Applications include sensor networks, IoT devices, cloud storage, and other mission-critical systems.

In summary, all papers reviewed make a significant contribution to the field of post-quantum cryptography and data security in cloud computing environments. The proposed methods and algorithms demonstrate high efficiency and reliability, ensuring data protection from quantum attacks. Further research and optimization of these methods will help ensure their stability and performance in real-world applications, which is critical for long-term data security in the context of rapidly developing quantum computing technologies.

Conclusion

The landscape of cloud computing has undergone significant transformation since its inception, evolving from early mainframe computing in the 1950s to the advanced, scalable platforms utilized today. This evolution was fueled by the vision of pioneers like John McCarthy, who in the 1960s foresaw a future where computational resources could be delivered as utilities, much like electricity or water. This foresight laid the groundwork for what we now recognize as cloud computing, a technology that integrates IT resources from various hardware platforms and offers users access through the Internet.

Despite its numerous advantages, cloud computing faces substantial security challenges, particularly with regard to data confidentiality, integrity, and availability. Traditional cryptographic methods such as RSA and ECC, which form the backbone of current cloud security protocols, are increasingly at risk due to the advent of quantum computing. Quantum computers, by leveraging principles of quantum mechanics like superposition and entanglement, have the potential to perform computations at speeds exponentially greater than classical computers. This computational prowess was starkly illustrated by the development of Shor's algorithm and Grover's algorithm, which demonstrated the ability of quantum computers to solve problems that are infeasible for classical machines. These developments pose a direct threat to existing cryptographic systems, which rely on the computational difficulty of certain mathematical problems for their security.

In response to the looming quantum threat, the field of post-quantum cryptography has emerged, focusing on developing cryptographic algorithms that can withstand quantum attacks. Various approaches within post-quantum cryptography show promise. Lattice-based cryptography, for instance, uses the complexity of lattice problems to offer strong resistance to quantum attacks, with algorithms like Kyber and NTRU leading the way. Hash-based cryptography, relying on the difficulty of reversing hash functions, provides robust digital signature solutions through schemes such as XMSS and SPHINCS+. Code-based cryptography, exemplified by the McEliece cryptosystem, leverages the complexity of decoding linear codes, ensuring high security against quantum threats. Multivariate polynomial cryptography, although promising, faces practical challenges due to the large key sizes required. Finally, isogeny-based cryptography uses the properties of isogenies between elliptic curves to offer secure key exchange protocols, such as SIDH, which hold significant potential in the quantum era.

The integration of post-quantum cryptographic algorithms into cloud computing platforms is essential to secure these environments against future quantum threats. This process involves developing and standardizing new cryptographic methods while ensuring their efficient implementation in practical cloud settings. The National Institute of Standards and Technology plays a crucial role in this effort, conducting a rigorous competition to identify and standardize the most promising post-quantum cryptographic algorithms. As cloud service providers begin to integrate these algorithms into their platforms, it is vital to conduct performance evaluations and real-world testing to ensure that the new methods do not introduce significant overhead or degrade service performance.

Looking forward, continued research and development are necessary to refine and optimize post-quantum cryptographic algorithms, ensuring they are secure and efficient. Standardization efforts must continue to facilitate the widespread adoption of these new cryptographic methods. Additionally, raising awareness about the quantum threat and the importance of post-quantum cryptography among stakeholders—including businesses, governments, and the general public—is critical. Educational initiatives should be launched to equip current and future IT professionals with the knowledge and skills needed to implement and manage post-quantum cryptographic systems.

In conclusion, the future of cloud computing depends on our ability to secure it against the emerging threat of quantum computing. Embracing post-quantum cryp-

tographic methods is crucial for safeguarding sensitive data and maintaining the trust and reliability of cloud services. This thesis underscores the importance of proactive measures in anticipation of quantum advancements, calling for a collaborative effort among researchers, industry professionals, and policymakers to ensure a secure digital future. The journey towards quantum-safe cloud computing is both challenging and promising, requiring innovation, dedication, and foresight. As we advance into this new era, the integration of post-quantum cryptography will play a pivotal role in protecting the integrity and security of our digital infrastructure.

References

[1] Lennart Baumgärtner, Benjamin Klein, Niko Mohr, Anika Pflanzer, Henning Soller, representing views from McKinsey Digital "When and how—to prepare for post-quantum cryptography", May 2022. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/when-and-how-to-prepare-for-post-quantum-cryptography#/

[2] Castryck W. and Decru T. An Ecient Key Recovery Attack on SIDH (preliminary version) Cryptology ePrint Archive. Paper 2022/975. https://eprint.iacr.org/2022/975

[3] Chen L., Jordan S., Liu Y.K., Moody D., Peralta R., Perlner R., Smith-tone D. "Report on Post-Quantum Cryptography", NISTIR 8105, National Institute of Standards and Technology, Gaithersburg, Maryland, April 2016. https://doi.org/10.6028/NIST.IR.8105.

[4] Alagic J., Alperin-Sheriff J., Apon D., Cooper D., Dang Q., Yi-Kai Liu., Miller C., Moody D., Peralta R., Perlner R., Robinson A., Smith-Tone D., "Status Report on the First Round of the NIST Post-Quantum Cryptography Standardization Process", NISTIR 8240, National Institute of Standards and Technology, Gaithersburg, Maryland, January 2019, 27 pp. http://dx.doi.org/10.6028/NIST.IR.8240.

[5] NIST Special Publication 800-145. A NIST Definition of Cloud Computing. SP 800-145. Sept. 2011. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf

[6] Ward Beullens, Jan-Pieter D'Anvers, Andreas Hülsing, Tanja Lange, Lorenz Panny, Cyprien de Saint Guilhem, Nigel P. Smart., "Post-Quantum Cryptography: Current state and quantum mitigation", European Union Agency for Cybersecurity (ENISA), May 2021. https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation.

[7] Miklós Ajtai. "The shortest vector problem in L2 is NP-hard for randomized reductions (extended abstract).", In 30th Annual ACM Symposium on Theory of Computing, pages 10–19. ACM Press, May 1998. https://eccc.weizmann.ac.il/eccc-reports/1997/TR97-047/index.html

[8] Daniel J. Bernstein, Johannes Buchmann, Erik Dahmen, "Post-quantum cryptography", Chicago, Darmstadt,December, 2008. https://www.researchgate.net/publication/226115302_Code-Based_Cryptography.

[9] Giuseppe Murolo, "QUANTUM COMPUTING AND POST-QUANTUM CRYPTOGRAPHY", 2021, Università di Bologna. https://amslaurea.unibo.it/25600/1/tesi%20murolo%20ultima.pdf

[10] Julian Berberich, Daniel Fink "Quantum computing through the lens of control: A tutorial introduction", Stuttgart, Germany, October, 2023. https://arxiv.org/abs/2310.12571,

[11] SujayKumar Reddy M, Chandra Mohan B, "Comprehensive Analysis of BB84, A Quantum Key Distribution Protocol", School of Computer Science and Engineering Vellore Institute of Technology, Vellore, India, December, 2023. https://arxiv.org/abs/2312.05609

[12] Frank Wilczek, "Entanglement Made Simple", Quanta Magazine, April, 2016. https://www.quantamagazine.org/entanglement-made-simple-20160428/

[13] "Seminar 8. Quantum algorithms", Voronezh State University, Voronezh, Russia. http://www.rec.vsu.ru/rus/ecourse/quantcomp/sem8.pdf

[14] James Dargan, "Quantum Journey From The Search Engine To Google Sycamore", THE QUANTUM INSIDER, July, 2022. https://thequantuminsider.com/2022/07/14/google-sycamore/

[15] Borisova V. V., Degtyarev D. V., "IMPLEMENTATION OF THE SHORE QUANTUM FACTORIZATION ALGORITHM", "Vestnik" of the AmSU, Issue 103, 2023, Vladivostok, Russia. https://cyberleninka.ru/article/n/realizatsiya-algoritma-kvantovoy-faktorizatsii-shora

[16] Standaert, François-Xavier, "Introduction to Side-Channel Attacks", UCL Crypto Group, Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium, December, 2010. https://www.researchgate.net/publication/225852558_Introduction_to_Side-Channel_Attacks

[17] "Welch's t-test: Breaking Barriers: Welch's t-test for nervous abnormalities", FasterCapital , March 2024 . https://fastercapital.com/ru/content/T--μ-Welch's-Test--Breaking-Barrieres--T--μ---μ-μ.html

[18] Philippe Coussy,, Daniel D. Gajski, Michael Meredith, Andres Takach, "An Introduction to High-Level Synthesis", IEEE Design & Test of Computers , August, 2009. https://ieeexplore.ieee.org/document/5209958

[19] S.A. Dupli, I.I. Shapovalov, "Topological methods in quantum computing", Bulletin of the Kharkov University, Kharkov, Ukraine, September, 2007 . http://nuclear.univer.kharkov.ua/lib/781_3(35)_07_p03-30.pdf

[20] "Classic McEliece algorithm", Dedicated to the memory of Robert J. McEliece, 1942–2019. https://classic.mceliece.org/index.html

[21] Danial Imam, Amber Riaz, "What is Cloud Computing?", April, 2023. https://cloud.google.com/learn/what-is-cloud-computing

[22] "HHL Algorithm for Linear Systems of Equations", Introduction to Quantum Information - PHY 612, May, 2014. https://physlab.org/wp-content/uploads/2023/05/HHL_22120009_Fin.pdf

[23] Sudeshna Chakraborty, Mark Heller, Alex Phipps, "Euclid's Algorithm" Department of Mathematics, Cleveland State University. https://www.csuohio.edu/sites/default/files/85-%202015.pdf

[24] Komarova A.V., Korobeinikov A.G., "Analysis of the main existing post-quantum approaches and electronic signature schemes", Russia, St.Petersburg, Russia, October 2019. https://clck.ru/39hREQ.

[25] Emirova Z.M., "Cloud Coumputing", Kazakhstan, Almaty, 2012. https://cyberleninka.ru/article/n/oblachnye-vychisleniya-1/viewer

[26] Omarov S., Kurmanova Z.K. "Modern cloud technologies", Kazakhstan, 2021. https://kazatu.edu.kz/webroot/js/kcfinder/upload/files//-17/%20.pdf

[27] Shemyakina M.A. "A quantum simulation algorithm Grover's algorithm", Russia, Shakhty, 2019 https://alley-science.ru/domains_data/files/05January2019/ALGORITM%20MODELIROVANIYa%20KVANTOVOGO%20ALGORITMA%20GROVERA.pdf

[28] Fedorov A., E.Kiktenko, Postnauka Journal, "Quantum algorithms", December, 2020 https://postnauka.org/longreads/156115

[29] Fedorov A., Hightech Journal, "Not just Shore and Grover: what quantum algorithms exist", May, 2023. https://hightech.fm/2023/05/23/quantum-algorithms

[30] D.A.Kronberg, Y.I.Ozhigov, A.Y. Chernyavsky, "Quantum Cryptography", Lomonosov Moscow State University, Faculty of Higher Education. http://sqi.cs.msu.ru/store/storage/ss8dw5n_quantum_cryptography.pdf

[31] Evgeniy A. Dolgochub, Alexey N. Polikanin, "Technologies of quantum cryptography", Novosibirsk, Russia, 2021. https://cyberleninka.ru/article/n/tehnologii-kvantovoy-kriptografii/viewer

[32] Max Rokatansky, "The Quantum Internet: the competition to create an indestructible online world", Nano News Net, July, 2021. https://acesse.dev/bF97g

[33] V. M. Solovyov, "Quantum computers and quantum algorithms. Part 2. Quantum algorithms", Saratov National Research State University named after N. G. Chernyshevsky, Saratov, 2016. https://l1nq.com/HSIdk

[34] techinsider.ru Journal, "Secret Cipher: What is the difference between classical, quantum and post-quantum cryptography", July, 2022. https://encr.pw/2tLZz

[35] Palash B.V., "AES ENCRYPTION", Department of computing software and automated systems Katanov Khakass State University, FORUM OF YOUNG SCIENTISTS 2(42), 2020. https://cyberleninka.ru/article/n/aes-shifrovanie

[36] G.V. Basalova, E-books: "Fundamentals of Cryptography: a course of lectures", Moscow : INTUIT, 2016. - 201 p. - Text : electronic. https://intuit.ru/studies/courses/691/547/lecture/12377

[37] Abhishek Sharma, "What is Cloud Computing — How Cloud Computing Works?", September, 2021. https://medium.com/ezdatamunch/what-is-cloud-computing-how-cloud-computing-works-5c88295ebfaa

[38] Prajakta Patil, Chiradeep BasuMallick, "What Is Cloud Computing? Definition, Benefits, Types, and Trends", February, 2022. https://www.spiceworks.com/tech/cloud/articles/what-is-cloud-computing/

[39] Kev Zettler, "What is cloud computing?" Cloud Overview A Guide to Cloud Computing and its benefits for modern enterprises. https://www.atlassian.com/ru/microservices/cloud-computing

[40] Mikljaev E.M. Mkrtychev S.V. Russia, Togliatti, January 2022. https://7universum.com/ru/tech/archive/item/13002

[41] Sommer Figone, "10 Industries That Can Benefit from the Cloud". https://rapidscale.net/resources/blog/desktop-as-a-service/10-industries-can-benefit-cloud

[42] Servercore Blog, "What is Cloud Computing? Types of Cloud-based Technologies and Services", March, 2024. https://l1nq.com/hxqbX

[43] "Understanding Cloud Computing Models – IaaS, SaaS and PaaS", dinCloud, An ATSG Company. https://www.dincloud.com/blog/understanding-cloud-computing-models

[44] John Preskill, "Quantum computing 40 years later", Institute for Quantum Information and Matter California Institute of Technology, Pasadena CA 91125, USA AWS Center for Quantum Computing, Pasadena CA 91125, USA, June, 2021 https://arxiv.org/pdf/2106.10522

[45] Emily Grumbling, Mark Horowitz "Quantum Computing: Progress and Prospects", National Academies of Sciences, Engineering, and Medicine, Washington, DC: The National Academies Press, 2019. https://nap.nationalacademies.org/read/25196/chapter/7#120

[46] Isaac L. Chuang, Neil Gershenfeld, and Mark Kubinec, "Experimental Implementation of Fast Quantum Searching", MIT Media Lab, November, 1997. https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.80.3408

[47] IBM, IBM Quantum Summit 2022, "IBM Unveils 400 Qubit-Plus Quantum Processor and Next-Generation IBM Quantum System Two", New York, November, 2022. https://acesse.dev/SYgHZ

[48] Intel Corporation, "Intel's New Chip to Advance Silicon Spin Qubit Research for Quantum Computing", June, 2023. https://www.intel.com/content/www/us/en/newsroom/news/quantum-computing-chip-to-advance-research.html#gs.8ztifz

[49] Xanadu, "Beating classical computers with Borealis", June, 2022. https://www.xanadu.ai/blog/beating-classical-computers-with-Borealis

[50] Bennett C.H., Brassard G., "Quantum Cryptography: Public Key Distribution and Coin Tossing" Proc.of IEEE Int. Conf. on Comput. Sys. and Sign. Proces., Bangalore, India, 1984. https://arxiv.org/abs/2003.06557

[51] Acin A., Gisin N., and Scarani V. "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks" Phys. Rev., 2004, 012309. https://www.researchgate.net/publication/2189702_Coherent_pulse_implementations_of_quantum_cryptography_protocols_resistant_to_photon_number_splitting_attacks

[52] Sevag Gharibian, "Deutsch's Algorithm", Virginia Commonwealth University, 2015, https://www.people.vcu.edu/~sgharibian/courses/CMSC491/notes/Lecture%206%20-%20Deutsch's%20algorithm.pdf

[53] Austin Hartshorn, Humberto Leon, Noel Qiao, Scott Weber, "Number Theoretic Transform (NTT) FPGA Accelerator", Worcester Polytechnic Institute, Worcester MA 01609, USA. https://digital.wpi.edu/downloads/p2676z164

[54] P.W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring", Worcester Polytechnic Institute, Worcester MA 01609, USA, November, 1994. https://ieeexplore.ieee.org/document/365700

[55] Malik Imran, Zain Ul Abideen, Samuel Pagliarini, "A Systematic Study of Lattice-based NIST PQC Algorithms: from Reference Implementations to Hardware Accelerators", Centre for Hardware Security (CHS), Tallinn University of Technology (TalTech), Estonia, September, 2020. https://arxiv.org/pdf/2009.07091

[56] Aviad Kipnis, Jacques Patarin, Louis Goubin, "Unbalanced Oil and Vinegar Signature Schemes", In: Stern, J. (eds) Advances in Cryptology — EUROCRYPT '99. EUROCRYPT 1999. Lecture Notes in Computer Science, vol 1592. Springer, Berlin, Heidelberg. https://link.springer.com/chapter/10.1007/3-540-48910-X_15

[57] Erdem Alkim, Joppe W. Bos, Leo Ducas, Patrick Longa, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Chris Peikert, Ananth Raghunathan, Douglas Stebila, "FrodoKEM Learning With Errors Key Encapsulation", June, 2021. https://frodokem.org/files/FrodoKEM-specification-20210604.pdf

[58] Shaik Mohammed Ilias, V.Ceronmani Sharmila, "Recent Developments and Methods of Cloud Data Security in Post-Quantum Perspective", Hindustan Institute of Technology and Science Chennai,Coimbatore, India, March, 2021. https://ieeexplore.ieee.org/document/9395901

[59] Tristen Teague, Mayeesha Mahzabin, Alexander Nelson, David Andrews, Miaoqing Huang, "Towards Cloud-based Infrastructure for Post-Quantum Cryptography Side-channel Attack Analysis", Miami, FL, USA, September 2023. https://ieeexplore.ieee.org/document/10412485

[60] Mojtaba Bisheh-Niasar, Daniel Lo, Anjana Parthasarathy, Blake Pelton, Bharat Pillilli, Bryan Kelly, "PQC Cloudization: Rapid Prototyping of Scalable NTT /INTT Architecture to Accelerate Kyber", Huntsville, AL, USA, October, 2023. https://ieeexplore.ieee.org/document/10318029

[61] Nagababu Garigipati, S. Srithar, V.Krishna Reddy, "A Multi-Layered Hybrid Security Algorithm Based on Integrity for the Cloud Computing Environment", Namakkal, India, July, 2023. https://ieeexplore.ieee.org/document/10212405

[62] Linus Töbke, Olaf Grote, Andreas Ahrens, "A Practical Approach to Quantum Resilient Cloud Usage Obtaining Data Privacy", Wismar, Germany, May, 2023. https://ieeexplore.ieee.org/document/10124397

[63] Olaf Grote, Andreas Ahrens, César Benavente-Peces, "Small Quantum-safe Design Approach for Long-term Safety in Cloud Environments", Istanbul, Turkey, October, 2021. https://ieeexplore.ieee.org/document/9659632