Grant Thornton

MINISTERSTVO PRŮMYSLU A OBCHODU

Financováno Evropskou unií NextGenerationEU

Quantum Technologies and Communications

Prepared for the Ministry of Industry and Trade

[June 2025]

Grant Thornton

Contents

List of abbreviations and explanations

Abbreviation	Explanation
3GPP	The 3rd Generation Partnership Project
4G/5G	Fourth/fifth generation mobile networks
AES	Advanced Encryption Standard
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
AMF	Access and Mobility Management Function
APDs	Avalanche photodiode
AQT	Alpine Quantum Technologies
ATIS	Standardisation organisation, Alliance for Telecommunications Industry Solutions
Czech Academy of Sciences	Czech Academy of Sciences
BSC-CNS	Spanish Supercomputing Centre, Barcelona Supercomputing Centre-National Centre for Supercomputación
CMOS	Complementary Metal-Oxide-Semiconductor
CRQC	A quantum computer capable of breaking current ciphers, short for Cryptographically Relevant Quantum Computer
CSP	Communications Service Providers
CZQCI	Project to deliver the EuroQCI physical infrastructure backbone network in the Czech Republic, Czech National Quantum Communication Infrastructure
Czech Republic	Czech Republic
CTU	Czech Technical University
DoS	A type of attack on internet services, known as Denial-of-service
DSA	Digital Signature Algorithm
DTLS	A protocol providing security for stateless datagram protocols, from the English 'Datagram Transport Layer Security
EAP	An authentication framework most commonly used in wireless networks and point-to-point systems Extensible Authentication Protocol
ECC	A cryptographic algorithm based on elliptic curve cryptography, in English Elliptic Curve Cryptography
ECDH	The Diffie–Hellman protocol using elliptic curves
ECDSA	Asymmetric cryptography algorithm for digital signatures, known as the Elliptic Curve Digital Signature Algorithm
ECIES	A hybrid encryption scheme based on elliptic curves, known as the Elliptic Curve Integrated Encryption Scheme

EPS	A packet system used in LTE networks, known as the Evolved Packet System
ETSI	European Telecommunications Standards Institute Institute
EU	European Union
EUR	Euro
EuroQCI	European Quantum Communication Infrastructure Initiative, Quantum communication infrastructure

FT	Fault-tolerant system
gNB	Base stations, gNodeB
GPU	Graphics Processing Unit
GSMA	The Global System for Mobile Communications Association
HHL	Quantum algorithm, Harrow-Hassidim-Lloyd algorithm
HNDL	Type of quantum attack, Harvest Now Decrypt Later
HPC	High-performance computing
HQC	Hybrid code encryption, from Hamming Quasi-Cyclic
HW	Hardware
IMSI catcher	Equipment for eavesdropping on telephone conversations
IoT	Internet of Things
IPsec	An encryption algorithm that protects data transmission between devices by encrypting individual IP packets and simultaneously verifying the source of that data
ISG	Industry Specification Group within the ETSI organisation Group
IT	Information Technology
ITU-T	International Telecommunication Union Telecommunication Standardization Sector International Telecommunication Union, Standardisation Sector
KEM	Key encapsulation mechanism
LAN	Local Area Network
LIGO	Gravitational sensor, Laser Interferometer Gravitational-Wave Observatory
LRZ	German supercomputing centre, German Leibniz-Rechenzentrum
MAX-CUT	Maximum cut problem
mK	millikelvin, very low temperatures
MUNI	Masaryk University
NCSC	UK National Cyber Security Centre
NFV	Network function virtualisation
NISQ	Current generation of quantum computers
NIST	The US National Institute of Standards and Technology Technology
NSA	US cryptographic organisation, The National Security Agency
PKI	Public Key Infrastructure
PQC	Post-quantum cryptography
QAOA	A quantum algorithm designed to solve combinatorial optimisation problems Approximate Optimization Algorithm
QC	Quantum computing
Qiskit SDK	Open-source software development kit for quantum computers
QKD	Quantum Key Distribution
QMITM	A type of quantum attack
QRNG	Quasirandom Number Generator
QSC	Quantum-safe cryptography
RSA	A public-key cryptosystem based on factorisation, Rivest-Shamir-Adleman
SDN	Software-Defined Networking
SIDH	Post-quantum cryptographic algorithm, Singular Isogeny Diffie-Hellman
SNSPDs	Superconducting nanowire single-photon detector

SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	A protocol utilising public-key encryption, information authentication and the detection of unauthorised data manipulation, Transport Layer Security
UE	User equipment
UK	Charles University
UPF	A network component in the 5G core that handles the routing, transmission and processing of user data separately from the control plane, User Plane Function
USD	US dollar
USTC	University of Science and Technology of China
VQE	A hybrid algorithm that utilises both classical and quantum computers to determine the state of a given physical system, known as the Variational Quantum Eigensolver
VŠB	Ostrava University of Mining and Technology
VTT	Finnish Technical Research Centre, in Finnish Valtion teknillinen tutkimuskeskus
VUT	Brno University of Technology
Wi-Fi	A group of wireless networking protocols based on the IEEE 802.11 standards, known as Wireless Fidelity
ZUC	A streaming encryption algorithm used in mobile networks to secure data traffic

Executive summary

Quantum computing (QC) is one of the applications of quantum mechanics, a broad scientific discipline based on quantum theory. Quantum theory provides the fundamental framework for understanding the behaviour of matter and energy at the microscopic level and has enabled the emergence of a whole range of new technologies. Today's 'second quantum revolution' means that we are able not only to observe but also to manipulate individual particles in a targeted manner, leading to the development of three main areas of application: quantum sensing, quantum communication, and quantum computers.

Quantum mechanics deals with physical phenomena at the subatomic level, which are fundamentally different from the ordinary physical laws of the macroscopic world. These include, in particular, the superposition of states, quantum entanglement, the probabilistic nature of measurement, and the impossibility of copying quantum information. These principles, which are not possible in the classical world, can be utilised in quantum applications. Within computer science, they represent a new computational model with the potential to significantly accelerate the solution of certain types of problems (e.g. factorisation, optimisation, material simulations).

Quantum computers and their development are limited by the physical properties of quantum systems – error rates, decoherence and the technological demands of operation (e.g. cryogenic cooling). The basic building block of quantum systems is the qubit (the quantum equivalent of a classical bit), which can be realised using various physical systems (superconducting circuits, ion traps, photonic systems, etc.). The implementation of quantum error correction and scaling to hundreds or thousands of logical qubits is key to achieving practically usable quantum computers. The world's leading players (IBM, Google, Quantinuum, Chinese and European teams) are set to reach hundreds of qubits by 2025 and are gradually improving the quality and performance of their devices. However, these are currently a small number of very expensive devices (the aforementioned entities invest hundreds of millions of USD annually) and all are in a deeply experimental phase. There is a whole range of different QC technological approaches, which vary in their suitability for specific computational tasks. Further development, experimentation, comparison of the viability of the various methods, identification of effective approaches and subsequent standardisation are required.

The deployment of quantum computers will enable the solving of complex scientific problems and practical simulations (designing materials with specific properties, batteries, chemical compounds, medicines, in logistics, in neural network training – AI, cryptography) whilst simultaneously posing a security risk to current encryption methods. For the time being, it can be said in simple terms that the performance of quantum computers does not exceed that of standard (legacy) systems; however, they are capable of solving specific sub-tasks that are inaccessible to standard systems – unsolvable within a conceivable timeframe. This type of combined use of standard computing systems and QCs (for specific sub-tasks) is also anticipated in the future. At present, only limited commercial use of QCs is possible in the form of renting machine time and the services of a research (scientific) team, which translates the client's requirements into instructions comprehensible to quantum devices (unitary operations).

Specific tasks accessible to QC include encryption and decryption, which in the foreseeable future are capable of breaking current cryptographic protocols (particularly RSA and ECC) used in 5G networks for authentication and key exchange, thereby compromising the overall security of digital communications. Grover's algorithm also threatens symmetric ciphers, albeit to a lesser extent. It is essential to migrate to post-quantum cryptography in good time and, where appropriate, to utilise QKD for backbone and critical infrastructure. This step must be taken well in advance of the development of quantum computing itself, as threats already exist today that will manifest later – attackers are already collecting (eavesdropping on) and storing standard encrypted communications, intending to decrypt them later once they acquire the relevant quantum technology. The estimated time until current encryption algorithms are broken by a quantum computer is estimated at 15 to 20 years, with the level of risk roughly doubling every 5 years.

Post-quantum cryptography (PQC) addresses the risk posed by quantum computers to current encryption algorithms. It focuses on developing new algorithms resistant to attacks by quantum computers, without requiring new physical infrastructure. NIST and ETSI are testing and standardising these new algorithms. The advantage of PQC is the possibility of software implementation on existing systems; the disadvantages are larger (longer) keys, and consequently greater demands on device performance, as well as a shorter history of security verification to date.

Quantum communication, another application of quantum mechanics, utilises quantum phenomena (particularly entanglement and the impossibility of measuring a quantum state without affecting it) to securely generate and distribute encryption keys (QKD). This technology enables the detection of any eavesdropping attempt and is considered secure in the long term, even against attacks by quantum computers. The main limitations of QKD lie in its range (currently in the order of tens to hundreds of kilometres without repeaters), cost, and the need for specialised infrastructure. However, intensive research is underway into the integration of QKD into conventional telecommunications networks, and initial successes in testing technologies have already been recorded in the field of satellite QKD.

The development of QC remains a highly complex and costly process. Investments in QC research are therefore being made not only by the world's largest players but also by individual states, either alone or in collaboration. Development in the EU is characterised by massive investments in the advancement of quantum technologies within specific programmes/projects (Quantum Flagship, EuroHPC Joint Undertaking, EuroQCI), and the development of QC is also part of the objectives of the Digital Decade policy. In the Czech Republic, a national quantum testing infrastructure is being established (the CZQCI project), and educational and research activities are being developed across universities (MUNI / CS Hub) and the Czech Academy of Sciences. A national quantum strategy is being prepared and cooperation within the European framework is being developed.

Recommended steps for state institutions and regulators include the need to:

- formulate minimum (binding) methodological rules for operators to ensure the cybersecurity of 5G and other communication networks in connection with the advent of quantum computing,
- create a reference register of PQC-compatible devices, and
- set minimum requirements for interoperability between classical and QKD cryptography.

Management summary

Quantum computing (QC) is one of the applications of quantum mechanics, a broad scientific discipline rooted in quantum theory. Quantum theory provides the fundamental framework for understanding the behaviour of matter and energy at the microscopic level and has enabled the development of numerous new technologies. Today's "second quantum revolution" signifies that we can not only observe but also deliberately manipulate individual particles, leading to advancements in three main application areas: quantum sensing, quantum communication, and quantum computing itself.

Quantum mechanics deals with physical phenomena at the subatomic level, which differ fundamentally from the classical laws of the macroscopic world. Key principles include superposition of states, quantum entanglement, the probabilistic nature of measurement, and the impossibility of copying quantum information. These principles, which are absent in the classical world, enable transformative applications in computing. In computer science, they introduce a new computational model with the potential to dramatically accelerate solutions to specific problems, such as factorisation, optimisation, and material simulations.

Quantum computers and their development are constrained by the physical properties of quantum systems – error rates, decoherence, and operational demands (e.g., cryogenic cooling). The basic building block of quantum systems is the qubit (analogous to the classical bit), which can be implemented through various physical systems such as superconducting circuits, ion traps, or photonic systems. Achieving practical quantum computers requires implementing quantum error correction and scaling to hundreds or thousands of logical qubits. Leading global players (IBM, Google, Quantinuum, and Chinese and European teams) are projected to reach hundreds of qubits by 2025, gradually improving device quality and performance. However, these remain expensive, experimental systems, with annual investments reaching hundreds of millions of USD. Diverse technological approaches to quantum computing exist, each suited to specific computational tasks, necessitating further development, experimentation, viability comparisons, and eventual standardisation.

Deploying quantum computers will enable the solving of complex scientific problems and practical simulations (e.g., designing advanced materials, batteries, chemical compounds, drugs, logistics optimisation, AI training, and cryptography), whilst simultaneously posing security risks to current encryption methods. Whilst quantum computers do not currently outperform classical (legacy) systems in general tasks, they excel at specific subtasks that are intractable for classical systems. A hybrid approach – combining classical and quantum systems for specialised subroutines – is expected to persist. Currently, limited commercial use of quantum computers exists via machine-time rentals and scientific team services for translating client requirements into quantum-readable instructions (unitary operations).

Key tasks accessible to quantum computers include encryption and decryption, which could soon break current cryptographic protocols (e.g., RSA, ECC) used in 5G networks for authentication and key exchange, thereby compromising the security of digital communications. Grover's algorithm also poses a threat to symmetric ciphers, albeit to a lesser extent. A timely transition to post-quantum cryptography (PQC) and the adoption of quantum key distribution (QKD) for critical infrastructure are essential. This transition must precede advancements in quantum computing, as attackers are already harvesting (eavesdropping on and storing) encrypted data for future decryption once quantum technology becomes available. The estimated timeframe for quantum computers to break current encryption is 15–20 years, with risks doubling approximately every five years.

Post-quantum cryptography (PQC) addresses quantum computing threats by developing algorithms resistant to quantum attacks without requiring new physical infrastructure. NIST and ETSI are testing and standardising these algorithms. Whilst PQC allows for software implementation on existing systems, drawbacks include larger keys, higher performance demands, and a shorter history of security validation.

Quantum communication, another application of quantum mechanics, utilises phenomena such as entanglement and the no-cloning theorem to securely generate and distribute encryption keys (QKD). This technology detects eavesdropping attempts and remains secure against quantum attacks. Current limitations of QKD include range (tens to hundreds of kilometres without repeaters), cost, and the need for specialised infrastructure. However, research into integrating QKD into standard telecommunications networks and satellite-based QKD is progressing.

QC development remains complex and costly. Beyond major global players, individual states and collaborative initiatives are investing heavily. In the EU, significant funding supports quantum technology through programmes and projects such as Quantum Flagship, the EuroHPC Joint Undertaking, and EuroQCI, in line with the Digital Decade policy goals. In the Czech Republic, a national quantum test infrastructure (the CZQCI project) is emerging, alongside educational and research activities at universities (e.g., MUNI/CS Hub) and the Academy of Sciences. A national quantum strategy is being prepared, alongside European collaboration efforts.

The recommended steps for state institutions and regulators include the need to:

- Formulate mandatory minimum methodological rules for operators to ensure the cybersecurity of 5G and other communication networks in the context of quantum computing advancements,
- Create a reference register of PQC-compatible devices, and
- Establish minimum interoperability requirements between classical and QKD cryptography.

1 Fundamentals of Quantum Technologies

1.1 Introduction

Quantum theory is a general theoretical framework, a physical theory that describes the behaviour of matter and energy at the atomic and subatomic levels and encompasses fields such as quantum mechanics, quantum electrodynamics, quantum fields and quantum statistics. **Quantum mechanics**, the cornerstone of all quantum physics and quantum theory in general, is a scientific discipline providing a mathematical framework and precise laws for describing and predicting the behaviour of subatomic particles (e.g. electrons, photons, quarks). In this microcosm, the laws of nature differ fundamentally from those of classical physics, giving way to probabilistic phenomena, the wave-particle duality, and the phenomenon of instantaneous correlation between particles regardless of their distance.

Years of research in the field of quantum technologies, which has resulted in the development of applications such as lasers, magnetic resonance, atomic clocks, electron microscopy, etc., has reached a stage where we are able to manipulate individual subatomic particles with great precision. This pace of progress has helped to significantly increase the volume of funding flowing into research and development of quantum technologies, which over the last decade has led to the development of further, entirely new applications. Today, these can be divided into three main areas:

- Quantum sensing
- Quantum computers and algorithms
- Quantum communication

1.2 Basic concepts of quantum theory

Quantum theory (more precisely, quantum mechanics) is a comprehensive physical theory that is highly counterintuitive. It is based on a few observed fundamental rules, from which all the consequences leading to applications follow. Therefore, quantum theory can be viewed from two perspectives – the first is a physical-philosophical perspective, in which the theoretical (mathematical) foundations of the theory are explored; the second perspective is practical, the pure application of principles leading to applications. The second approach is appropriate for this study – it does not serve to understand the theory itself, but is rather a guide whereby we accept certain basic rules (postulates) and examine their consequences. Explanations of phenomena, insofar as they lie within the mathematical foundations of the theory, are not the subject of this study due to their complexity.

Of the postulates of quantum theory, the following principles are particularly important for the subsequent description:

1. Every quantum system is in some **probabilistic state**, mathematically expressed by **a** so-called **wave function** or **state vector** (denoted by $|a\rangle$, $|b\rangle$, etc., representing a vector in Hilbert (mathematical) space), which can in principle be described, but it is not possible to obtain this information from an unknown state. A quantum state can be decomposed into basis states (according to measured quantities; for an electron, for example, position, energy, spin), and each basis state is assigned a so-called probability amplitude, which determines how much it contributes to the result (the overall state of the system).
2. Manipulation of the state takes place using special operations permitted by theory, which we call **unitary operations**. A unitary operation is reversible and ensures that ‘probability is not lost’ from the system – that is, that the sum of all possibilities remains 100%. If we imagine that a quantum state is like an arrow pointing in a certain direction within the space of possibilities (a vector), then a unitary operation is a special ‘movement’ or ‘rotation’ of this arrow, which changes something in the system but loses nothing. The arrow can rotate, change direction, but it will never shorten, lengthen or disappear. All possibilities remain preserved. If you perform a unitary operation and then ‘reverse’ it, you will end up exactly where you started. In quantum physics, it is important that probability is not lost as the system evolves, and unitary operations ensure this. The actual application of a unitary operation to a quantum system takes the form of a physical interaction with the particles in the system (e.g. using electromagnetic fields, microwaves, lasers or electrical signals, depending on the type of physical qubit).
3. The only way to obtain classical information from a quantum system is **by measuring** it. When measuring a quantum state, we determine the specific value of a selected physical quantity in the system, such as energy, spin, momentum, position, polarisation or other properties of the particles. In the quantum world, these quantities can only take on certain (discrete) values – they are quantised, and the measurement result is always just one of the possible quantised states, determined by probabilities based on the original

quantum state. However, as already mentioned, the measurement provides us with only partial information. At the same time, an irreversible change occurs in the system, whereby the remaining information about the quantum state is lost.

These principles lead to many well-known and lesser-known manifestations of quantum theory. Some of these are:

- **Superposition**

Principle 1 also has a specific rigorous mathematical description, which allows a system that can be in state $|a\rangle$ or in state $|b\rangle$ (0 or 1), may also be in the state $\alpha\,|a\rangle+\beta\,|b\rangle$, i.e. in a state that is composed of both possibilities. This rule is called superposition. An example of this is the well-known Schrödinger's cat, which is 'both alive and dead at the same time'. However, this description using the word 'at the same time' is, however, highly imprecise and leads to the widespread but inappropriate description of quantum computations as being parallelised. Superposition may at first glance appear to be parallelisation, but due to the implications of the remaining principles, this interpretation is highly inadequate.

- **Probabilistic (quantum) measurement**

It elaborates on and describes the third quantum principle in greater detail. A quantum measurement can only provide us with information about the system that is selected from a set of possible outcomes associated with the measurement. Each measurement is specified by the quantum states it is capable of distinguishing (e.g. $|a\rangle$, $|b\rangle$, $|c\rangle$, etc.), which are classically represented as a, b, or c. A system in the superposition $\alpha\,|a\rangle+\beta\,|b\rangle$ of states $|a\rangle$ and $|b\rangle$, yields results of a or b only with a certain probability, precisely defined by the parameters α and β. After the measurement, the entire system is reduced to the state $|a\rangle$ or $|b\rangle$ depending on the result (destructive nature of the measurement). To gain a more precise understanding of the parameters α and β, it is therefore necessary to repeat the entire experiment (the process from preparing the state to measuring it) several times. Even so, it is not possible to obtain complete information about these parameters.

- **Interference**

One of the consequences of Principle 1, which would not be possible under a 'parallel conception', is so-called interference, whereby some measurement results may be amplified when the system changes, whilst others are attenuated. This is a phenomenon in which the wave functions of quantum particles can 'interfere' with one another – much like waves on water – even in the case of a single particle in a superposition (where it exists in multiple states simultaneously). If multiple states exist, all possible probability amplitudes from each of them must be summed. These amplitudes can reinforce or cancel each other out – this is precisely what interference is. The result of this superposition can be an increase in the probability of a particle appearing in certain locations (constructive interference) and, conversely, a reduction or cancellation in others (destructive interference). Interference forms the basis for many algorithms, where, using precisely defined operations, we perform a calculation in which the results useful to us are amplified to the point where they emerge from the measurement with sufficiently high probability. The complexity of developing quantum algorithms lies in the combination of the restrictions imposed by Principle 2 on unitary operations and the destructive nature of measurement.

- **Entanglement**

With a larger number of system components, it is possible to achieve strong correlations between individual components. An entangled state can be recognised by the fact that a measurement on one particle immediately determines the state of the other. In quantum mechanics, the example of the spin of two electrons is often used. If the electrons are entangled, if you measure the spin (a quantum property) of one and find, for example, the value 'up', the other will always be 'down' – even if they are light-years apart. The measurement result is random, but always perfectly correlated. (Imagine you have two dice that are entangled. You roll one in Prague and the other, say, in New York. If you roll a six in Prague, a six will also appear in New York at that very moment – no matter how far apart the two dice are. The result of the roll is random, but as soon as you find out the result for one, you immediately know the result for the other.) Entanglement typically occurs during the joint creation of particles (for example, when a particle decays into two smaller ones), or artificially, if particles interact in such a way that they enter a shared quantum state. Quantum correlations, however, are stronger than classical (statistical) ones. The strength of quantum correlation is measurable and leads to applications that are not possible in a classical setting. A major application is, for example, in quantum communication, where one of the key-securing protocols is based on the creation of such entangled states. However, most particles in nature are not entangled – entanglement is therefore a rare and fragile state that is easily lost (known as decoherence).

- **Projective measurements and weak measurements**

The measurements described above are so-called projective measurements (also known as strong or von Neumann measurements), where the change in state following the measurement is absolute. This means that the measurement result is always just one of the possible eigenstates of the measured operator, and after the measurement the system collapses into this single state (no superposition – the probability of any other state is eliminated). A strong measurement severely disturbs (decoherences) the original quantum state. However, we also know of weak measurements, which do not necessarily degrade the system's state completely, but only partially. A weak measurement is one in which the interaction between the measured system and the measuring apparatus is very weak, with the result that we obtain only a small (inaccurate) amount of information about the system, but at the same time we hardly disturb the system at all. The information obtained in this way is therefore weaker than that from a projective measurement. Typically, this type of measurement is carried out by weakly entangling the measured system with an auxiliary system. A projective measurement on the auxiliary system then yields less

information about the measured system, which is less affected by the measurement. Weak measurements are important, for example, in quantum error correction (in quantum computers).

- **No-cloning**

The specificity of operations permitted by quantum theory (principle 2), in conjunction with the destructiveness of measurement, results in the impossibility of copying a quantum state. Any attempt to copy a quantum state leads to its destruction. This principle is known as the no-cloning theorem.

- **Decoherence**

Quantum states are extremely fragile; they interact easily with their surroundings, causing the state to lose the information stored within it. We can imagine this as the environment continuously performing weak measurements on the system, from which information is gradually lost in this way. This phenomenon is also known as quantum noise. Since any interaction with the environment leads to decoherence, when designing quantum devices we must ensure the best possible protection from the environment. Many systems are therefore housed in a vacuum and maintained at very low temperatures (mK).

1.3 Quantum Sensors

Quantum sensing brings improvements in measurement accuracy to various fields, sometimes by several orders of magnitude. The principles used for this purpose vary and differ from application to application. For example, entanglement can be used to further improve atomic clocks, or to create more sensitive magnetometers. Interference is utilised in photonic sensors, microscopy, or in gravitational wave detectors (LIGO). Another example is the creation of more sensitive radio wave receivers, which are also more energy-efficient[1] . This list is not exhaustive and merely highlights the diversity of the subject.

1.4 Quantum computers

1.4.1 What are (or will be) quantum computers for?

Quantum computers, which operate on quantum principles, introduce a new paradigm to the field of computing. This different approach to computation is expected to enable the acceleration of certain specific operations. This is one reason why considerable attention is being paid to their development. It is important to bear in mind that one cannot expect a universal acceleration of all calculations; applications can be found in very specific areas of mathematical operations. Finding quantum algorithms that may be useful is a complex process influenced by specific constraints of quantum theory – the destructive nature of measurement, and the specificity of system evolution (limitations to unitary operations). Of particular interest for quantum computing are areas where an exponentially large space is being searched (various optimisations), or which have some relevance to quantum physics (materials, batteries, chemistry, medicine, etc.). These can be divided into three groups:

1. Quantum systems themselves, which are very difficult to simulate classically, could be simulated on well-controlled quantum systems – simulating the quantum with the quantum. This group includes research areas such as the design of materials with specific properties, batteries, chemical compounds or medicines.

2. Quantum computers can also help solve non-quantum problems with an exponentially large number of possibilities, for which no classical efficient algorithms are available. These include various optimisations through, for example, quantum annealing (the concept of finding minima and maxima in a given environment and identifying optimal scenarios), e.g. in logistics, but also in training neural networks (however, despite years of research in this area, there are still no reliable algorithms available that have been proven to be more effective than classical approaches).

3. Quantum computers have a different hierarchy of computational complexity, which opens up new avenues in theoretical computer science, education and the exploration of the limits of computational capabilities. The third area thus brings together various specific quantum algorithms whose effectiveness has been theoretically proven (Shor's, Grover's, or HHL – see below). All these algorithms utilise specific properties of quantum theory to solve a specific problem and are therefore not a universal approach capable of generating classes of algorithms.

[1] https://ieeexplore.ieee.org/document/9492845

As there are as yet no standard working examples of quantum computer applications (all are still at the experimental stage), it is more a matter of speculation as to the fields in which quantum computers will not outperform classical ones, should their practical implementation succeed (e.g. noise cancellation, etc.)

Every quantum computer can simulate a classical computation. If a quantum and a classical computer had the same performance and capacity, they would be almost equally fast. As current quantum computers are considerably slower, this comparison is not entirely appropriate, but it does indicate that for computations that are efficient on classical computers, there is no need to use quantum computers.

It is estimated that in the future there will be specialised quantum devices similar to graphics processing units (GPUs), which will be available primarily as cloud-based solutions integrated into high-performance computing. We can anticipate a certain convergence of high-performance computing (HPC), high-performance data analytics (HPDA), artificial intelligence (AI), quantum computing (QC) and their applications across other scientific, industrial and societal fields. An increase in the importance of quantum algorithms is expected; these will not provide complete solutions to problems, but will rather be subroutines used to accelerate computations in hybrid tasks.

The beginnings of practical QC applications can be illustrated by the following examples:

- JPMorgan Chase, in collaboration with IBM Research, has explored the possibility of using quantum computing to estimate the price of options.
- Mitsubishi Chemical, in collaboration with Keio University, is investigating the potential use of quantum computers in simulating complex electrochemical reactions.
- Phasecraft offers a database of materials for which it can provide optimised algorithms for their simulation on quantum devices.

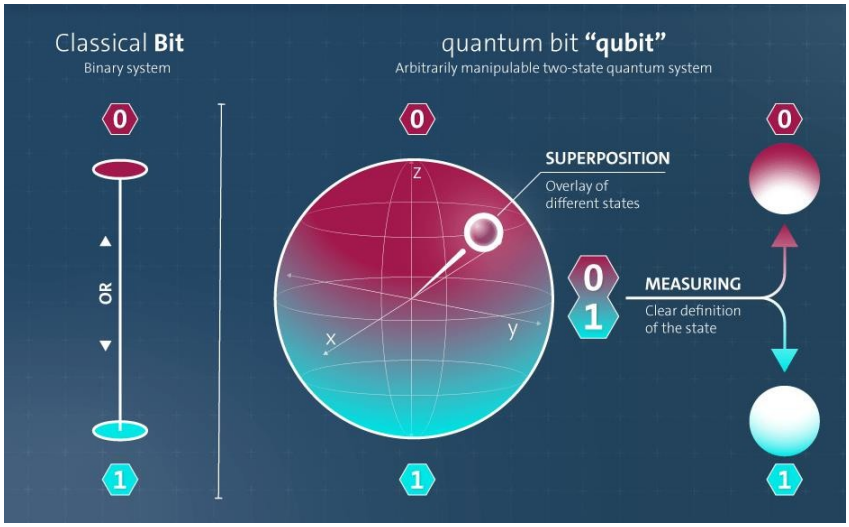
Quantum computers are also expected to play a role in the development of AI and vice versa (in order of development stage):

- The use of classical neural networks to optimise or solve various quantum problems
- The use of quantum computers to accelerate certain processes in machine learning
- Fully quantum neural network – storing information in qubits (the least developed area)

1.4.2 The principle of a quantum computer

The basic unit of information in classical computers is a single bit – it can have a value of 0 or 1. Bits are assembled into registers, on which we perform various operations that change the state of the register. The basic unit of information in quantum computers is the quantum bit, or qubit, which, unlike a bit, can also be in a superposition state $|0\rangle$ and $|1\rangle$. By combining multiple qubits into a register, we can construct a device analogous to classical computers. Quantum computation on such a device takes place using unitary operations. The computation is then concluded by measuring at least part of the quantum register, the aim of which is to convey information about its state
to the user. A quantum algorithm must be designed to ensure that the partial information about the register's state obtained during a quantum measurement has the highest possible informational value. However, this is a fundamental complication arising from the theory, which means that there are few quantum algorithms and they are only suitable for specific tasks.

Figure 1: Visualisation of a classical bit and a quantum bit (qubit)



From a technological perspective, one of the key factors is the error rate, or the inaccuracy of all operations involving quantum systems. It is relatively straightforward to have multiple qubits; however, as the number of qubits increases, it becomes difficult to maintain their error rate at levels achievable with a small number of qubits. The error rate increases particularly in two-qubit operations. Furthermore, current technologies are not physically capable of handling large numbers of qubits. Most functional quantum computers therefore have only a few dozen or a few hundred qubits.

From a practical perspective, another fundamental problem is decoherence. This gradually degrades the quantum information stored in the registers (qubits). Quantum computations on devices with higher levels of quantum noise are therefore time-limited and are currently far from being useful. However, efforts to reduce decoherence are in direct conflict with our requirement to be able to control the system (state preparation, computation and measurement). This is another reason why the development of quantum computers is technologically challenging. The requirements for quantum computers were formalised in 1996 by David P. DiVincenzo, an American theoretical physicist working in Germany:

- A scalable system with a well-defined qubit;
- The ability to initialise a qubit into a simple and well-defined state;
- Long coherence times;
- The ability to perform universal (arbitrary) computations;
- The ability to measure individual qubits.

When a device meets these requirements, we say that it is a quantum computer. Not all quantum computing devices meet all of these requirements. In particular, if point 4 is not met, the device is reduced to a system known as a quantum simulator, which can only perform specific calculations. An example is the system from D-Wave Systems.

Considerable effort is being devoted to meeting all five requirements, particularly the limitation of noise (decoherence). The current stage of development is known as the NISQ era (noisy intermediate-scale quantum), where we are limited not only by noise but also by the technological capabilities of manufacturing individual components and supporting techniques, which impose constraints on the size and quality of the devices.

Various approaches are used to suppress noise:

- Noise mitigation (reduction) and designing algorithms to function despite persistent noise – an effort to achieve so-called quantum utility, where the main goal is the algorithm's usefulness rather than its scalability (the ability to apply it to larger tasks).
- Hardware approaches, such as cat qubits (Alice & Bob) and topological qubits (Microsoft). With these approaches, manufacturers attempt to 'encode' quantum information into the part of the (more complex) quantum system that is less affected by the environment. The environment thus mainly interacts with the part of the state that does not contain computational quantum information, and therefore does not degrade it.
- Quantum error correction leading to fault-tolerant (FT) computations (described in the following separate chapter).

1.4.3 Quantum error correction

In classical computers, there is also a gradual degradation of information; however, this can be slowed down by means of error correction to such an extent that classical computers perform calculations practically without errors. The basic principle of error correction is the replication of bits which, using specific coding, store the information in question, and in the event of an error, it is possible to correct it by obtaining information from another part of the system. Conventional error correction thus relies on the possibility of replicating information (copying), which is inadmissible in quantum theory, as measurement in quantum theory irreversibly alters the state of the measured system.

The attempt to create a quantum analogue of classical error correction thus comes up against the limitations imposed by quantum theory. Algorithms for quantum error correction are therefore significantly different from classical approaches. The similarity lies in the fact that the qubits of a given technology (physical qubits) are grouped and encoded into larger units, which we call logical qubits (the definition and classification of qubit types is discussed in more detail in the following chapter). The fundamental aim is for the error rate and decoherence on the logical qubit to be lower than on the physical qubits.

The principle behind the operation of quantum error correction protocols lies in the ability to encode quantum information into one part of the system (physical qubits), whilst ensuring the ability to detect what error has occurred and correct it using weak measurements. This requires that errors on the physical qubits be sufficiently small and do not accumulate during the implementation of the protocol. There is therefore a threshold error size that the technology itself must achieve in order for error correction to be applied to it.

1.4.4 Basic building blocks of quantum computers

- **Physical qubit**

These qubits are the building blocks of quantum computers. They are actual physical systems used to store and manipulate quantum information. Each physical qubit can exist in a superposition of 0 and 1 and can be entangled with other qubits, enabling quantum computers to perform complex operations.

However, physical qubits are highly fragile and prone to errors caused by external noise, imperfect control and interactions with the environment (decoherence). Due to these instabilities, operations involving physical qubits are error-prone, which limits the reliability and scalability of current quantum computers.

Physical qubits are, however, essential for the development of quantum computers. They are used in today's NISQ (Noisy Intermediate-Scale Quantum) devices, such as the IBM Eagle processor or the Google Sycamore chip.

- **Logical qubit**

In quantum computing, logical qubits are a higher-level concept. These qubits are no longer a single physical entity; rather, they can be described as an encoded state distributed across many physical qubits.

The main purpose of these qubits is to achieve error correction, which they accomplish using quantum error-correcting codes. This system works by distributing information across multiple physical qubits in such a way that even if some physical qubits experience errors, the overall logical qubit remains stable and intact.

Logical qubits can detect and correct errors without disrupting the stored quantum information, making them resistant to noise and decoherence. The construction and operation of logical qubits is a crucial step towards creating fault-tolerant quantum computers capable of reliably performing long and complex computations.

Depending on the error correction methods and the required error rate, hundreds or even thousands of physical qubits are needed to create a single logical qubit.

1.4.5 Types of physical qubits

The way a quantum computer works is determined by the type of physical qubit used. The technology is not yet established, and there are several competing principles, each with its own advantages and disadvantages, as in practice not all qubits are of the same nature. In real quantum processors, the following are known:

- **Superconducting qubits**
  - Principle: Qubits consist of superconducting loops (e.g. Josephson junctions) through which current flows without resistance. The state of the qubit is determined by the quantum states of the current or phase.
  - Advantages: Easily scalable using lithographic techniques (CMOS-compatible), fast gates (~ns).
  - Disadvantages: Requires extreme cooling (~10 mK, cryostat), coherence ~100 µs (limited), high precision requirements.
  - Challenges for FT: Large number of qubits due to error rates, need for high-fidelity (accuracy) gates and an effective error correction code.
  - Manufacturers: IBM, Google, Rigetti, IQM (Finland),

- **Ion trap**
  - Principle: Individual ions are trapped in an electromagnetic trap and manipulated using lasers. The qubit is the electronic/spin state of the ion.
  - Advantages: Long coherence (on the order of seconds to minutes), high fidelity of two-qubit operations.
  - Disadvantages: Slower operations (ms), more difficult to scale (requires precise optics, cooling systems).
  - Challenges for FT: Better integration of optics and faster gates, modular scaling (e.g. linking multiple traps).
  - Manufacturers: IonQ, Honeywell/Quantinuum, Alpine Quantum Technologies (Austria)

- **Neutral atoms**
  - Principle: Neutral atoms are trapped in light traps (optical tweezers) and excited to Rydberg states, where they strongly interact with one another.
  - Advantages: Naturally high connectivity (every particle with every other particle), long coherence
  - Disadvantages: Requires extremely precise optics and lasers; complex control of multiple particles.
  - Challenges for FT: Improving gate fidelity and the stability of optical lattices.
  - Manufacturers: QuEra, Pasqal (France)

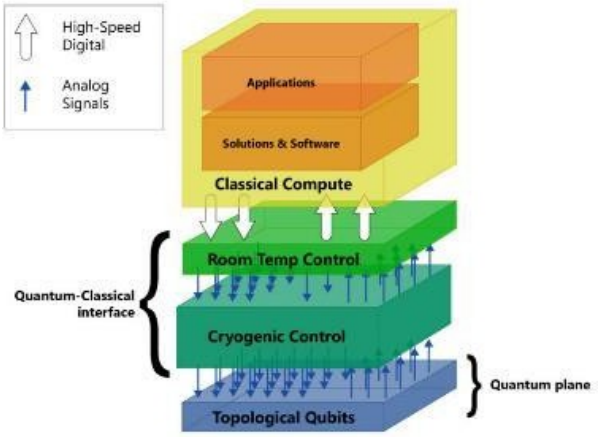
- **Photonic quantum computers**
  - Principle: Qubits are formed by photons in various modes (polarisation, path). Calculations are performed using interference and measurements.
  - Advantages: Operate at room temperature, easy distribution (optical fibres).
  - Disadvantages: Difficult deterministic implementation of quantum gates, low probability of interaction between photons.
  - Challenges for R&D: Ensuring deterministic gates and high-quality sources of single-photon states.
  - Manufacturers: PsiQuantum, Xanadu, Quandela

- **Spin qubits (quantum dots)**
  - Principle: Utilises the spin of an electron or hole in a quantum dot. Manipulation via magnetic field or microwaves.
  - Advantages: Potential integration with conventional chips, low power consumption.
  - Disadvantages: Very small dimensions, difficult to control and read.
  - Challenges for FT: Need for precise fabrication of quantum dots, improvement of coherence and readability of spin states.
  - Manufacturers: Intel, Universal Quantum (UK)

1.4.6 How quantum computers work

Quantum computations are performed on quantum chips, which may be based on various technologies. These chips are connected to classical interfaces that issue the computation, control the computation, and collect and interpret the results. However, given the technological complexity required for quantum chips to function correctly (very low temperatures, vacuum), creating a functional interface between classical and quantum technology is technologically very challenging.

Figure 2: Interconnection of the quantum and classical layers of quantum chip technology

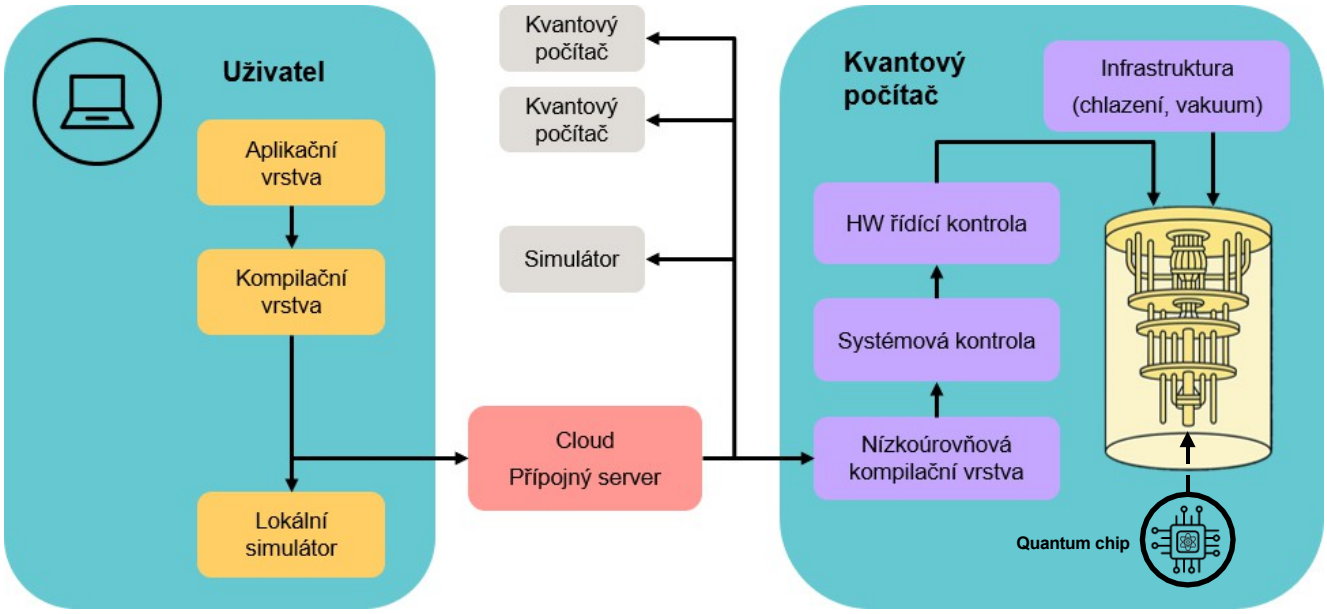


Typically, this integration consists of multiple layers, and the process of handling a user's request can be summarised, in simplified terms, as follows:

1. The user designs their algorithm in the application layer.
2. The algorithm is compiled in the compilation layer – it is optimised for the selected quantum computer and rewritten into a universal language.
3. The computation request is either executed locally (on a simulator) or sent to the cloud, which processes the request and queues it.
4. When it is the quantum programme's turn to run, the request is passed to the low-level compilation layer, where it is rewritten (recompiled) into a language understood by the devices operating the quantum computer in question. The programme is implemented as a time-specified set of operations.
5. The request is then processed by the system control, whereby individual operations are sent at the appropriate time to individual devices in the hardware layer, which in turn generate the relevant signals that are transmitted to the quantum processor.

Auxiliary devices ensure the proper functioning of the infrastructure required for the operation of the quantum chip itself – cryogenic cooling, vacuum maintenance, and the maintenance of constant atmospheric conditions for the optimal operation of all instruments. This entire system is illustrated in Figure 3.

Figure 3: Interconnection of the classical and quantum interfaces

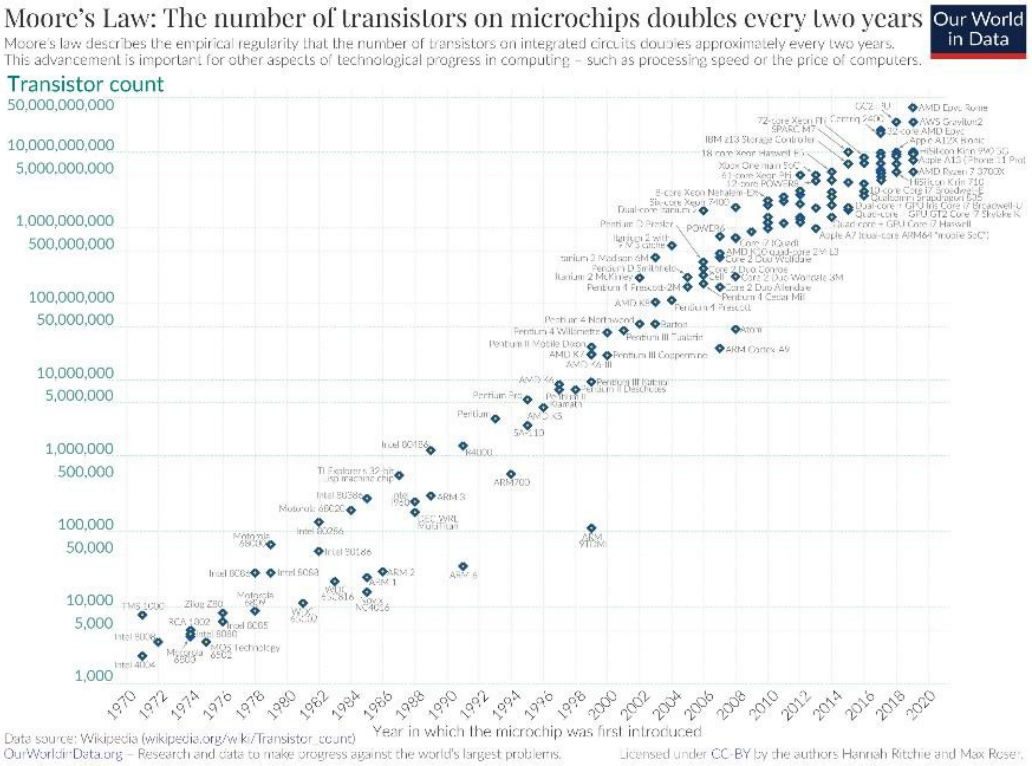


1.4.7 Manufacture of quantum components

Classical chips are manufactured using CMOS (Complementary Metal-Oxide-Semiconductor) technology. This process involves photolithography, in which complex transistor patterns are etched onto silicon wafers. Empirical data from the development of classical chips reveal patterns that are generally referred to as Moore's Law. This states that the number of transistors in integrated circuits doubles every two years[2] :

[2] https://ourworldindata.org/moores-law

Figure 4: Moore's Law from 1970 to 2020



This means that these components are inevitably becoming smaller, right up to the material limit of their computational power – it will no longer be possible to increase their performance further, not because of technical constraints in manufacturing, but because of the physical limits of the material used (silicon). Nowadays, we are talking about dimensions on the scale of a few atoms, and when developing such small classical chips, it is no longer possible to ignore quantum effects, which must be taken into account in their design so that they do not interfere with the requirements for standard chip behaviour. (However, these quantum effects are highly localised and cannot be utilised for quantum computations, which would require better control over the system.) Quantum computers could help overcome the problem of miniaturising classical chips by acting as solvers for specific complex sub-tasks.

In contrast, the manufacture of quantum chips depends on the type of physical qubits implemented. Superconducting qubit chips are made from superconducting materials such as niobium or aluminium. These materials exhibit zero electrical resistance at cryogenic temperatures, which enables the efficient use of these qubits. Spin qubits utilise the spin states of electrons confined within semiconductor quantum dots. Their manufacture involves advanced nanofabrication techniques to create and control these quantum dots. Chips with photonic qubits require the use of optical components, such as beam splitters and phase shifters, often fabricated on silicon photonic platforms. Each of these technologies requires specific manufacturing approaches that are not yet fully standardised, as is the case with the production of classical chips.

Whilst classical computer chips are capable of operating at temperatures ranging from 0 °C to 85 °C depending on the application of the technology, quantum components require extremely low temperatures to maintain the coherence of individual qubits. Temperatures vary depending on the types of physical qubits used, as described above. Most of these types require temperatures close to absolute zero, which necessitates continuously operating cryogenic equipment in the vicinity of the qubits to ensure the appropriate temperature conditions.

Photonic physical qubits are an exception; they can operate at room temperature, which offers advantages in terms of simpler integration and scalability, but at the same time places demanding requirements on the precise control of optical paths, interference and the detection of individual photons, which currently limits scalability in practice. Another limitation is that, unlike the deterministic gates in superconducting qubits, photonic gates are often probabilistic and require post-selection, which complicates scaling. Finally, there are also limitations with photon detectors. Either avalanche photodiode (APD) detectors are used, which operate at room temperature but have higher noise and lower performance, and are therefore often insufficient for high-precision quantum experiments, or superconducting single-photon detectors (SNSPDs) are used, which, however, only function at temperatures below 1 K. These detectors have high detection efficiency (often > 90%), low noise and very good temporal resolution, which is why they are preferred for quantum applications.

1.4.8 The state of development of quantum technologies and communication

The following chapter describes current technologies in the field of quantum computing across various organisations and countries. The description of the technologies includes key metrics indicating the state of technological development, such as the number of qubits and, for example, the speed of processing complex mathematical tasks. Related technical parameters, the description of which would require excessive technical expertise and whose elaboration within this study is not particularly relevant, are supplemented with references to the relevant sources.

- **IBM**

In the early stages of quantum technology development, IBM focused primarily on increasing the number of qubits to continuously boost the computational power of its devices; the IBM Condor processor, with a capacity of 1,121 qubits, now dominates this field. In 2023, however, IBM changed its strategy and, in addition to increasing processor capacity, began focusing on the quality and complexity of applications. The currently used IBM Quantum Eagle processor, with a capacity of 127 qubits, is now being replaced in experiments by the latest IBM Quantum Heron processor, with a capacity of 133 or 156 qubits. When comparing the Condor processor with the Heron processor, IBM does not expect the Condor processor to be as useful for performing quantum computations as the Heron, and regards it more as a research project aimed at expanding the company's hardware and software suite and testing the potential capacity of the processors. On the other hand, Heron represents a significant improvement in performance and is expected to deliver markedly better results in complex quantum computations[3] . IBM is continuously developing the next generation of processors with the aim of achieving a capacity of 100 million qubits with the Starling model by 2030 and the integration of quantum error correction[4] .

In developing its systems, IBM focuses not only on the quantum systems themselves, but also on increasing their versatility and utility. In particular, they are currently focusing on achieving so-called 'quantum utility', which means that their quantum systems would outperform classical computers when solving specific tasks. This can be achieved not only by improving the quality of processors, but also by combining classical and quantum computing approaches (quantum-centric supercomputing), and through modularity leading to the possibility of quantum interconnecting processors (IBM Quantum System Two utilises 3 Heron processors). Further contributing to this progress are Qiskit SDK, an open-source software development kit for quantum computers, and Qiskit Runtime, an optimised runtime environment developed by IBM. These systems are also available to external users, with access available on a pay-as-you-go basis ($96 per minute) or via subscription.

Figure 5: IBM quantum computer

[3] https://www.allaboutcircuits.com/news/closer-look-at-ibms-heron-and-condor-quantum-processors/

[4] https://www.ibm.com/roadmaps/quantum/

- **Google**

In 2019, Google achieved a breakthrough in quantum technology with the launch of the Sycamore model, which had a capacity of 53 qubits and was able, during testing, to perform a specific computational task in a fraction of the time taken by a classical supercomputer – they were the first to announce evidence of quantum supremacy (where quantum computation is significantly faster than classical computation). This result was later questioned by IBM and scientists from the Chinese Academy of Sciences, but not refuted. On the one hand, the research suggests that Google overestimated its estimate of the time required for classical computation (there are also more efficient methods for classical computation), but on the other hand, these classical results can only be obtained at the cost of using considerable resources, exceeding those of quantum computing.

Over the following years, Google worked hard on developing new models and improving existing ones; a key milestone in current development is the introduction of the Willow quantum chip with a capacity of 105 qubits in 2024. This latest product has become the flagship of Google's quantum development and, in computational tests, has once again outperformed the most powerful supercomputers; according to Google, it performed a calculation in 5 minutes that would have taken a classical supercomputer 10^{25} years.

Figure 6: Presentation of Google's Willow quantum chip

However, the Willow chip is, above all, an important milestone on the path to quantum error correction. By increasing the array of physical qubits encoding a single logical qubit – from a 3x3 grid of encoded qubits through a 5x5 grid to a 7x7 grid – the team succeeded in reducing the qubit error rate, thereby, according to team members, achieving values 'below the threshold' that enables scaling. However, as the implementation of a single logical qubit utilised almost the entire chip, this possibility remains purely hypothetical. Furthermore, error correction was only successful on the qubit that was not being manipulated, which is another factor introducing error rates into quantum computations.

- **IQM**

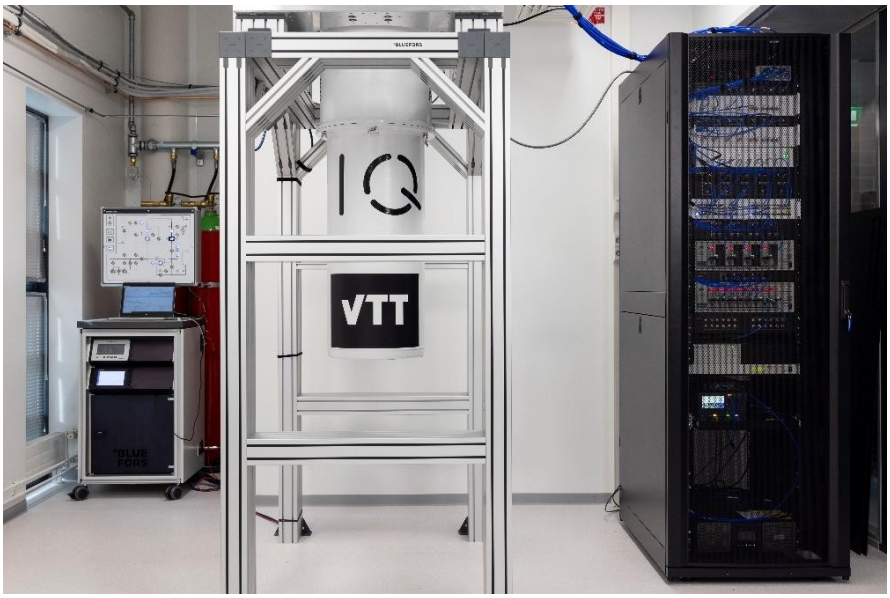
IQM Quantum Computers is a Finnish company founded in 2018 that focuses on the development of bespoke quantum processors, particularly for research and government institutions. IQM builds its processors on superconducting qubits and concentrates not only on increasing their number, but above all on improving the quality of operations, gate fidelity and stability. In 2023, it announced that it had achieved over 99.9% fidelity in two-qubit gates. In addition, it is working on technologies such as tunable couplers and quantum error correction schemes.

Instead of building its own cloud-based approach, IQM supplies complete quantum systems directly to partners, for example in Finland in collaboration with the VTT research centre[5] (5-, 20- and 50-qubit systems), or in Germany as part of the Euro-Q-Exa project[6] . The plan is to deliver a 24-qubit system in which all qubits are connected to a central resonator, thereby achieving connectivity between every qubit. The company is striving for European technological sovereignty and is collaborating on programmes such as Quantum Flagship, OpenSuperQ and Qu-Pilot. It is pursuing a fully vertical approach, from chip design to cryogenic infrastructure.

[5] https://thequantuminsider.com/2025/03/04/vtt-and-iqm-launch-first-50-qubit-quantum-computer-developed-in-europe/

[6] https://meetiqm.com/press-releases/iqm-selected-to-deliver-two-advanced-quantum-computers-as-part-of-euro-q-exa-hybrid-system/

Figure 7: VTT's Helmi quantum computer



- **Quantinuum**

Quantinuum is one of the leading research institutions in the field of quantum computers based on the principle of ion traps. Through gradual development, Quantinuum is slowly overcoming the main drawback of ion traps, which is poor scalability. It achieves this by replacing linear traps with so-called racetracks, where it is possible to store more ions at the cost of slower operations.
In collaboration with Microsoft, Quantinuum has achieved a breakthrough in the development of error-resilient quantum computers by demonstrating the creation of 4 logical qubits from 32 physical qubits in the Quantinuum H2 quantum processor[7] . Testing confirmed an error rate 800 times lower than the corresponding physical error rate. This model thus achieves an accuracy of 99.9% in the quantum operations performed[8] .

In 2025, Quantinuum plans to launch its first commercially available model, Helios. This system builds primarily on the highly advanced computational capabilities of the H2 model and its potential for further reliable scalability for industrial applications. Key features of the Helios model will include a capacity of over 50 logical qubits, whilst utilising insights from the H2 system in the field of sophisticated error correction techniques, thereby enhancing the stability and reliability of quantum operations. This model is expected to be used primarily in complex mathematical fields, such as knot theory, thanks to its effective analysis of complex topological structures[9] . Another anticipated benefit is the system's ability to enhance generative quantum artificial intelligence capabilities, particularly in fields such as drug discovery and materials science[10] .

- **Zuchongzhi**

In 2020, researchers from the University of Science and Technology of China (USTC) unveiled the Jiuzhang quantum computer, following the earlier release of Google's Sycamore model. At that time, both models achieved what is known as 'quantum computational advantage' or 'quantum supremacy' in tests, outperforming the most advanced classical supercomputers in specific tasks. In 2021, China continued to advance this technology by developing a 66-qubit programmable superconducting quantum computing system called Zuchongzhi 2.1. Recently, the successor to this model, Zuchongzhi 3.0 with a capacity of 105 qubits, was unveiled; according to available information, in one of the key tests of quantum technologies, random circuit sampling (RCS), it achieves results up to a million times better than Google's state-of-the-art Willow model.

When comparing the Zuchongzhi 3.0 and Willow models, however, it is also necessary to take into account the direction in which the individual scientific teams have taken their development. Zuchongzhi 3.0 focused primarily on scale and speed, whilst Google's Willow emphasised accuracy

[7] https://www.quantinuum.com/products-solutions/quantinuum-systems

[8] https://thequantuminsider.com/2024/04/16/three-nines-surpassed-quantinuum-notches-milestones-for-hardware-fidelity-and-quantum-volume/

[9] https://www.nature.com/articles/d41586-025-01094-z

[10] https://thequantuminsider.com/2025/02/04/quantinuum-touts-generative-quantum-ais-massive-commercial-potential/

via error-corrected qubits. Any claim of primacy or advantage is therefore subject to caveats regarding what was measured. The USTC experiment maximised the size and complexity of the circuit (while maintaining a sufficiently low error rate), whilst Google's experiment confirmed that logical qubits can outperform physical qubits in terms of reliability. Both of these experiments are major milestones on the path to useful quantum computers[11] .

- **AQT**

Alpine Quantum Technologies (AQT) is an Austrian company based in Innsbruck, founded in 2018 as a spin-off from the University of Innsbruck and the Austrian Academy of Sciences. It specialises in ion trap-based quantum computers – specifically, it uses individual ions trapped in a linear Paul trap as qubits. This approach offers long coherence times and high precision in operations, which are performed using laser pulses.

AQT emphasises modularity and compactness – their aim is to develop quantum computers as 'rack-mounted' devices compatible with conventional IT infrastructure. It offers access to its systems via the cloud as well as through physical devices for partners. In 2023, AQT announced the achievement of fidelities above 99.9% for both single- and two-qubit operations and continues to integrate the components needed for scaling, including microscopic ion chips and photonic interfaces. It currently offers the Marmot (20 fully connected qubits) and IBEX Q1 (12 fully connected qubits) quantum computers. AQT also offers remote access to its quantum simulators and computers via [the] Arnica[12]product.

- **D-Wave**

D-Wave Quantum Inc. is a Canadian company based in Burnaby (British Columbia), founded in 1999. It is one of the pioneers in the field of quantum computing, but unlike most other manufacturers, it focuses primarily on quantum annealing rather than universal quantum computing. It uses superconducting qubits arranged in specialised topologies (e.g. Chimera, Pegasus, Zephyr), which enable the solving of combinatorial optimisation problems. D-Wave builds systems with thousands of qubits — in 2020, it unveiled the Advantage system with 5,000 qubits, and in 2023, it announced the Advantage2 platform with the aim of achieving over 7,000 qubits and improved connectivity.

Although annealing processors are not universal (quantum algorithms such as Shor's or Grover's cannot be run efficiently on them), D-Wave has been striving in recent years to move closer to general-purpose quantum computing — it is developing a gate-model system (a classical quantum processor with gates), the initial version of which is to be accessible via the cloud. In addition to hardware, it also offers a comprehensive software layer, including the Ocean programming language, tools for hybrid computing and simulation libraries.

D-Wave collaborates with a number of industrial partners (e.g. Volkswagen, Lockheed Martin) on real-world applications of quantum annealing in logistics, planning and machine learning. The company also offers access to its systems via the Leap cloud service, including integration with AWS. Despite taking a different path from other manufacturers, D-Wave has a strong market position and was the first to offer a commercially available quantum computer[13] .

1.4.9 Selected quantum algorithms

As already mentioned, finding quantum algorithms that are both useful and faster than their classical alternatives is a complex process influenced not only by the limitations of quantum theory itself, but also by physical reality, embodied particularly in decoherence. Among the best-known algorithms are Shor's algorithm, Grover's algorithm, and the HHL algorithm. More modern approaches tend to focus on hybrid approaches, where quantum computations replace part of a larger computation. These include VQE and QAOA algorithms, for which greater efficiency compared to classical algorithms has not yet been demonstrated.

1.4.9.1 Shor's algorithm

Shor's algorithm is one of the most significant quantum algorithms from a cryptographic perspective. Peter Shor (*1959, American theoretical computer scientist) demonstrated that a quantum computer can efficiently factor large numbers, which means breaking these numbers down into the prime factors of which the original large number is composed, and thereby solve discrete logarithm problems, i.e. complex mathematical tasks that can be performed by one party but are very difficult for the other party to perform, and on which the security of common asymmetric ciphers such as RSA and ECC relies. Theoretically, this means that a sufficiently powerful quantum computer could factor, for example, a 2048-bit number (RSA modulus) in a matter of hours or days, thereby undermining the security of RSA and related

[11] https://postquantum.com/industry-news/zuchongzhi-3-0-quantum-chip/

[12] https://www.aqt.eu/products/arnica/

[13] https://www.dwavequantum.com/company/newsroom/press-release/d-wave-announces-general-availability-of-advantage2-quantum-computer-its-most-advanced-and-performant-system/

algorithms (e.g. the Diffie-Hellman algorithm, on the basis of which cryptographic keys are securely transmitted via public communication channels[14]).

Practical observations:

- It is estimated that breaking RSA-2048 would require a quantum computer with 'cryptographically relevant' parameters, i.e. with around twenty million qubits and advanced error correction[15] . Today's experimental quantum computers achieve performance in the tens to hundreds of qubits, which means that, for the time being, they do not pose a threat to well-implemented cryptography.
- In the estimate, it is possible to reduce the number of qubits at the cost of a higher number of operations.
- Current quantum computers are still too error-prone to run Shor's algorithm on numbers larger than a few bits; however, development in the field of quantum computing is constantly accelerating. This can be demonstrated by the development of quantum processors, whose performance has increased from 53 qubits (Google's Sycamore processor[16]) to 1,121 qubits (IBM's Condor processor[17]) over a five-year period, representing a more than twenty-fold increase. Furthermore, in 2024, Google unveiled the Willow chip with 105 qubits, which achieves a breakthrough in error correction[18] , and in spring 2025, a Chinese team from Hefei University of Science and Technology presented the Zuchongzhi 3.0 prototype with 105 qubits, which is expected to be even faster[19] ; we can therefore expect a gradual increase in the effective use of Shor's algorithm.

1.4.9.2 Grover's algorithm

Another significant quantum algorithm is Grover's algorithm, which accelerates brute-force search, i.e. searching in an unstructured database (Lov Kumar Grover, *1961, Indian physicist and computer scientist). Grover's algorithm reduces the time complexity of a brute-force search to roughly the square root of the number of combinations. In practical terms, this means that a quantum computer would be able to search the space of symmetric keys twice as fast as a classical computer. The impact on symmetric cryptography (e.g. AES) is such that the effective security level of an n-bit key drops to roughly n/2 bits. For example, a 128-bit key would have a strength of only 64 bits for a quantum attacker, which may no longer be sufficient. Fortunately, it is relatively easy to compensate for this loss – by switching to 256-bit keys. Both NIST and experts state that AES-128 and similar algorithms are still considered secure for the immediate future, but in the long term it is advisable to plan for the deployment of longer keys such as AES-256 in order to maintain a sufficient security margin[20] . An analysis was carried out within 3GPP to determine whether the 5G standard should be extended to support 256-bit ciphers; the conclusion was that this is not yet necessary in Release 16, but 256-bit algorithms are anticipated in the future[21] .

Practical observations:

- Encoding into a quantum database is not the only way to use Grover's algorithm; many computational tasks incorporate this search algorithm as a subroutine (certain machine learning network functions, etc.). In such cases, it is potentially possible to use a hybrid scheme where the quantum computer is repeatedly called with a partial task.
- Grover's algorithm is highly demanding to implement, and existing quantum computers do not yet provide any speed-up due to their error rates.
- Furthermore, the speed-up of Grover's algorithm diminishes very rapidly even with very small errors[22] and it is more likely that only a small speed-up in computations can be expected[23] .

[14] https://cdn.atis.org/atis.org/2025/02/25152429/Preparing-5G-for-the-Quantum-Era-WP-V9.pdf

[15] https://arxiv.org/pdf/1905.09749

[16] https://www.science.org/content/article/ordinary-computers-can-beat-google-s-quantum-computer-after-all

[17] https://www.ibm.com/quantum/blog/quantum-roadmap-2033

[18] https://blog.google/technology/research/google-willow-quantum-chip/

[19] https://english.news.cn/20250303/727767580e4a472ca44fd08f25666a25/c.html#:~:text=HEFEI%2C%20March%203%20%28Xinhua%29%20,in%20China%27s%20quantum%20computing%20advancements

[20] https://cdn.atis.org/atis.org/2025/02/25152429/Preparing-5G-for-the-Quantum-Era-WP-V9.pdf#:~:text=Asymmetric%20key%20cryptography%20faces%20significant,posing%20a%20profound%20security%20risk

[21] https://journal.accsindia.org/show.article.php?id=44#:~:text=introducing%20256-bit%20algorithms%20in%20future%20releases

[22] https://iopscience.iop.org/article/10.1088/1367-2630/16/7/073033

[23] https://journals.aps.org/pra/abstract/10.1103/PhysRevA.99.012339

1.4.9.3 HHL algorithm

Linear systems of equations $Ax\rightarrow=b\rightarrow\rightarrow$, where A is a known matrix and $b\rightarrow\rightarrow$ is the right-hand side, represent a fundamental computational problem found in both scientific and industrial applications, ranging from simulations of physical systems to machine learning. The classical solution of a system of dimension n requires a time that depends at least linearly on the size of the input. However, if we can appropriately encode both the vector $b\rightarrow\rightarrow$ and the matrix A into a quantum state and an operation, it is possible to use the HHL algorithm, which, under certain conditions, provides a solution in polylogarithmic time in n , i.e. O (log n). This difference is exponential compared to classical methods.

The HHL algorithm (Harrow–Hassidim–Lloyd) does not return a solution in the form of an explicit vector $x\rightarrow$, but in the form of a quantum state $|x\rightarrow\rangle$, which can be further manipulated quantum mechanically. Acceleration is possible if the matrix A is sparse, well-conditioned, and there is an efficient procedure for its quantum exponentiation. In such a case, it is possible to use the quantum algorithm to obtain
information about the solution, such as the calculation of expected values or correlations, without the need to fully decode the result.

Practical observations:

- The HHL algorithm does not solve the classical problem of 'multiplying the inverse of a matrix', but rather enables the acquisition of computationally accessible quantum representations of the solution.
- A prerequisite for acceleration is not only the sparsity of the matrix, but also its good condition (low condition number). For ill-conditioned problems, the computational complexity worsens.
- The quantum representation of the result does not allow for easy extraction of all components of the solution, but is suitable, for example, for calculating averages or nested computational steps within the quantum algorithm.
- As with other algorithms, HHL also requires extensive quantum memory and a low noise level, which current quantum processors do not yet provide[24] .
- Practical applications of HHL are expected to be found primarily in hybrid scenarios, where the quantum component solves a specific subproblem within a larger classical architecture.

1.4.9.4 VQE (Variational Quantum Eigensolver)

Many important tasks in physics, chemistry or optimisation involve finding the ground state of a quantum system, i.e. the state with the lowest possible energy. Classical algorithms for finding the ground states of quantum systems (e.g. molecules) suffer from an exponential increase in computational complexity with the size of the system.

The VQE algorithm circumvents this problem with a hybrid approach: a quantum computer prepares a parameterised quantum state and measures the expected energy value, whilst a classical computer optimises the parameters of the quantum state to minimise the energy.

This variational approach is well suited to current quantum computers with limited circuit depth. The computational complexity does not grow exponentially with the number of parameters, but the success of the algorithm depends heavily on the choice of ansatz (i.e. the chosen form of the parameterised quantum state) and the optimisation strategy.

Practical insights:

- VQE is one of the leading algorithmic candidates for the use of NISQ devices in the field of quantum chemistry.
- The accuracy of the calculation can be significantly affected by noise in the quantum hardware and the optimiser's inability to find the global minimum.
- Many practical implementations of VQE combine it with advanced classical optimisers and error-mitigation techniques.
- There is no general proof that VQE can find solutions faster than the best known classical methods.

1.4.9.5 QAOA (Quantum Approximate Optimization Algorithm)

Many optimisation problems, such as scheduling, resource allocation or MAX-CUT problems, are NP-hard (with complexity growing exponentially with the size of the problem) and classical algorithms provide only approximate solutions to them. QAOA is a quantum algorithm designed for these tasks, which utilises the alternation of two types of quantum operations: one corresponds to the classical energy of the problem (the so-called cost Hamiltonian) and the other serves to mix states (the mixer Hamiltonian).

In this way, QAOA prepares a quantum state that has a high probability of corresponding to a good solution to the optimisation problem. The parameters of the operations are optimised (as in VQE) by a classical algorithm. With a sufficient number of steps (algorithm depth), the algorithm theoretically approaches the exact solution, but in practice it is limited by the actual physical implementation.

[24] https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.050502

Practical observations:

- QAOA is proving to be a promising algorithm for the combined quantum-classical solution of combinatorial problems.
- The algorithm's effectiveness depends not only on the depth of the circuit, but also on the choice of initial parameters and the properties of the optimisation environment.
- Practical implementations face the limitations of current hardware – limited connectivity, error rates and low fidelity may prevent the achievement of advantages over classical heuristics.
- The ability to achieve quantum acceleration remains an open question – for QAOA, there is no proof that it achieves even quadratic, let alone exponential, advantages over classical algorithms.

1.5 Quantum communication

Unlike classical communication methods, the emerging field of quantum communication utilises the principles of quantum physics for the secure and efficient transmission of information and data. Classical communication methods rely on electromagnetic waves for transmission, whereas quantum communication uses qubits to transmit information; thanks to the property of superposition, these can exist in multiple states simultaneously. Another critical condition for the effectiveness of quantum communication is the property of quantum entanglement between individual qubits. Particles entangled in this way have interconnected states, meaning that the state of one particle immediately affects the state of the other particle, regardless of the distance separating them. This phenomenon is of fundamental importance for quantum communication, as it enables the instantaneous transmission of information between entangled particles[25] .

As described above, one of the key problems in cryptography is finding methods to establish a cryptographic key between two communicating parties so that each of these parties has the same key, and no one else has any (even partial) information about this key. It has been known since 1994 that all the algorithms originally used (RSA, Diffie-Hellman, …) will provide zero security once a so-called quantum computer is built. Worse still, all communication sent today is being stored on a large scale by attackers and will be decrypted retrospectively once quantum computers with sufficient processing power become available.

This has led to a search for alternatives, such as algorithms for which there is no known method of breaking them using either classical or quantum computers (so-called post-quantum algorithms). However, these algorithms can still be broken, not only by quantum computers but also by classical computers, as has already happened with several finalists in the NIST competition.

1.5.1 Quantum Key Distribution (QKD)

Another alternative is so-called Quantum Key Distribution (QKD) devices. These devices utilise the principles of quantum theory to make key sharing extremely secure. The following chapter, which focuses on QKD, provides a simplified description of the main features of how it works. The term 'quantum communication' will be used here to refer to classical communication supported by quantum technologies for sharing cryptographic keys.

1.5.1.1 QKD devices for key generation

QKD key generation devices are currently experimental devices with significant variations in their specifications; in other words, they are still at the development stage. At present, there are no standards specifying exactly what QKD devices must comply with; there are no standards regarding security requirements, no testing methodologies, and no laboratories capable of verifying these specifications. These issues are currently being addressed at EU level.

The principle of key generation in a quantum environment can be explained using the BB84 protocol. The protocol involves two parties, usually referred to as Alice and Bob, who wish to generate a secure shared key (Alice and Bob are, in fact, devices executing this protocol). Alice repeatedly and randomly prepares states (systems) from four specific possibilities. Each system is a potential source of one bit of the key. Alice's four choices encode not only a potential bit of the shared key (2 options), but also a random bit that designates the so-called encoding basis (2 options). The state prepared in this way from Alice's four (2 × 2) choices is sent to Bob, who randomly selects a basis for measuring the sent system. Alice and Bob then exchange information via a standard (unencrypted but authenticated) channel about how they performed their measurements. Since quantum measurements are typically destructive, if Alice's encoding basis differs from Bob's measurement basis, the protocol is designed such that the results of the quantum state measurements will be random for Bob and will not correspond in any way to the key bit that Alice sends. Therefore, if they detect errors, they know that someone has been eavesdropping, and they discard the key. Conversely, if Alice's encoding basis matches Bob's measurement basis, there is no change in state that would affect

[25] https://arxiv.org/abs/quant-ph/0702225

the result of Bob's measurement; he will therefore always measure the bit that Alice sends him. If everything is in order, they use the remaining bits as a secure encryption key.

Another advantage of using QKD devices is their resistance to quantum computers – quantum computers cannot be used to compromise the key in any way, as is the case with classical encryption algorithms. This security is therefore based on physical properties and does not depend on trust in the algorithm. The use of QKD devices thus leads to greater communication security.

QKD in relation to cryptography in a quantum environment is described further in Chapter 3.3.

1.5.1.2 Practical application of QKD in communication

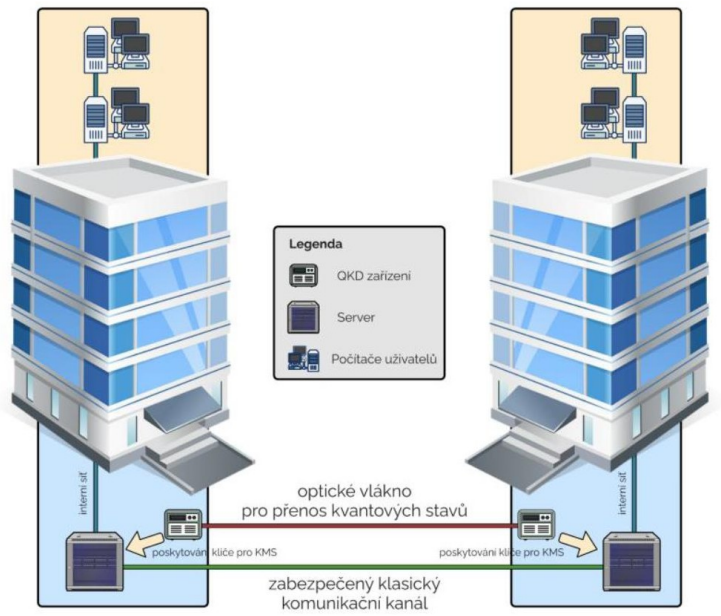
In practical terms, we can envisage quantum-secure communication as a connection between two devices that perform all security tasks themselves, including testing for the presence of a potential eavesdropping third party. The advantage is that existing optical networks can be used for the connection. However, to bridge longer lengths of optical fibre and achieve an acceptable amount of cryptographic key generated per second (key bit rate, measured in kbps), it is currently important that communication between devices takes place via so-called dark fibre, an unlit optical fibre (or pair of fibres), reserved solely for this communication. Furthermore, the connection must be uninterrupted, without amplifiers or switches that would disrupt quantum transmission.

The use of QKD devices is thus limited by the structure and existence of the optical infrastructure, its quality parameters (attenuation) and the availability of unused fibres. The cost of leasing optical fibres also plays a major role; for dark fibres in the Czech Republic, this ranges from 0.5 to 2.5 CZK per metre of fibre per month (excluding VAT), depending on the region and provider.

The QKD system consists of a pair of devices: a transmitter and a receiver. The transmitter sends single-photon signals containing encoded quantum information. These signals are transmitted via optical fibre to the receiver, which attempts to capture and decode them. Attenuation (along the transmission path) and the key bit rate are key parameters of this technology.

Once a shared key has been generated, the QKD devices then pass this key to the Q-KMS (Quantum Key Management System), which provides it to systems for encrypting standard communications in much the same way as any other generated key. The difference compared to classical (non-quantum) keys, however, lies precisely in its high security during generation and distribution. A diagram of the integration of QKD devices into the communication infrastructure is shown in Figure 8 below.

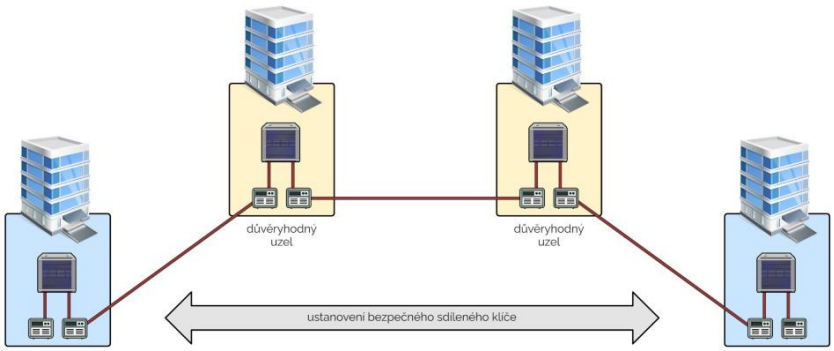
Figure 8: Visualisation of QKD usage for data transmission



The connection described above links only two communication nodes. In real-world operation, however, there is a network of variously interconnected nodes. Typically, nodes that are not directly connected communicate with one another. Even in such cases, highly secure communication can be ensured using QKD devices. In practice, a single pair of QKD devices is used for each direct connection, which generates a unique key between these nodes. For connecting remote nodes, there are algorithms that use the keys generated 'in pairs' at the directly connected

nodes. As there are currently no methods that can generate a key in this way without also having to generate a key on the connecting nodes, these connecting nodes must be trusted (so-called 'trusted nodes'). From a theoretical point of view, these methods are not inadmissible; they are merely technologically challenging to implement.

Figure 9: Creating a secure shared key via trusted intermediate nodes



1.5.1.3 Selected protocols for quantum key generation

Several types of protocols can be cited whose task is to ensure the secure distribution of encryption keys between two parties (e.g. Alice and Bob) using the principles of quantum mechanics. Their main functions and steps include the generation and exchange of quantum states, eavesdropping detection and error correction, and privacy enhancement (post-processing), with the output being a secure secret key that can be used for symmetric encryption.

- **BB84 protocol**

Secure distribution of a cryptographic key between two parties without a prior shared secret is a fundamental problem. The BB84 protocol [BB84] (essentially described above) was designed in 1984 and is the oldest and most widely used QKD protocol. Its conceptual simplicity makes it ideal for the first practical implementations. It utilises quantum bits, which are randomly prepared in different polarisation or spin states, and transmitted between the sender (Alice) and the receiver (Bob). Alice prepares a qubit in one randomly chosen basis out of two, and Bob measures the received qubit also in one randomly chosen basis. Only afterwards do they compare the bases used via a public channel, without disclosing the measurement results. Matching measurement bases determine the shared key. Any attempt by an attacker (Eve) to eavesdrop on the quantum channel leaves a detectable trace in the form of increased error rates.

The protocol requires that one node be capable of generating quantum states, whilst for the other node, the ability to measure the received state is more essential. To enhance security, so-called decoy states are used. These (occasionally generated) states act as a security trap, enabling the detection of whether someone is interfering with the transmission without knowing which pulses were key.

- **BBM92 protocol**

Whilst BB84 utilises active preparation and measurement of quantum states, the BBM92 protocol [BBM92] is based on quantum entanglement. A pair of photons in an entangled state is split between Alice and Bob, who perform measurements in randomly chosen bases. Entanglement results in a correlation between the measurements, from which a key can be derived. Unlike BB84, there is no need to actively prepare individual quantum states – the entangled source can be centralised and passively distribute pairs.

BBM92 is considered an entanglement-based analogue to BB84, with the advantage of enabling distributed key generation. Entangled protocols generally offer better resistance to certain types of attacks, but are technically more demanding to implement; in particular, a trio of devices is required – one for generating the entangled state and two for the communicating nodes.

- **Ekert91 protocol**

The Ekert protocol [Ekert91], proposed in 1991, utilises quantum entanglement and Bell's inequality theory to verify the security of communication. Alice and Bob measure entangled states in chosen directions, and in addition to key generation, they test the correlations of the results using Bell tests. If the results violate Bell's inequalities, this means that the communication could not have been classically simulated – which also means that no eavesdropping has taken place.

The protocol's security is based on the violation of Bell's inequalities, which provides theoretically strong protection against attacks even when the behaviour of the devices is unknown. However, practical implementation is very challenging due to the need for precise measurement of quantum correlations and sensitivity to noise.

- **COW protocol (Coherent One-Way)**

Quantum key distribution does not have to rely exclusively on individual particles or quantum entanglement – an alternative approach is offered by the COW protocol, which utilises coherent light pulses transmitted in a single direction. The key is encoded into the presence or absence of a light pulse within a time window. The receiver (Bob) records whether it has detected a pulse, whilst simultaneously testing the coherence between neighbouring pulses using interferometry, which enables the detection of an eavesdropper.

The COW protocol is designed with practical implementation in standard optical networks in mind, with low demands on quantum sources and detectors. Thanks to its resilience to losses and its ability to operate with intensity modulation, it is suitable for long distances. It does not provide the same level of theoretical security as protocols using individual quantum particles, but it is attractive for commercial deployment in real-world networks, e.g. within metropolitan QKD networks.

1.5.2 The state of development of quantum communication

- **Toshiba Europe**

As part of testing the possibilities of secure quantum communication, a quantum-encrypted signal was transmitted over a 254 km-long commercial telecommunications network in Germany using standard optical fibres and simple semiconductor technology, without the need for cryogenic equipment. This breakthrough enables the integration of quantum key distribution (QKD) and other quantum-secure communication protocols into existing telecommunications infrastructure on a national scale, significantly reducing costs and barriers to deployment. The trial represents a significant step towards a global quantum internet, as it demonstrates that quantum data can remain stable over long distances using commonly available equipment in standard data centres[26] .

- **China**

In 2016, a Chinese research team launched the Micius quantum satellite, which became the first of its kind to successfully conduct a quantum key distribution (QKD) experiment from space to Earth. In 2017, as part of further testing of the Micius satellite, a quantum entanglement link was established over a distance of 7,600 km with a counterpart in Austria[27].

Following the successes of the Micius satellite, scientists from South Africa and China achieved the longest quantum entanglement to date in 2024, at a distance of 12,900 km, using the Chinese Jinan-1 quantum microsatellite in low Earth orbit. The international team demonstrated real-time quantum key generation using quantum key distribution (QKD) technology. This process enabled the secure encryption of data transmitted between ground stations in China and South Africa using one-time pad encryption, and allowed more than a million quantum-secure bits to be transmitted between the two countries in a single orbit[28] .

- **Boeing USA**

In 2026, Boeing plans to launch the Q4S satellite mission to demonstrate the exchange of quantum entanglement in orbit, a significant step towards building a secure global quantum internet. The aim of this first initiative of its kind, developed in collaboration with HRL Laboratories, is to explore how quantum networks can operate over vast distances whilst maintaining synchronisation and minimising data loss. The Q4S mission will test communication based on quantum teleportation, which could enable future applications such as fault-tolerant quantum computing, secure voting and blind quantum computing. Boeing's vision is to deploy these quantum technologies on a large scale, and satellites equipped with entangled photon sources will provide critical data for the development of space-based quantum networks and ultra-secure communications[29] .

[26] https://www.toshiba.eu/newsroom/toshiba-breakthrough-brings-quantum-communications-to-existing-national-scale-telecommunications-infrastructure/

[27] https://www.sciencedaily.com/releases/2025/03/250319142833.htm

[28] https://spaceinafrica.com/2025/03/20/south-africa-and-china-establish-12900-km-quantum-satellite-link/

[29] https://boeing.mediaroom.com/2024-09-10-Boeing-Pioneering-Quantum-Communications-Technology-with-In-Space-Test-Satellite

2 5G architecture and its cryptographic protection

2.1 5G security architecture

2.1.1 Authentication protocols

The purpose of primary authentication and key agreement (AKA) procedures is to enable mutual authentication between the user equipment (UE) and the network and to provide key material that can be used between the UE and the serving network in subsequent security procedures. The basic authentication protocols according to the 3GPP TS 33.501 (Rel-15) specification are[30] :

- **5G-AKA**

This authentication protocol is a direct continuation of the protocol known from 3G and 4G networks, using symmetric keys between the UE and the network only within 3GPP access technologies (e.g. NR, LTE), and is one of two mandatory authentication methods within the 5G architecture.

- **EAP-AKA**

The second authentication protocol required for access to the 5G core via any type of access is EAP-AKA. This method integrates the EAP (Extensible Authentication Protocol) framework firmly into 5G security, unlike EPS (Evolved Packet System), where support for EAP-AKA/EAP-AKA' was used only for non-3GPP access. Unlike 5G AKA, this authentication protocol is also applicable to non-3GPP access (e.g. Wi-Fi, LAN, unauthorised access), thereby offering broader possibilities and flexibility of use.

2.1.2 Encryption and data protection

Building on previous generations, the 5G architecture continues to utilise proven security and encryption algorithms to provide secure communication services for end devices as well as the infrastructure itself. As with 4G, encryption algorithms based on SNOW 3G, AES-CTR and ZUC are used, along with integrity algorithms based on SNOW 3G, AES-CMAC and ZUC[31]. The main key derivation function is based on secure HMAC-SHA-256.

5G systems also include protection against eavesdropping and signal-modifying attacks. A new feature compared to previous generations is data integrity protection not only for data at the control plane level, but also for user plane data. This new feature enables the effective detection of any attempts to modify data during transmission and is particularly valuable for small-volume data transfers, especially with regard to IoT devices[32] .

As part of 3GPP Rel-15, a new and key feature, network slicing, was also introduced for 5G. This technology enables communication service providers (CSPs) to create virtual networks that are optimised for the specific needs of particular users or applications. This concept allows the physical network infrastructure to be literally divided into virtual segments that can be managed independently and provide specific levels of performance, throughput and security.

In other words, 5G network slicing is a network architecture that enables the multiplexing of virtualised and independent logical networks on the same physical network infrastructure. Each network segment is an isolated end-to-end network tailored to meet the various requirements of a specific application. In practice, network slicing therefore means that a 5G network operator can create various virtual

[30]https://www.3gpp.org/technologies/sec-npn

[31]https://www.3gpp.org/dynareport?code=35-series.htm

[32]https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security---enabling-a-trustworthy-5g-system

networks, which will also guarantee the various parameters required for different customers and applications. The logical part of the network therefore serves only a specific purpose or a specific customer, thereby providing unique independence and security for individual virtual networks.

2.2 Points of vulnerability

- **Authentication between the UE and the network core**

In 5G networks, user identity protection is ensured by the Subscription Concealed Identifier (SUCI), which replaces the permanently identifying Subscription Permanent Identifier (SUPI). The SUCI is generated by the user equipment (UE) using asymmetric cryptography, specifically the Elliptic Curve Integrated Encryption Scheme (ECIES), which utilises the home network's public key. This mechanism ensures that the user's true identity is not revealed during the initial connection to the network, thereby protecting against eavesdropping attacks such as IMSI catchers. The protection of the user's identity and data is part of the 5G-AKA and EAP-AKA authentication protocols and is specified within 3GPP TS 33.501.

- **Transport encryption**

Data transmission between base stations (gNB) and the network core (5GC) takes place over unsecured transport networks, which requires the implementation of security measures to ensure data confidentiality and integrity.

The 3GPP 33.501 specification recommends the use of protocols such as IPsec (an encryption algorithm that protects data transmission between devices by encrypting individual IP packets and simultaneously authenticating the source of the data) or TLS (a protocol that uses public-key encryption, authentication of information, and detection of unauthorised data tampering) to secure these connections. These protocols provide encryption and data integrity protection, thereby safeguarding against eavesdropping and unauthorised interference.

- **Control channels**

Control channels in 5G, which transmit data between the UE and the network, are protected using standard 128-NEA1/2/3 encryption algorithms and 128-NIA1/2/3 integrity algorithms. These algorithms prevent eavesdropping and data modification during transmission.

- **Software-defined elements**

5G utilises new technologies that virtualise services previously provided by hardware. These services include:

1) Network Functions Virtualisation (NFV)

This technology allows communication services to be separated from dedicated hardware, such as routers and firewalls. This separation means that network traffic can provide new services dynamically without the need to install new hardware. Deploying network components with Network Functions Virtualisation takes a fraction of the time required to deploy traditional networks. Virtualised services can also run on cheaper generic servers instead of proprietary hardware.

2) Software-defined networking (SDN)

is an approach to networking that uses software drivers or application programming interfaces (APIs) to communicate with the underlying hardware infrastructure and to control network traffic. This model differs from traditional networks, which use dedicated hardware devices to control network traffic. SDN can create and manage a virtual network, or control traditional hardware via software.

Whilst network virtualisation allows different virtual networks to be segmented within a single physical network or devices in different physical networks to be interconnected to form a single virtual network, software-defined networks enable a new way of controlling the routing of data packets via a centralised server.

These technologies increase network flexibility and efficiency, but at the same time increase the risk of virtualised network services being compromised through the exploitation of software component vulnerabilities or unauthorised access to network functions.

3 Cryptography

3.1 Introduction to cryptography

Information encryption is one of the fundamental requirements in a digital environment, as it secures the transmission of information and data and prevents the misuse of such materials. Data security is based on two fundamental encryption methods: symmetric and asymmetric key encryption.

3.1.1.1 Symmetric encryption

In symmetric encryption, the same key is used for both encrypting and decrypting the message being sent, which offers several advantages to this method of security, such as the speed of message processing due to the use of a single encryption key (compared to the asymmetric method), efficiency in the use of computing power and energy required to encrypt and decrypt the message, and compatibility with a wide range of systems and devices, meaning very easy integration into existing and functioning applications and systems without the need for major modifications. Conversely, it is precisely the simplicity of a single key in this model that poses a security risk in situations where this key falls into the wrong hands; in this respect, this method is more vulnerable in terms of key distribution than the asymmetric method.

Among the most widely used symmetric encryption algorithms are:

- AES (Advanced Encryption Standard)
- 3DES (Triple Data Encryption Standard) – an older standard, now being replaced by AES
- Blowfish

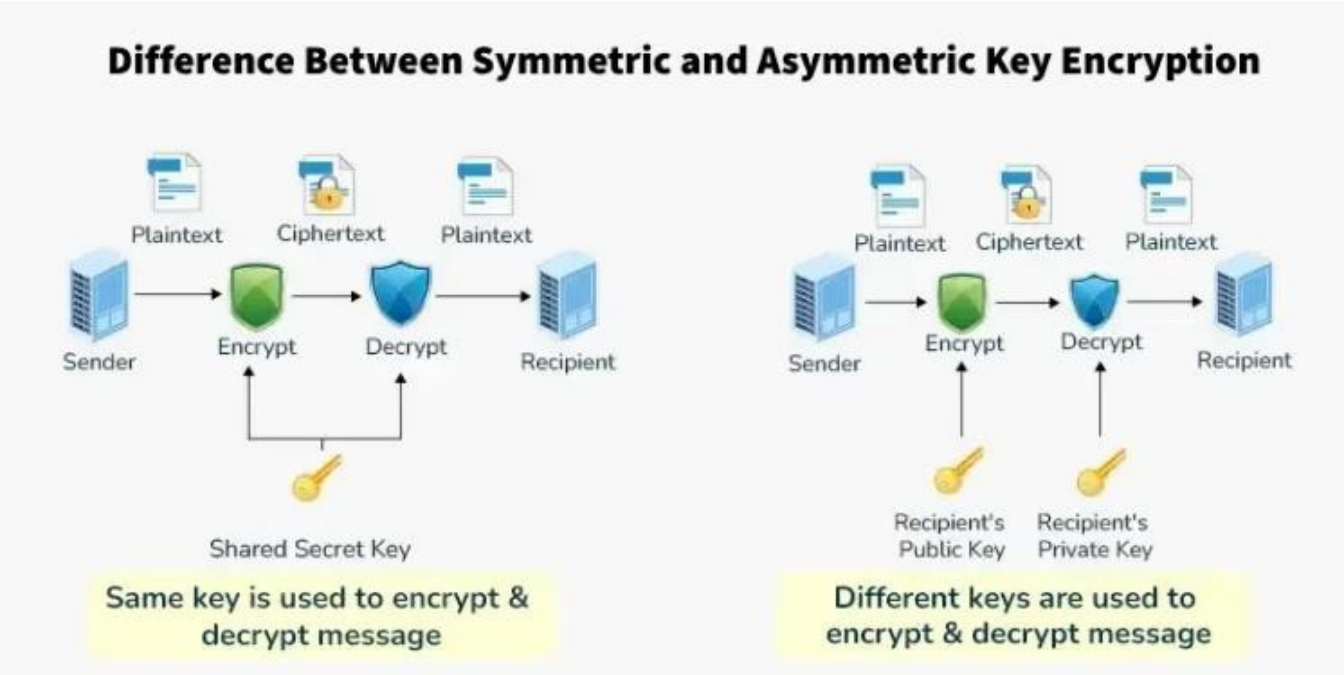
3.1.1.2 Asymmetric encryption

Unlike the previous, symmetric, encryption method, in this case a single ‘public’ key is used to encrypt the message, which is publicly available to all network users for encrypting data, and a separate ‘private’ key is used to decrypt the message, which is unique to each user. This private key can also be used for digital signatures and authenticity verification. The advantage of this principle is greater information security, particularly because there is no need to share a secret key in advance (unlike with symmetric encryption). Anyone can encrypt data for the recipient using their public key, but only the recipient can decrypt it using their private key.

The most widely used asymmetric encryption algorithms include:

- RSA (Rivest-Shamir-Adleman)
- ECC (Elliptic Curve Cryptography) – stronger security with smaller keys, ideal for IoT devices, for example
- DSA (Digital Signature Algorithm)

Figure 10: The difference between symmetric and asymmetric key encryption



3.2 Post-quantum cryptography (PQC)

Post-quantum cryptography is a field of cryptography concerned with the development and implementation of algorithms resistant to quantum attacks without the need for new hardware components. These algorithms are designed to be secure against both classical and quantum computers, and their integration into existing networks requires minimal changes to the current infrastructure. The rationale for deploying PQC lies in the ability of quantum computers to solve the mathematical problems underpinning current asymmetric cryptographic systems (e.g. RSA or ECC) far more efficiently than classical computers. In particular, Shor's algorithm enables the factorisation of large numbers or the solving of discrete logarithm problems, upon which these classical methods are based.

To ensure the resilience of cryptographic systems against new threats, PQC algorithms utilise mathematical problems that are considered difficult to solve even with the aid of quantum algorithms. The main classes of algorithms include:

- Lattice-based
- Code-based
- Hash-based
- Multivariate (multivariate polynomials)

In 2024, NIST introduced new standards[33] , which stand out for their compact key sizes and operational efficiency, making them suitable for integration into current communication systems. These keys include:

- **ML-KEM** (Module-Lattice-Based Key-Encapsulation Mechanism)[34] : a post-quantum cryptographic key-encapsulation mechanism (KEM) that enables two parties to securely establish a shared secret key over a public channel and is based on the CRYSTALS-Dilithium algorithm. Its security is based on the mathematical problem of Module Learning with Errors and is currently expected to withstand attacks by quantum computers; the standard defines three security levels: ML-KEM-512, -768 and -1024.

[33] https://csrc.nist.gov/projects/post-quantum-cryptography

[34] https://csrc.nist.gov/pubs/fips/203/final

- **ML-DSA** (Module-Lattice-Based Digital Signature Algorithm)[35] : used to verify data integrity and the identity of the signatory, whilst also ensuring so-called non-repudiation, i.e. the impossibility of subsequently denying the signature. The ML-DSA standard defines the CRYSTALS-KYBER algorithm for generating and verifying digital signatures, which are considered secure even against attacks by quantum computers.

- **SLH-DSA** (Stateless Hash-Based Digital Signature Algorithm)[36]: this standard defines a stateless hash-based digital signature algorithm designed to verify the integrity of data and the identity of the signer, whilst ensuring the authenticity of the signature. SLH-DSA is based on the SPHINCS+ algorithm, which was selected for standardisation as part of the NIST process for post-quantum cryptography.

Furthermore, in March 2025, the **HQC** (Hybrid Key Encryption) algorithm was selected for standardisation to expand the portfolio of post-quantum KEM ciphers[37] .

3.2.1 Advantages of PQC

- **Compatibility and ease of deployment**: Unlike QKD, it requires no new physical channels or hardware. It can be implemented as a software update to existing systems, which facilitates its deployment. Furthermore, during the transition period, PQC can be combined with traditional cryptographic protocols, enabling a gradual transition to quantum-resistant systems without disrupting existing operations. This hybrid approach should thus ensure continuity and security during the migration period.
- **Broader scope of cryptographic functions**: PQC offers not only a replacement for key exchange but also for digital signatures and other asymmetric functions. This is important for 5G networks, which utilise cryptography across a wide range of services, from user authentication to application interface security. PQC algorithms enable the creation of quantum-resistant digital signatures that can replace existing ECDSA signatures (an asymmetric cryptography algorithm) in 5G core protocols and certificates. In contrast, QKD addresses only the distribution of symmetric keys.

3.2.2 Disadvantages of PQC

- **Key size and its impact on performance**: PQC generally requires larger key sizes compared to traditional public-key cryptography. This could result in longer encryption and decryption times. Other potential challenges include increased storage requirements, higher memory usage and bandwidth demands. On a smaller scale, these obstacles might go unnoticed; however, the need to use keys in large volumes presents a problem. At the same time, performance issues may arise with older devices, which could hinder the deployment of this cryptography.
- **Insufficient vetting and the risk of future attacks**: Although the NIST algorithms have undergone intensive testing as part of the standardisation process, their long-term resistance to as yet unknown attacks is not guaranteed. History shows that even well-vetted algorithms can be broken using a standard computer. An example is the aforementioned SIDH algorithm, which is vulnerable to efficient key recovery attacks[38] . Even during the final round of the NIST selection process, several algorithms were broken using a classical computer[39] .

3.3 The applicability of quantum key distribution (QKD)

The principles and current state of development of quantum key distribution as a method of quantum cryptography, which utilises the principles of quantum mechanics to securely share secret keys between two parties—where the quantum state cannot be measured without affecting it—were presented in Chapter 1.5.1. In practice, this method works by one party transmitting individual photons in specific quantum states, which represent bits of information. The other party then measures these photons. If anyone attempts to eavesdrop on the transmission, the quantum properties of the photons change, causing detectable errors in the communication. This ability to detect eavesdropping is a key element of QKD security.

[35] https://csrc.nist.gov/pubs/fips/204/final

[36] https://csrc.nist.gov/pubs/fips/205/final

[37] https://csrc.nist.gov/pubs/ir/8545/final

[38] https://eprint.iacr.org/2022/975.pdf

[39] https://www.cryptomathic.com/blog/nist-pqc-finalists-update-its-over-for-the-rainbow

The purpose of using QKD is to combine standard and quantum technologies – to securely distribute an encryption key between two parties using quantum phenomena, whilst the encrypted communication itself then takes place over classical (legacy) communication systems. The quantum key itself is distributed via a special quantum channel, but also using standard technologies.

3.3.1 Advantages of QKD

- **Eavesdropping detection**: Any attempt at eavesdropping is detectable thanks to the quantum properties of the transmitted particles, i.e. when there is an increase in the error rate of the transmitted quantum bits. The communicating parties perform statistical checks for errors and deviations in the shared key, and if they detect that the error threshold has been exceeded, the quantum channel is considered compromised and the key is not used.
- **Clearly defined security:** Unlike asymmetric cryptography algorithms, which are based on mathematical problems and the assumption that no efficient solution exists on either classical or quantum computers (this assumption has already been shown to be incorrect for many algorithms, in some cases with a delay of several decades), the security of QKD is based on the highly transparent and straightforward laws of quantum physics.
- **Long-term security**: Unlike classical methods, which may be broken by quantum computers in the future, QKD provides security based on physical principles. Communication networks secured solely by mathematical operations may be vulnerable to 'Harvest Now Decrypt Later' attacks (see below).
- **Integration into existing infrastructure**: Recent experiments show that QKD can be implemented using existing optical and satellite networks, which reduces costs and increases the expected availability of the technology.

3.3.2 Disadvantages of QKD

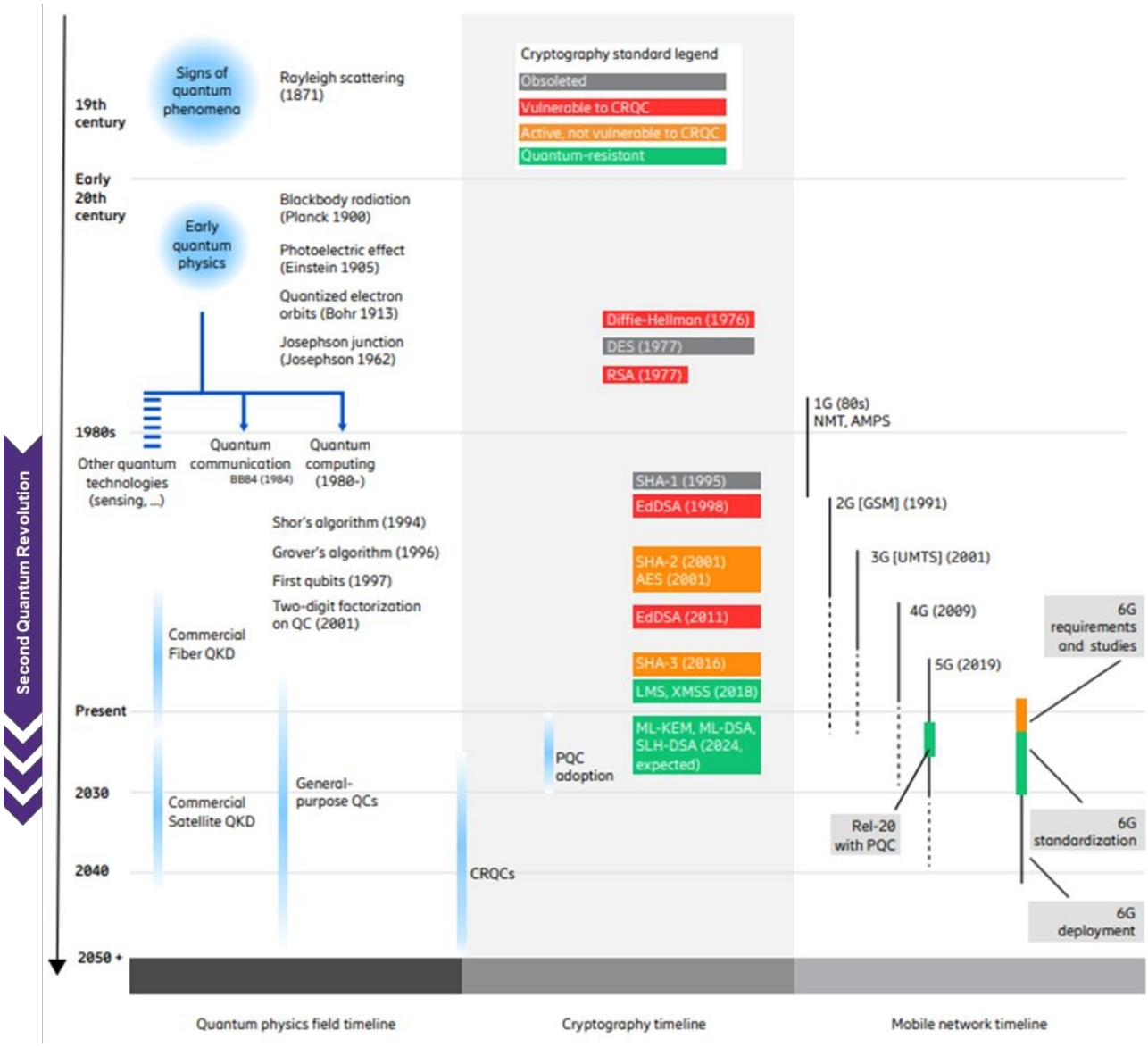
- **Limited range**: The extreme sensitivity of quantum communication to noise currently limits the maximum length of a single quantum link to approximately 170 km in commercial systems. Consequently, it is necessary to build physical infrastructure or extend this distance using quantum repeaters, which are still under development, or via specially positioned nodes; however, these in turn increase potential risks (QKD systems can be compromised at this 'trusted' node). In a 5G network environment, this means that QKD is currently only usable for backbone and metropolitan interconnections (e.g. between exchanges, data centres, base stations and the network core), where dedicated fibres can be laid. It cannot be used directly for mobile users.
- **High cost**: QKD systems require specialised equipment, precision optical components, cryogenic cooling of detectors to suppress noise, etc. Such equipment is currently expensive, and its installation and maintenance are demanding. In addition to the quantum transmitters themselves, conventional supporting infrastructure (for service connections, synchronisation, management) is also required, which increases complexity. Ericsson states explicitly that QKD requires specialised hardware, high maintenance and is associated with high costs, which makes its wider deployment impractical.
- **The need for authentication**[40]: QKD alone does not ensure the authentication of communicating parties, which requires a combination with classical cryptographic methods. The quantum channel requires a trusted, classically authenticated channel (e.g. using a pre-shared secret or a classical digital signature) to prevent man-in-the-middle attacks. This reliance on classical cryptography must be protected using algorithms which are, in turn, potentially vulnerable to quantum computation. For example, the UK's National Cyber Security Centre (NCSC) warns against relying solely on QKD and emphasises that the deployment of standardised PQC is more suitable for critical infrastructure.

[40] https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies

4 History of development

The purpose of the following diagram is to illustrate the history of development of the individual technologies covered by this study, namely quantum physics (or QC), cryptography and mobile network technology, and to place the aforementioned cryptographic standardisation activities within a timeline relative to developments in QC and mobile technologies.

Figure 10: History of technological development in quantum physics, cryptography and mobile networks



5 Threats to quantum computing to 5G

A sufficiently powerful quantum computer, also referred to as a CRQC (capable of breaking current ciphers), would have a fundamental impact on the security features of 5G networks. The threats can be divided into two main categories: (1) Breaking asymmetric cryptography, which ensures authentication and key exchange, and (2) weakening symmetric cryptography used for data encryption. Additionally, new types of attacks enabled by quantum technologies can also be considered (e.g. side-channel attacks, QMITM, HNDL).

5.1 Breaking asymmetric cryptography

Once a quantum computer capable of running Shor's algorithm on keys of common lengths (e.g. 2048-bit RSA or the stronger 256-bit ECC) becomes available, all 5G security protocols utilising these algorithms will become vulnerable. An attacker with a CRQC could eavesdrop on and decrypt communications in real time that are currently considered secure. In the context of 5G, this means that such an attacker could compromise both the confidentiality and integrity of DTLS/IPsec-secured channels within the core or between networks. For example, an encrypted connection between an operator's core and a base station could be compromised if an attacker factorialises the RSA/ECDH used and obtains the encryption keys. Furthermore, they could forge digital signatures and potentially impersonate legitimate network elements. This would render the authentication infrastructure ineffective: an attacker could act as a 'man-in-the-middle' between the user and the network without being detected by existing mechanisms, as they would be able to mimic valid certificates or signatures. Such a situation could threaten not only users' privacy (eavesdropping on calls, obtaining sensitive data), but also the security of critical services (manipulation of commands in industrial applications using 5G, disruption of IoT sensors, etc.).

5.2 Implications for symmetric cryptography

Although Grover's algorithm does not pose as acute and total a threat as Shor's, its effect cannot be overlooked. In a 5G environment, a potential attacker could accelerate a brute-force attack against encrypted messages or authentication codes. For example, if the cipher used had only a 128-bit key, a quantum attack would effectively reduce it to 64 bits, which under certain circumstances could allow it to be broken (provided the attacker had extreme computational power and time). It is generally considered that 128-bit symmetric algorithms currently provide a sufficient security margin even against quantum attacks; however, for systems requiring long-term security (a horizon of 20 years or more), many experts already recommend switching to 256-bit keys as the standard. Within 5G, therefore, symmetric components are likely to be strengthened in the future, e.g. the gradual replacement of the 128-EEA3 algorithm (ZUC with a 128-bit key) with the 256-EEA4 variant using a 256-bit key, once it has been standardised[41] . As early as Rel-17, 3GPP extended support for algorithms to 192-bit keys in certain cases, and 256-bit keys are simply the next logical step towards strengthening security. This would eliminate the impact of Grover's algorithm (a 256-bit key would be reduced by Grover to an effective ~128 bits, which is still considered secure)[42] .

Another aspect of symmetric cryptography is the length and security of hash functions and MACs. Quantum attacks may also speed up the search for hash collisions (e.g. using Grover's algorithm modified for the problem of finding a preimage). This could theoretically affect integrity codes in 5G that use hashes (e.g. HMAC-SHA256). However, it is expected that a transition to longer hashes (SHA-384/512) or the use of so-called quantum-resistant hashes (e.g. based on higher output entropy) would be a sufficient measure. Current 5G specifications already account for SHA-256/384, so there is a certain margin here as well[43] .

[41] https://www.3gpp.org/ftp/tsg_SA/WG3_Security/TSGS3_94AH_Kista/SA_83/33841-g10.docx

[42] https://www.3gpp.org/ftp/tsg_sa/WG3_Security/TSGS3_115_Athens/SA_103/33246-j00.doc

[43] https://atis.org/?download_id=1961732&sdm_process_download=1

5.3 Quantum decryption

In so-called quantum decryption attacks, attackers exploit the capabilities of future powerful quantum computers (CRQC) to break current encryption methods. This process may not be instantaneous and may require a certain amount of time, during which attackers intercept encrypted communications. Once the quantum computer has successfully decrypted the data, the attacker gains access to sensitive information without the communicating parties being aware of the breach.

An example of such an attack on 5G network infrastructure could be a situation where communication between mobile devices and network nodes is secured by public-key infrastructure (PKI) systems, for example using RSA or ECC (elliptic curve cryptography). An attacker with a quantum computer implementing Shor's algorithm intercepts the encrypted messages flowing within this communication. The quantum computer can then quickly break the public key used, thereby obtaining the keys used to encrypt the data.

Once the attacker obtains these keys, they are able to decrypt not only the intercepted communication, but also all other messages—past, present and future—that have been or will be encrypted using the relevant public key. This can lead to large-scale data breaches, the exposure of sensitive personal information, confidential business data or even critical information relating to national security. These attacks therefore pose a serious security threat that organisations must take very seriously as they prepare for the advent of quantum technologies.

5.3.1 "Harvest now, decrypt later" (HNDL)

In this type of attack, attackers intercept and store data currently transmitted in encrypted form with the aim of decrypting it as soon as a sufficiently powerful quantum computer (a so-called CRQC) becomes available. This poses a significant risk to data that is intended to remain confidential for a long period.

This can be illustrated by the example of 5G mobile network infrastructure. An attacker can strategically intercept encrypted communications between users and base stations or between individual network elements. Such sensitive data (such as government or corporate secrets) is typically encrypted today using modern standards such as the Advanced Encryption Standard (AES-128) or Elliptic Curve Integrated Encryption Schemes (ECIES), which are considered secure against classical computer attacks. However, attackers do not attempt to decrypt this data immediately. Instead, they store it securely and wait for the arrival of sufficiently powerful quantum computers capable of breaking current encryption, for example using Shor's algorithm (for public keys) or Grover's algorithm (for symmetric keys). This strategy allows today's security measures to be circumvented and makes the HNDL attack a highly dangerous threat to the long-term confidentiality of data in 5G networks.

A few years ago, it was generally assumed that Grover's algorithm required doubling the length of symmetric keys – i.e. using AES-256 instead of AES-128 – to ensure the same level of security against a quantum attack. However, according to the current position of the National Institute of Standards and Technology (NIST), Grover's algorithm does not pose an immediate threat to AES-128. Nevertheless, the resilience of AES-128 depends significantly on the quality of the entropy used in key generation. Low-quality entropy can make the AES-128 cipher vulnerable not only to future quantum attacks but also to current classical attacks, as stated in the ATIS study 'The Impact of Entropy on the Resistance of Symmetric Encryption to Quantum Attacks'.

Given the nature of HNDL attacks, intercepted sensitive encrypted data may remain at risk for many decades. In this context, a crucial question arises: How long will AES-128 remain sufficiently secure in the face of rapidly evolving quantum technologies? Although current NIST guidance provides short-term reassurance, organisations should actively consider strategies to ensure long-term security. One option is to transition early to more robust algorithms, such as AES-256 or other quantum-resistant encryption methods. This proactive approach will help protect sensitive communications from both current and future threats in a dynamically evolving cybersecurity landscape.

5.3.2 Quantum Impersonation Attack

Quantum impersonation attacks represent a type of cyber threat in which an attacker also exploits the capabilities of quantum computers to break public-key cryptography (PKI) systems. The essence of such an attack is impersonating another person or entity by stealing a digital identity. This means that an attacker can use compromised digital signature keys to sign documents, send fake messages or carry out transactions that appear to originate from legitimate users. This type of attack therefore does not merely involve the ability to decrypt communications, but also enables large-scale fraud and identity theft.

This can be exploited in infrastructures where PKI is used, for example, for authentication between individual network operators. Authentication often occurs when interconnecting networks of different operators, for example in different geographical areas or separate administrative domains. Here, PKI is used to verify identity and ensure that both parties are communicating with trusted

counterparts using digital certificates. However, if the PKI is compromised by a quantum attack, an attacker can gain access to operational and configuration data transmitted between operators, thereby obtaining sensitive information about the network structure, including the location of key network elements such as gNBs (5G base stations), UPF (User Plane Function) or AMF (Access and Mobility Management Function). This knowledge can then be used to plan targeted attacks, for example to take out critical network nodes using 'denial-of-service' (DoS) attacks or to bypass security by understanding the paths of data flows within the network.

5.3.3 Quantum Man-in-the-Middle (QMITM)

A Quantum Man-in-the-Middle (QMITM) attack is an advanced form of the classic Man-in-the-Middle attack, in which an attacker utilises the capabilities of quantum computers (CRQC) to intercept and modify communication between two parties in real time. The essence of the attack is that the attacker intercepts an encrypted message, immediately decrypts it, modifies its content, re-encrypts it and forwards it, whilst neither of the communicating parties realises that a change has occurred. In this way, not only confidentiality but, in particular, the integrity and authenticity of the communication are directly compromised.

Let us imagine a typical situation in which an attacker using a quantum computer with advanced methods (e.g. Shor's algorithm) intercepts communication within a 5G network. Thanks to the ability to efficiently factor keys or compute discrete logarithms, the attacker obtains the original encryption or signature keys without the user or server noticing. The attacker can then easily modify the message's content—for example, changing the amount or the destination account in a financial transaction—and forward the message, re-encrypted, to the recipient. Both communicating parties believe they are communicating securely, so the attacker's interference goes completely unnoticed.

Unlike a quantum decryption attack, which focuses primarily on breaching data confidentiality and does not interfere with the content of the data during transmission, a QMITM attack allows for direct, undetected manipulation of messages in real time. This capability represents a significant shift in the threats associated with the advent of quantum computing technologies and requires entirely new security measures.

5.3.4 Side-Channel Attacks

Side-channel attacks represent a specific type of security threat that does not directly concern the use of quantum computers, yet significantly threatens both current and post-quantum cryptography (PQC). The principle behind this attack is the exploitation of indirect information that a device inadvertently provides during its operation (response times, energy consumption, electromagnetic emissions or deviations in certain parameters). Through detailed analysis of this data, information about the encryption keys in use can be deduced without the attacker directly breaking the cipher itself. As post-quantum cryptographic protocols have not yet undergone extensive testing in real-world deployments, they may be even more vulnerable to such attacks.

The target of a side-channel attack could be, for example, a smartphone or an Internet of Things (IoT) device. Although these devices commonly use cryptographic methods to secure communications, their normal operation simultaneously generates a whole range of ancillary physical signals, such as minor deviations in power consumption or electromagnetic radiation, which attackers can analyse. In the future, there could even be specialised quantum algorithms that would more effectively detect and interpret these barely perceptible changes, thereby making side-channel attacks even easier. Such possibilities present a challenge for the development of secure cryptographic solutions that would be resilient not only to quantum threats but also to these indirect threats.

5.3.5 Efficient Key Recovery Attacks

This type of attack has proven to be an effective way of breaking the SIDH (Singular Isogeny Diffie-Hellman) cryptographic protocol, which was previously one of the candidates for ensuring secure post-quantum cryptography. The main essence of this type of attack lies in enabling the efficient reconstruction of the private key in SIDH, specifically in the SIKEp434 variant (Supersingular Isogeny Key Encapsulation), a key encapsulation method in SIDH that previously corresponded to security level 1 according to NIST. The attack was carried out on a standard processor in approximately 10 minutes. Even faster breaches were possible with the SIKEp182 and SIKEp217 variants (in 55 and 85 seconds respectively). These results suggest that all variants derived from the SIDH protocol are potentially vulnerable when used in modern cryptography. Given this threat and the successful cracking of SIDH/SIKE, this protocol was not included among the post-quantum cryptography standards according to NIST[44] . This is therefore not directly an attack using quantum computing resources, but rather an illustration of the risk faced by, and which will continue to be faced by, efforts to provide PQC protection against the types of attacks mentioned above.

[44] https://eprint.iacr.org/2022/975.pdf

5.4 Strengthening the resilience of cryptography against quantum attacks

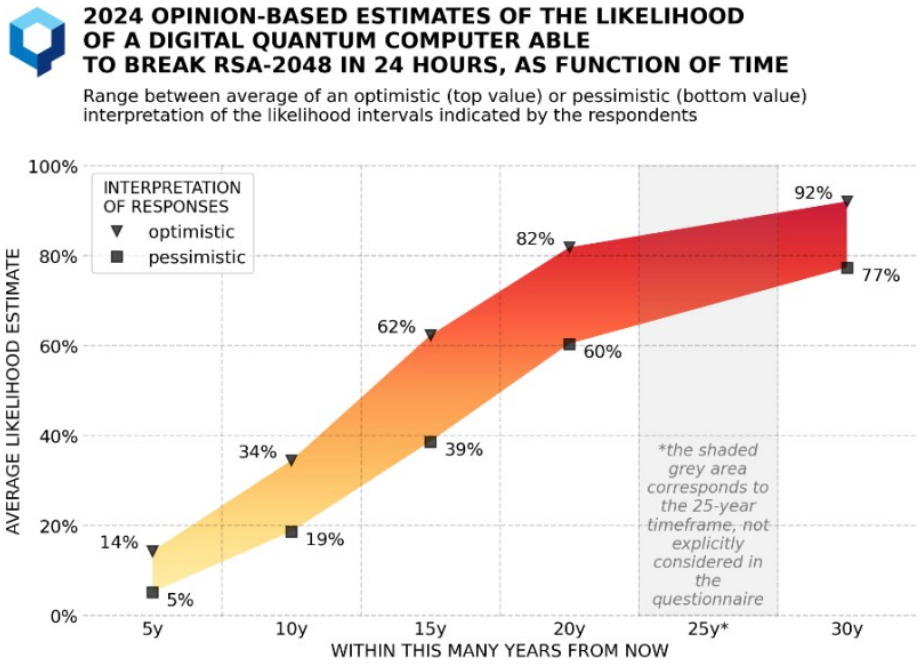
From the risks described above, particularly HNDL, where, with the significant reduction in the cost of storage capacity, some data is already being stored for later decryption, it is clear that the recommendation is to defend against future attacks today using known methods. In this context, one can apply an inequality commonly accepted within the professional community, which states that society should begin the transition to quantum-ready technologies before the sum of the time required for preparation (migration time) and the time required to preserve secrecy.

In addition to using post-quantum cryptography (for asymmetric cryptography) and doubling the key size in protocols (for symmetric cryptography), available technologies allow for the use of the concept of double encryption, whereby a single message is sequentially encrypted using one pre-quantum and one post-quantum cipher. This yields the benefits of both approaches. In the case of pre-quantum ciphers, this involves proven experience in their use, coupled with often years of attempts to break them. In the case of post-quantum ciphers, the benefits lie in their expected resistance to quantum cryptography.

As a further enhancement, keys can be generated using QKD and this key can also be used for additional encryption, i.e. triple encryption – using a pre-quantum cipher, a post-quantum cipher and a cipher with a key derived using quantum mechanical phenomena, QKD. However, the final step requires both communication nodes to be connected via quantum technologies (currently most commonly via optical cables), and would therefore involve more technologically demanding preparation.

The Global Risk Institute[45] (GRI) conducts an annual survey of experts in quantum technologies to gather estimates regarding the future development of quantum computing. For the year 2024, the 'Quantum Threat Timeline Report 2024'[46] is available which, among other things, estimates the likelihood of a quantum computer being developed that will be capable of breaking an RSA-2048 key within 24 hours (known as 'Q-Day'). From this data, it can be deduced that the currently estimated timeframe for a quantum computer to break current encryption algorithms is around 15 to 20 years, with the level of risk roughly doubling every 5 years. These estimates must be taken into account when planning the migration to quantum-ready technologies and drawing up the relevant timetable/roadmap by the relevant government bodies and regulators.

Figure 11: Chart – Quantum Threat Timeline Report 2024



[45] https://globalriskinstitute.org/

[46] https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

6 Regulation and standardisation

6.1 International initiatives

Successfully managing the transition to quantum-resistant security for telecommunications networks requires coordination at both the international level and the level of national regulations. At the international level, the standardisation organisations NIST, ETSI and ITU-T, as well as 3GPP, play a key role:

6.1.1 NIST (US National Institute of Standards and Technology)

It leads the aforementioned standardisation process for post-quantum cryptography. In July 2022, it announced the selection of algorithms and, in 2024, published draft FIPS federal standards for post-quantum key exchange and signatures. NIST also issues recommendations on when the transition should take place. For example, in May 2022, the White House issued National Security Memorandum 10, which sets out policies for quantum resilience: federal agencies must take stock of their cryptographic systems and plan for migration to PQC with the aim of mitigating quantum risks as much as possible by 2035. This date reflects expectations as to when CRQC might become available. The US therefore officially plans to be ready by the mid-2030s at the latest. NIST is working closely with the IETF (Internet Engineering Task Force) to incorporate PQC into protocols, and with industry to test implementations. The US NSA has also issued new guidelines (Suite 3) for national security systems, which envisage the deployment of approved PQC algorithms as soon as possible after their standardisation.

6.1.2 ETSI (European Telecommunications Standards Institute)

In Europe, standardisation of quantum-secure communication is primarily overseen by the CYBER Technical Committee, the QSC (Quantum-Safe Cryptography) Working Group, and a separate ISG (Industry Specification Group) for QKD. ETSI QSC focuses on the practical implementation of PQC: it publishes technical reports on the performance and suitability of PQC for various applications, on the combination of classical and post-quantum algorithms into hybrid schemes, on the impacts of quantum attacks on symmetric algorithms, and so on. In 2024, for example, QSC completed report TS 104 016 on a framework for migration to quantum-safe algorithms and an inventory of protocols requiring modification. In parallel, the ISG-QKD at ETSI is establishing common interfaces and requirements for quantum key distribution networks so that different QKD systems are interoperable and secure. For example, it defines standards for QRNGs (quantum random number generators), specifying what security proofs for QKD systems should look like, and for the integration of QKD into network architectures (the ETSI TS 104 014 standard addressing system interoperability). In doing so, ETSI supports the development of the European quantum communications ecosystem and ensures that new technologies can be integrated into existing infrastructure. Through the CEN/CENELEC organisations, Europe also coordinates the standardisation roadmap for quantum technologies in general. In 2025, ETSI published standard TS 104 015[47]for secure and efficient hybrid key exchange combining classical and post-quantum ciphers (the so-called Covercrypt scheme), which enables a smooth transition to post-quantum data protection, followed by further refining standardisation activities.

6.1.3 ITU-T (International Telecommunication Union, Standardisation Sector)

The ITU has established study groups focused on the security of quantum networks. For example, the ITU-T SG13 study group publishes the Y.3800 series of recommendations for QKD network architecture, and the SG17 study group, focused on security, has published the X.1710 framework for securing QKD networks. The ITU is therefore creating a global framework for quantum key distribution networks so that different implementations (from Europe, China, the US, etc.) can interoperate. This is important as there is a real risk of fragmentation in standards given the differing approaches of, for example, China or the US. The ITU is striving to facilitate consensus in this area, for example by publishing roadmap documents and overviews of technical solutions.

6.1.4 GSMA

In addition to these standardisation bodies, there are also industry associations specifically for the telecommunications sector. For example, the GSMA (an association of mobile operators) has established the Post Quantum Telco Network Task Force, which shares best practices among operators

[47] https://www.etsi.org/newsroom/press-releases/2513-etsi-launches-new-standard-for-quantum-safe-hybrid-key-exchanges-to-secure-future-post-quantum-encryption#:~:text=Today%2C%20ETSI%20announces%20the%20launch,sensitive%20data%20to%20decrypt%20them

and is developing uniform recommendations for the migration of telecommunications networks to PQC. Previously, 3GPP analysed the implications of quantum threats, with the 2019 3GPP TR 33.841 study in particular examining support for longer 256-bit keys in 5G as a possible immediate response to the quantum threat. In February 2025, 5G Americas (a regional association in the Americas) published a detailed white paper with recommendations, such as conducting an inventory of all cryptographic systems in networks, collaborating with suppliers on quantum migration, and introducing cryptographic agility into infrastructure. These recommendations are also relevant globally.

7 Quantum activities of the EU and the Czech Republic

Since 2018, the European Union has been implementing the ambitious Quantum Flagship initiative[48], which has a total budget of one billion euros spread over a ten-year period. This programme supports the development of four key areas of quantum technologies: quantum computing, quantum communication, quantum metrology and sensing, and quantum simulation. To this must be added further billions of euros included in the national programmes of European Member States, such as Germany, the Netherlands, Denmark, Finland, as well as Poland, Hungary and the Balkan states.

7.1 EU quantum computing technologies and their costs

Estimating the cost of quantum computers is highly problematic; the available data is minimal and may be misleading. The most advanced players (Google, IBM, Microsoft, Rigetti, etc.) do not offer quantum computers for sale and do not currently plan to do so. The computers they have developed are housed within corporate supercomputing centres and made available via cloud computing solutions in the form of machine time rentals.

Prices for computing time on quantum computers can therefore only be estimated; larger contracts requiring significant amounts of computing time are confidential and protected by non-disclosure agreements. However, 'renting computing time' is also an imprecise term, as the computational operation constitutes the entire project: the rental of the actual computing time on a quantum computer and the services of the experts operating the equipment. The client specifies the task, a team of (hired) experts converts the task into a quantum algorithm, optimises it for a specific quantum device, performs the computation (enters operations into the system and takes measurements) and interprets the results.

A rough estimate of the potential cost of quantum computers is provided by several quantum computer purchases within the EuroHPC Joint Undertaking (JU), which are described in more detail below. However, these figures have limited informative value, as they cannot be regarded as commercial purchases, but rather as scientific collaboration agreements under which quantum computer manufacturers design, supply and assemble a quantum computer at an HPC centre. Such a supply also carries significant prestige for the quantum computer manufacturer. These suppliers do not share any information regarding the sale of quantum computers outside the EuroHPC programme and show no willingness to disclose their pricing policy.

Six sites have been selected across the EU to host quantum computers, which will operate within the EuroHPC Joint Undertaking project. The total investment exceeds €100 million, with half funded by the European Commission and the other half by individual Member States or consortia. Each of the quantum facilities is to be integrated into existing supercomputing infrastructure, with the aim of creating a European hybrid ecosystem capable of performing quantum-classical computations. One of the objectives of the entire initiative was the deployment and subsequent testing of diverse quantum technology platforms, ranging from ion traps and superconducting qubits to photonic technologies.

The Czech Republic has joined the European quantum development effort through the LUMI-Q project, which will be implemented in Ostrava at the IT4Innovations National Supercomputing Centre. The VLQ49 quantum computer with 24 qubits from IQM Quantum Computers will be connected here to the existing Karolina supercomputer. The total investment amounts to approximately €5 million, with half of the funds coming from the European budget (EuroHPC JU) and the other half covered by a consortium of nine Member States.

As part of the EuroHPC JU, Poland is acquiring a 20-qubit Piast-Q quantum computer[50] for €12.3 million from AQT. Furthermore, through Creotech Instruments, it is implementing a project to develop a quantum computer capable of scaling up to 1,000 qubits by 2029[51] . The first phase of the project, which aims to develop a 100-qubit system, is fully funded by the European Quantum Flagship programme and has a budget of between €18 and €20 million. The project involves hardware development, quantum operation control and integration with classical computing systems.

[48] https://qt.eu/about-quantum-flagship/

[49] https://www.it4i.cz/en/infrastructure/vlq-quantum-computer

[50]https://www.datacenterdynamics.com/en/news/aqt-to-deliver-rack-based-piast-q-quantum-computer-to-psnc/

[51]https://creotech.pl/news/creotech-instruments-has-signed-an-executive-agreement-with-the-european-commission/

Germany is one of Europe's leading nations in the field of quantum technologies. In 2020, the federal government announced a plan for direct public investment of €2 billion aimed at creating a quantum ecosystem and supporting research and industrial applications. Several flagship projects have been funded from these resources. For example, the Euro-Q-Exa[52]quantum computer, which is being developed within the EuroHPC JU by IQM in collaboration with LRZ and the Fraunhofer-Gesellschaft, received direct funding of €25 million. This comprises two systems, one of which will operate with 54 qubits and the other with 150 qubits. In 2024, IBM opened Europe's first Quantum Data Centre in Ehningen near Stuttgart, designed to operate commercial quantum computers on European soil. IBM and its partners invested approximately €290 million in the construction and operation of the centre.

As part of the Quantum Spain strategy, Spain unveiled the country's first quantum computer in 2025, developed exclusively using European technologies and integrated into the MareNostrum 5 supercomputer[53] . This computer is the result of collaboration between the start-up Qilimanjaro Quantum Tech and the GMV group. As part of the EuroHPC JU project, a contract was signed in early 2025 for the MareNostrum-Ona project, a quantum computer that will also be located at BSC-CNS. This project, with a total budget of €8.5 million, will be Europe's first quantum annealing computer, which will be particularly useful for solving optimisation problems and aims to complement the existing quantum technologies available to European researchers.

As part of the EuroHPC JU project, France expects a 12-qubit quantum computer, Lucy[(54),]from the companies Quandela and attocube by the end of 2025[55]. The total budget for this project is €8.5 million.

Estimates of QC costs can also be derived from available data on the collaboration between the aforementioned Finnish quantum computer manufacturer IQM and VTT Technical Research Centre of Finland. As part of this collaboration, three quantum computers (5-qubit, 20-qubit and 50-qubit) have been built, which are also made available for commercial use; a budget of over €20 million for these computers was provided by the Finnish government. By 2027, the plan is to have 300 qubits available with the aim of strengthening research in the field of materials modelling. VTT has secured a special government grant of €70 million for this purpose. IQM offers quantum computing time on its facilities via its IQM Resonance product on a pay-as-you-go basis at $0.30 per second, which, whilst providing some indication of the cost of this form of quantum computing, is clearly dependent on the type and complexity of the task required.

7.2 Quantum activities in the Czech Republic

At the European level, the creation of infrastructure for quantum-secure communication is being carried out under the auspices of the EuroQCI project[56]. The first phase involves the creation of a national quantum testbed. In the case of the Czech Republic, this is being provided by the CZQCI project[57], with similar projects also being implemented in other European countries. In the subsequent phase, these national infrastructures should then be interconnected. Technologically, this mainly involves optical-based interconnection using optical fibres and satellite communications.

The CZQCI project itself is focused on building a test version of a national backbone quantum communication infrastructure that will connect Prague, Brno and Ostrava. The aim is to validate technologies for quantum-secure communication and prepare the Czech Republic for integration into the European EuroQCI infrastructure planned for 2030. The project includes educational programmes for the general public and experts, opportunities for public sector and industry partners to test quantum communication, and a specialised laboratory for research and teaching.

[52]https://eurohpc-ju.europa.eu/signature-procurement-contract-eurohpc-quantum-computer-located-germany-2024-10-15_en

[53]https://quantumspain-project.es/en/quantum-spain-presents-the-first-quantum-computer-in-spain-developed-with-100-european-technology/

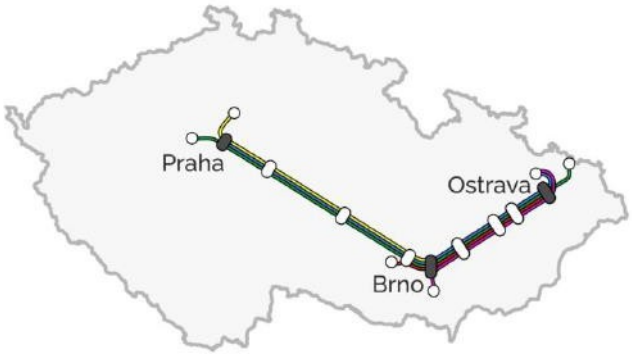
[54]https://www.quandela.com/qpus/lucy/

[55]https://quantumzeitgeist.com/european-researchers-gain-remote-access-to-cutting-edge-12-qubit-quantum-computer-via-euroqcs-france-initiative/

[56]https://digital-strategy.ec.europa.eu/cs/policies/european-quantum-communication-infrastructure-euroqci

[57]https://www.cybersecurityhub.cz/strategicke-projekty/czqci

Figure 12: Visualisation of the test quantum infrastructure in the Czech Republic



Through the CZQCI project, Czech partners will gain experience in the deployment and operation of a quantum network, enabling them to better assess the possibilities for its practical application, particularly in the fields of cybersecurity and telecommunications. The project will also support international cooperation and the exchange of experience within the European area, whilst raising awareness of quantum technologies among both the professional and general public.

The CZQCI project is coordinated by CyberSecurity Hub, z.ú. and is being carried out by a consortium comprising:

- The Czech Technical University in Prague,
- CESNET z.s.p.o.,
- Masaryk University,
- the Institute of Scientific Instruments of the Czech Academy of Sciences,
- Palacký University in Olomouc,
- VŠB – Technical University of Ostrava,
- Brno University of Technology.

The National Initiative for Quantum Technologies (NIKT[58]) has existed in the Czech Republic since 2016 and was established in connection with the EU Quantum Flagship initiative. The aim of this initiative is to promote and support the development of quantum technologies. Its members include the Faculty of Mathematics and Physics at Charles University, the Faculty of Science at Palacký University Olomouc, the Faculty of Nuclear and Physical Engineering at the Czech Technical University in Prague, the Faculty of Informatics at Masaryk University, the Institute of Instrumentation of the Czech Academy of Sciences, the Central European Institute of Technology at Masaryk University, and Cybersecurity Hub z.ú.

In the field of quantum computing, a 24-qubit quantum computer is set to be launched at the IT4Innovations national supercomputing centre at VŠB – Technical University of Ostrava (see previous chapter).

The Czech Republic has also joined the European quantum communication infrastructure project EuroQCI through the CZQCI project (see previous chapter). This project is coordinated by Cybersecurity Hub, z.ú., which is currently also preparing a consultancy service in the field of quantum technologies.

Czech institutions that provide practical access to quantum technologies include:

- CTU: it is possible to utilise the collaboration between IBM and CTU, which enables access to processing time on a quantum computer, with CTU also coordinating the allocation of processing time. Furthermore, it provides a laboratory with equipment for quantum key distribution (QKD) and organises developer meetings and training in the field of quantum technologies from secondary school age onwards[59] . CTU also collaborates with research and commercial partners on the European photonic quantum computer project (Epique), which is funded by the EU. IT4Innovations at VŠB Ostrava will facilitate access to the LUMI-Q quantum computer.
- The CZQCI project provides training courses in quantum communication technologies and enables physical connections for public institutions and the commercial sector to test their readiness for quantum communication.

[58] https://nikt.cz/

[59] https://qworld.net/

- The Institute of Instrumentation of the Czech Academy of Sciences (ÚPT AV ČR) is involved in a number of research projects within consortia, such as the in-house development of quantum ion clocks and the implementation and expansion of a network of coherent transmission links for the distribution of precise time derived from these clocks.
- The QEENTEC[60] project coordinated by ÚPT AV ČR and carried out by the Institute of Photonics and Electronics, the Jaroslav Heyrovský Institute of Physical Chemistry, Palacký University in Olomouc and CESNET, focuses on the development of hybrid quantum gates for quantum computers.
- The QM4ST[61] project led by the University of West Bohemia in Plzeň and bringing together Charles University, the Czech Technical University in Prague and the Brno University of Technology, focuses on the study of materials exhibiting entirely new properties explainable by quantum physics, such as spintronics, superconductivity, photocatalysis, electrolysis, fuel cells and photonics.

A national quantum strategy is currently being prepared, which should provide a strategic framework for state support for education and industry in quantum technologies.

[60] https://www.jh-inst.cas.cz/grant/quantum-engineering-and-nanotechnology-queentec

[61] https://qm4st.zcu.cz/cs/

8 Conclusion

Quantum technologies represent a fundamental shift in computing, communications and security. The deployment of quantum computers will enable the solving of complex scientific problems and practical simulations, but at the same time will pose a security risk to current encryption methods. Examples of areas that will undoubtedly be impacted by the development of quantum computing include the design of materials with specific properties, batteries, chemical compounds, medicines, logistics, machine learning – AI, cryptography and the security of communication networks in general.

Development is rapid, but the practical use of quantum computers and quantum communication in everyday operations requires overcoming technological and infrastructural barriers. We are still in a very early phase of QC utilisation; all available devices are as yet experimental, and although some may offer commercial access, it is a highly complex and costly process. Investment in QC research is therefore being made not only by the world's largest players but also by individual states, either alone or in collaboration – in the EU, this takes the form of the Quantum Flagship initiative and specific quantum computer construction projects such as the EuroHPC Joint Undertaking and EuroQCI. The Czech Republic is actively involved in European development through both research capacity and funding.

Since quantum computers can effectively solve specific sub-tasks that are unsolvable for standard systems within a reasonable timeframe, the most viable approach currently appears to be the combined use of standard computing systems alongside quantum ones. In practice, complex tasks solved by classical computing systems will be able to trigger a specific sub-task in the cloud, solved by a quantum computer.

In the foreseeable future, quantum computers will be capable of breaking current cryptographic protocols (particularly RSA and ECC), which are used in 5G networks for authentication and key exchange, thereby compromising the overall security of digital communications. To ensure security in the era of quantum computers, it is therefore necessary to combine post-quantum cryptography, quantum key distribution and the modernisation of communications infrastructure. These steps to protect data must be taken early enough to pre-empt the development of quantum computers themselves, as threats already exist today that will manifest later, once quantum computers become available to potential attackers. To this end, the standardisation of new encryption algorithms (NIST, ETSI) is being pursued at the international level, but further steps will also need to be taken at the national level.

Investment in post-quantum cryptography, active support for standardisation, and capacity-building in the field of quantum security are key steps that should be taken by both public institutions and the private sector.

Beyond the scope of the new Cyber Security Act (nZKB-NIS2, currently in the approval process), the following steps can be recommended, which would help state institutions and regulators ensure the transition to a quantum-secure infrastructure:

a) Formulate minimum (binding) methodological rules for operators to ensure the cybersecurity of 5G and other communication networks in the context of the advent of quantum computing, which would include:
    - A timeline and method (roadmap) for the introduction of advanced encryption standards (PQC or hybrid), prepared for future quantum decryption, including steps for a multi-phase migration.
    - Minimum technical requirements for audit/detection/monitoring systems
    - A uniform procedure for security audits of system suppliers
    - Rules for the protection of internal data and (security) requirements for staff

b) Create a reference register of PQC-compatible devices

c) Establish minimum requirements for interoperability between classical and QKD cryptography