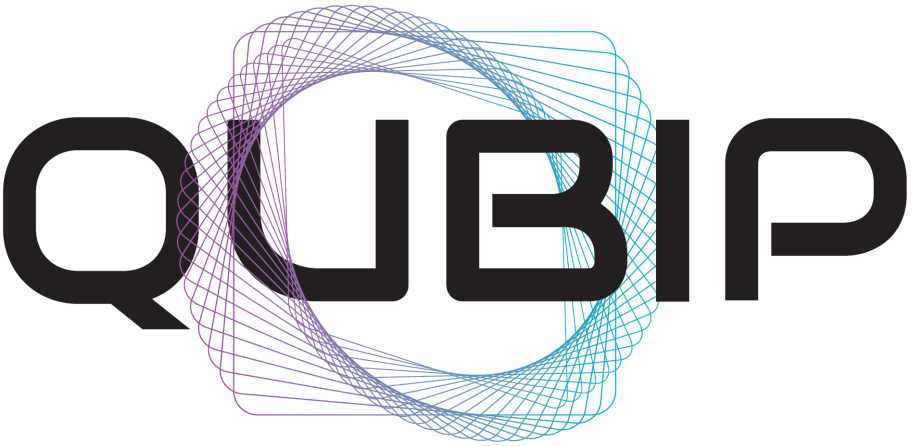
Horizon Europe



QUANTUM-ORIENTED UPDATE TO BROWSERS AND INFRASTRUCTURES FOR THE PQ TRANSITION (QUBIP)

Expected capabilities of Quantum Computers

Deliverable number: D1.1

Version 1.0

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Project Acronym:	QUBIP
Project Full Title:	Quantum-oriented Update to Browsers and Infrastructures for the PQ transition
Call:	HORIZON-CL3-2022-CS-01
Topic:	HORIZON-CL3-2022-CS-01-03
Type of Action:	HORIZON-IA
Grant Number:	101119746
Project URL:	https://www.qubip.eu
Start date:	1 September 2023
Duration:	36 months

Editors:	Bartolomeo Montrucchio	– POLITO
Deliverable nature:	Report (R)	
Dissemination level:	Public (PU)	
Contractual Delivery Date:	31 August 2024	
Actual Delivery Date	22 July 2024	
Number of pages:	25	
Keywords:	quantum computers, quantum computing, quantum algorithms	
Contributors:	Marco Russo Antonio Pastor	– POLITO – TID
Peer review:	Piedad Brox Dmitry Belyavskiy Hubert Kario	– CSIC – REDHAT – REDHAT
Approved by:	ALL partners	

Table 1: Document revision history

Issue Date	Version	Comments
13/05/2024	0.1	Initial table of contents
03/07/2024	0.2	First draft version for internal review
22/07/2024	1.0	Final version for submission

Abstract

This document presents Deliverable D1.1 of the Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition (QUBIP) project. It provides a comprehensive overview of the capabilities of quantum computing and the necessity for transitioning from classical to quantum paradigms. The document explores various quantum computing technologies, including superconducting qubits, photonic qubits, neutral atoms and trapped ions, detailing their unique attributes and challenges. It reviews significant quantum algorithms such as Grover's algorithm and Shor's algorithm, emphasizing their implications for cryptanalysis. The feasibility of Shor's algorithm and its potential to break widely used cryptographic systems are assessed, along with the impact of quantum computing on lattice-based cryptography. The deliverable concludes by discussing the broader implications of quantum computing for industry and the urgency of preparing for the Post-Quantum (PQ) transition.

Contents

1 Introduction **9**

2 Quantum Computing Technologies **10**
2.1 Introduction . . . 10
2.2 Superconducting Qubits . . . 10
2.2.1 Advantages of Superconducting Qubits . . . 10
2.2.2 Disadvantages of Superconducting Qubits . . . 11
2.3 Photonic Qubits . . . 11
2.3.1 Advantages of Photonic Qubits . . . 11
2.3.2 Disadvantages of Photonic Qubits . . . 12
2.4 Trapped Ions and Neutral Atoms . . . 12
2.4.1 Advantages of Trapped Ions and Neutral Atoms . . . 12
2.4.2 Disadvantages of Trapped Ions and Neutral Atoms . . . 12
2.5 Non-Universal Quantum Computing . . . 13
2.5.1 Quantum Annealing . . . 13

3 Review of the Main Quantum Algorithms **15**
3.1 Introduction . . . 15
3.2 Grover's Algorithm . . . 15
3.2.1 Algorithm Steps . . . 15
3.2.2 Quantum Circuit Representation . . . 16
3.2.3 Conclusion . . . 16
3.3 Shor's Algorithm . . . 16
3.3.1 Algorithm Steps . . . 16
3.3.2 Example . . . 17
3.3.3 Computational Complexity . . . 18
3.3.4 Conclusion . . . 18

4 Applications of Quantum Computing to Cryptanalysis **19**
4.1 Introduction . . . 19
4.2 Current Feasibility of Shor's Algorithm . . . 19
4.3 Breaking Lattice Cryptography . . . 20

5 Quantum Computing Impact in the Security of Communication Protocols **21**
5.1 Impact of Quantum Computing Algorithms . . . 21
5.2 Impact in Protocols . . . 22

6 Conclusions **24**

List of Figures

2.1 Energy diagram changes over time as the quantum annealing process runs, and a bias is applied. 13

3.1 Quantum circuit for Grover's algorithm. 16
3.2 Quantum circuit for Shor's algorithm. 17

List of Tables

1 Document revision history 4

List of Acronyms

CNF	Cloud-native Network Functions
CPE	Customer Premise Equipment
CRQC	Cryptographically Relevant Quantum Computer
DSA	Digital Signature Algorithm
EAP	Extensible Authentication Protocol
ECC	Elliptic-Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme
GapSVP	Decisional Shortest Vector Problem
GNFS	General Number Field Sieve
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IPsec	IP Security
LWE	Learning With Errors
NFV	Network Functions Virtualization
NIST	National Institute of Standards and Technology
OAM	Operations, Administration, and Maintenance
OSS	Operations Support Systems
OWE	Opportunistic Wireless Encryption
POP3	Post Office Protocol version 3
PQ	Post-Quantum
PQC	Post-Quantum Cryptography
PSK	Pre-Shared Keys
QA	Quantum Annealing
QC	Quantum Computer
QFT	Quantum Fourier Transform
QKD	Quantum Key Distribution
QPU	Quantum Processing Unit
QUBIP	Quantum-oriented Update to Browsers and Infrastructures for the Post-quantum transition
RSA	Rivest–Shamir–Adleman
SAE	Simultaneous Authentication of Equals
SBA	Service Based Architecture
SDN	Software-Defined Networking
SD-WAN	Software-Defined Wide Area Network
SIM	Subscriber Identity Module
SIVP	Shortest Independent Vector Problem
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell protocol
SUCI	SUbscription Concealed Identifier
SUPI	SUbscription Permanent Identifier
TLS	Transport Layer Security
VPN	Virtual Private Network
WPA3	Wi-Fi Protected Access 3

1 Introduction

This deliverable aims to provide a comprehensive overview of what quantum computing can achieve and why a transition from classical to quantum paradigms is required.

Chapter 2 delves into various quantum computing technologies, exploring the mechanics and potential of superconducting qubits, photonic qubits, trapped ions and neutral atoms, and other emerging technologies. Each section will detail the unique attributes and challenges associated with these technologies, providing insight into the current state and future prospects of quantum hardware.

Chapter 3 reviews the main quantum algorithms that exemplify the power of quantum computation. Grover's algorithm, known for its ability to speed up database searches, and Shor's algorithm, famous for its capability to factor large integers exponentially faster than the best-known classical algorithms, are examined in detail.

Chapter 4 focuses on the applications of quantum computing to cryptanalysis, a critical area that underscores the urgency of transitioning to quantum-resistant cryptographic methods. We assess the current feasibility of implementing Shor's algorithm and its implications for breaking widely used cryptographic systems. Furthermore, we explore the potential of Quantum Computers (QCs) to challenge lattice-based cryptography, which is considered one of the most promising PQ cryptographic schemes.

Finally, in Chapter 5 we present some applications and the expected impact that quantum computing technologies have on the communication industry.

Through this deliverable, we aim to elucidate the transformative capabilities of QCs and highlight the necessity of preparing for the imminent transition to Post-Quantum Cryptography (PQC).

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2 Quantum Computing Technologies

2.1 Introduction

Quantum computing technologies are at the forefront of scientific research and development, offering unprecedented computational capabilities. This chapter delves into the primary technologies driving quantum computing forward. We explore superconducting qubits, photonic qubits, trapped ions, and neutral atoms, each with their unique advantages and challenges. By examining these technologies, we aim to provide a comprehensive understanding of the current state and future potential of quantum hardware.

2.2 Superconducting Qubits

Superconducting qubits are a leading technology in the field of quantum computing, utilizing the principles of superconductivity to create quantum bits, or qubits. These qubits are typically made from superconducting materials such as niobium or aluminum, which, when cooled to near absolute zero, exhibit zero electrical resistance (superconductivity).

There are several types of superconducting qubits, including charge qubits, flux qubits, and phase qubits. Each type manipulates different quantum properties to encode information. For instance, charge qubits use the presence or absence of Cooper pairs (pairs of electrons) on a superconducting island to represent the qubit states, whereas flux qubits use the direction of the circulating supercurrent. Phase qubits, on the other hand, leverage the phase difference of the superconducting wave function across a Josephson junction.

One of the key advantages of superconducting qubits is their scalability. They can be fabricated using standard lithographic techniques and integrated into complex circuits. Furthermore, they can be coupled to each other using microwave photons, allowing for the creation of entangled states necessary for quantum computation. Superconducting qubits also benefit from relatively fast gate times, which are essential for executing quantum algorithms efficiently.

However, superconducting qubits also face challenges, such as maintaining coherence times long enough to perform computations and minimizing errors due to environmental noise. Researchers are actively developing techniques such as error correction codes and improving qubit design to address these issues. Moreover, the need for extremely low temperatures (millikelvin range) requires sophisticated cryogenic systems, which adds complexity and cost to the overall setup.

2.2.1 Advantages of Superconducting Qubits

- **Scalability:** Superconducting qubits can be fabricated using well-established lithographic techniques, allowing for the integration of many qubits into a single chip.
- **Fast Gate Times:** They offer relatively fast operation speeds (order of tens of nanoseconds), which are beneficial for running quantum algorithms efficiently.
- **Strong Coupling:** The ability to couple qubits strongly through microwave photons enables effective entanglement and interaction between qubits, crucial for complex quantum operations.
- **Mature Fabrication Techniques:** Leveraging existing semiconductor fabrication technologies aids in the rapid development and scaling of superconducting qubit systems.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2.2.2 Disadvantages of Superconducting Qubits

- **Short Coherence Times:** The coherence times of superconducting qubits are limited, which can lead to errors during quantum computations.
- **Environmental Sensitivity:** They are susceptible to noise from the environment, necessitating advanced error correction methods.
- **Cryogenic Requirements:** The need for operation at millikelvin temperatures demands complex and expensive cryogenic systems.
- **Material Defects:** Variations and defects in the superconducting materials can impact the performance and reliability of the qubits.

In summary, superconducting qubits represent a promising and rapidly advancing area of quantum computing technology, with significant potential applications ranging from solving complex computational problems to advancing our understanding of quantum mechanics. Continuous research and development are focused on overcoming the existing challenges to fully harness their capabilities. The currently most powerful superconducting QC is IBM Condor, with 1121 qubits, due in 2025 [1].

2.3 Photonic Qubits

Photonic qubits utilize photons, the fundamental particles of light, as the carriers of quantum information. These qubits are advantageous because photons can travel long distances with minimal loss and are less susceptible to decoherence from their environment. Photonic qubits are typically encoded using properties such as polarization, time-bin, or spatial modes of the photons.

One of the primary benefits of photonic qubits is their compatibility with existing optical communication infrastructure. This allows for potential integration with current fiber optic networks, facilitating long-distance quantum communication. Additionally, photonics-based systems often operate at room temperature, eliminating the need for complex cryogenic cooling.

Photonic qubits can be generated using sources like spontaneous parametric down-conversion or quantum dots, and can be manipulated with devices such as beam splitters, phase shifters, and waveguides. Detection of photonic qubits is achieved using highly sensitive photodetectors.

However, there are challenges associated with photonic qubits. Efficient single-photon sources and detectors are still an area of active research, and losses in optical components can impact the fidelity of quantum operations. Furthermore, integrating photonic qubits into scalable quantum circuits remains a significant technical hurdle.

2.3.1 Advantages of Photonic Qubits

- **Low Decoherence:** Photons are less susceptible to environmental noise, resulting in longer coherence times.
- **Room Temperature Operation:** Photonic systems can operate without the need for cryogenic cooling.
- **Integration with Optical Networks:** Compatibility with existing fiber optic infrastructure enables long-distance quantum communication.
- **High Speed:** Photons can travel at the speed of light, facilitating fast information transfer. Gates are in the order of picoseconds to nanoseconds.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

2.3.2 Disadvantages of Photonic Qubits

- **Photon Loss:** Losses in optical components and fibers can degrade qubit fidelity.
- **Single-Photon Sources and Detectors:** Efficient generation and detection of single photons are challenging and require further development.
- **Scalability:** Integrating a large number of photonic qubits into scalable quantum circuits is technically demanding.

The currently most powerful photonic QC is Xanadu Borealis, with 216 qubits (2022) [2].

2.4 Trapped Ions and Neutral Atoms

Trapped ions and neutral atoms are another promising approach to building QCs, leveraging individual atoms or ions as qubits. These systems utilize electromagnetic fields to trap and manipulate the particles, with quantum information encoded in the internal states of the atoms or ions.

Trapped ion qubits are typically confined using radiofrequency or optical fields in ion traps. They offer extremely long coherence times and high-fidelity quantum operations. Quantum gates are performed using laser pulses to induce interactions between the ions. Similarly, neutral atoms are trapped in optical lattices or tweezers, and manipulated using laser light.

One of the main advantages of these systems is the high degree of control over individual qubits, allowing for precise quantum operations. Additionally, trapped ions and neutral atoms can achieve high-fidelity measurements and entanglement, crucial for quantum computation and error correction.

However, these systems face challenges such as the complexity of trapping and cooling the particles, and the scalability of the setups. Trapping and controlling a large number of ions or atoms in a stable manner is technically demanding. Furthermore, the requirement for sophisticated laser systems and vacuum chambers adds to the complexity and cost.

2.4.1 Advantages of Trapped Ions and Neutral Atoms

- **Long Coherence Times:** Trapped ions and neutral atoms exhibit long coherence times, reducing decoherence effects.
- **High-Fidelity Operations:** They enable high-fidelity quantum gates and measurements, essential for accurate quantum computation.
- **Precise Control:** Advanced trapping and manipulation techniques allow for precise control of individual qubits.
- **Strong Interaction:** The strong interaction between trapped ions or neutral atoms facilitates efficient entanglement and quantum operations.

2.4.2 Disadvantages of Trapped Ions and Neutral Atoms

- **Complex Setup:** Trapping and cooling systems are complex and require precise engineering.
- **Scalability:** Scaling up the number of qubits while maintaining stability and control is challenging.
- **Expensive Infrastructure:** The need for advanced laser systems, vacuum chambers, and cooling technologies increases the overall cost.
- **Slower Gates:** The gate durations are currently in the order of microseconds.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

In summary, both photonics qubits and trapped ions or neutral atoms offer unique advantages and face specific challenges. Continuous advancements in these technologies are essential for realizing practical and scalable QCs. The currently most powerful neutral atoms QC is Quera Aquila, 256 qubits (2023) [3], whereas the trapped ions one is IONQ Forte, 36 qubits (2022) [4].

2.5 Non-Universal Quantum Computing

Universal QCs, such as those based on the gate model, can theoretically perform any computation that a classical computer can, and more, given enough time and resources. In contrast, non-universal quantum computing models are specialized and cannot efficiently simulate any arbitrary quantum algorithm. These models are designed to solve specific types of problems more efficiently than classical algorithms, rather than providing a general-purpose quantum computational framework. For instance, they may lack the full set of operations needed to perform arbitrary quantum computations but can still be extremely powerful for certain tasks. One notable example of a non-universal quantum computing approach is Quantum Annealing (QA), which focuses on solving optimization problems by exploiting quantum fluctuations.

2.5.1 Quantum Annealing

QA is a general method to find the global minimum of a given function in a set of candidates. The class of algorithmic methods for QA is a promising metaheuristic tool for solving local search problems in multivariable optimization contexts. These problems usually consist in finding the maximum or minimum for a cost function that comprises several independent variables and a large number of instances [5]. The evaluation of cost in this context must necessarily be computed in probabilistic terms.

A single configuration is defined as a ‘tuple’ of values over the whole set of independent variables. The value of the cost function depends on the configurations, being the solution to the problem set as the definite optimal configuration which minimizes, or maximizes, the cost function with some arbitrarily chosen confidence level or probability.

2.5.1.1 Implementation

To detail this architecture, it is useful to start with the qubits that are the lowest energy states of the superconducting loops that make up the D-Wave Quantum Processing Unit (QPU). These states have a circulating current and a corresponding magnetic field. At the end of the QA process, each qubit collapses from a superposition state into either 0 or 1 (a classical state). A qubit’s state is implemented in a circulating current with a corresponding magnetic field [6].

The physics of this process can be shown (visualized) with an energy diagram, as in Figure 2.1.

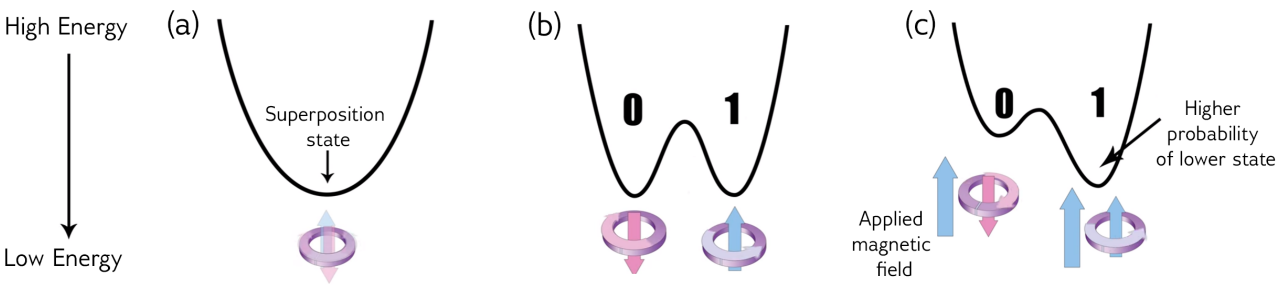


Figure 2.1: Energy diagram changes over time as the quantum annealing process runs, and a bias is applied.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

This diagram changes over time: to begin, there is just one valley (a), with a single minimum. The QA process runs, the barrier is raised, and this turns the energy diagram into what is known as a double-well potential (b). Here, the low point of the left valley corresponds to the 0 state, and the low point of the right valley corresponds to the 1 state. The qubit ends up in one of these valleys at the end of the anneal.

Everything else being equal, the probability of the qubit ending in the 0 or the 1 state is equal (50 percent). You can, however, control the probability of it falling into the 0 or the 1 state by applying an external magnetic field to the qubit (c). This field tilts the double-well potential, increasing the probability of the qubit ending up in the lower well. The programmable quantity that controls the external magnetic field is called a bias, and the qubit minimizes its energy in the presence of the bias.

The bias term alone is not useful, however. The real power of the qubits comes when you link them together so they can influence each other. This is done with a device called a coupler. A coupler can make two qubits tend to end up in the same state — both 0 or both 1 — or it can make them tend to be in opposite states. Like a qubit bias, the correlation weights between coupled qubits can be programmed by setting a coupling strength. Together, the programmable biases and weights are the means by which a problem is defined in the D-Wave QC.

As stated, each qubit has a bias and qubits interact via the couplers. When formulating a problem, users choose values for the biases and couplers. The biases and couplings define an energy landscape, and the D-Wave QC finds the minimum energy of that landscape: this is QA.

The currently most powerful QA computer is D-Wave Advantage [7], with 5000 qubits.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

3 Review of the Main Quantum Algorithms

3.1 Introduction

Quantum algorithms are the key to unlocking the true potential of QCs. In this chapter, we review the main quantum algorithms that demonstrate the power of quantum computation. Grover's algorithm, renowned for its ability to accelerate database searches, and Shor's algorithm, famous for its capability to factor large integers exponentially faster than classical algorithms, are discussed in detail. These algorithms exemplify the transformative impact quantum computing can have on various fields.

3.2 Grover's Algorithm

Grover's algorithm [8] is a quantum algorithm that provides a quadratic speedup for unstructured search problems. It was discovered by Lov Grover in 1996 and is one of the fundamental algorithms in quantum computing. The algorithm can search through an unsorted database of N entries in $O(\sqrt{N})$ time, compared to $O(N)$ time required by classical algorithms.
Given a function $f : \{0,1\}^n \to \{0,1\}$, where $f(x) = 1$ for exactly one unknown $x = x_0$ and $f(x) = 0$ for all other x, Grover's algorithm aims to find x_0.

3.2.1 Algorithm Steps

The algorithm consists of the following steps:

1. **Initialization:** Start with an equal superposition of all possible states. This is achieved by applying the Hadamard gate to each qubit in the $|0\rangle^{\otimes n}$ state:

$$|\psi_0\rangle = H^{\otimes n}|0\rangle^{\otimes n} = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle$$

   where $N = 2^n$.

2. **Oracle Query:** Apply the oracle U_ω that marks the correct state x_0:

$$U_\omega|x\rangle = \begin{cases} -|x\rangle & \text{if } x = x_0 \\ |x\rangle & \text{if } x \neq x_0 \end{cases}$$

3. **Amplitude Amplification:** Perform the Grover diffusion operator D to amplify the amplitude of the correct state:

$$D = 2|\psi_0\rangle\langle\psi_0| - I$$

4. **Iteration:** Repeat the Oracle Query and Amplitude Amplification steps approximately $\frac{\pi}{4}\sqrt{N}$ times.
5. **Measurement:** Measure the quantum state. The measurement will yield the correct state x_0 with high probability.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

3.2.2 Quantum Circuit Representation

The quantum circuit for Grover's algorithm can be represented as in Figure 3.1.

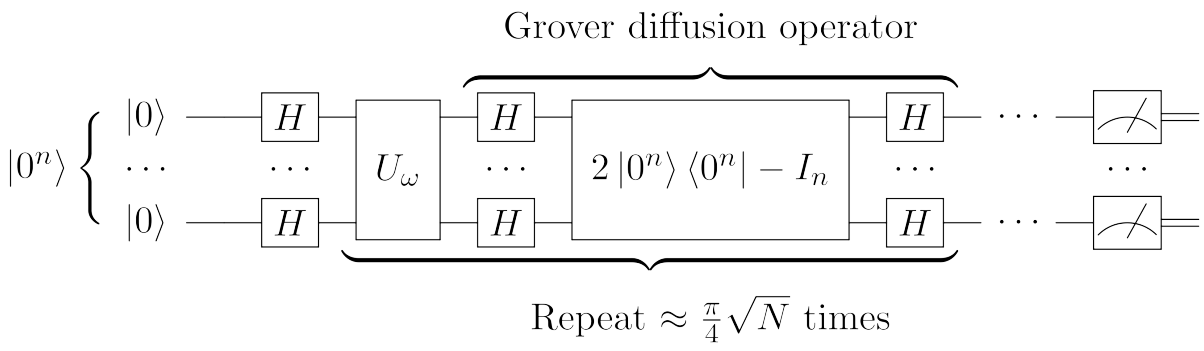


Figure 3.1: Quantum circuit for Grover's algorithm.

In that circuit, the initial Hadamard gates create the superposition state. The oracle U_ω is applied, followed by the Grover diffusion operator, which includes Hadamard gates, phase shift Z gates, and more Hadamard gates. This process is repeated the required number of times.

3.2.3 Conclusion

Grover's algorithm provides a significant speedup for search problems, showcasing the power of quantum computing. While it offers a quadratic improvement over classical methods, it still requires an exponentially large number of qubits for large N, posing practical implementation challenges.

3.3 Shor's Algorithm

Shor's algorithm, proposed by Peter W. Shor in 1994 [9, 10], is a quantum algorithm for integer factorization. It provides an exponential speedup over the best-known classical algorithms, making it significant for cryptography, particularly for breaking widely-used public-key cryptosystems such as RSA.
The problem addressed by Shor's algorithm is to factorize a composite integer N into its prime factors. Specifically, given an integer N, the goal is to find its prime factors p and q such that $N = pq$.

3.3.1 Algorithm Steps

Shor's algorithm can be broken down into the following main steps:

3.3.1.1 Step 1: Choose a Random Number

Choose a random integer a such that $1 < a < N$ and calculate the greatest common divisor $(\gcd)$ of a and N. If $\gcd(a, N) \neq 1$, then we have found a non-trivial factor of N.

3.3.1.2 Step 2: Quantum Period Finding

If $\gcd(a, N) = 1$, use the quantum period-finding subroutine to find the period r of the function $f(x) = a^x \mod N$. The period r is the smallest positive integer such that $a^r \equiv 1 \mod N$.

The quantum period finding algorithm involves the following steps:

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

1. Initialize two quantum registers. The first register will hold the superposition of states, and the second register will hold the function values. The first register requires $2n$ qubits, where n is the number of bits needed to represent N. The second register requires n qubits.
2. Apply the Hadamard gate to each qubit in the first register to create an equal superposition of all possible states.
3. Compute the function $f(x) = a^x \mod N$ using a quantum circuit and store the result in the second register.
4. Apply the inverse Quantum Fourier Transform (QFT) to the first register.
5. Measure the first register to obtain a value that is used to deduce the period r.

Here, U_f is the unitary operation that maps $|x\rangle |0\rangle \rightarrow |x\rangle |a^x \mod N\rangle$.

3.3.1.3 Step 3: Determine Factors

Check if the found r is indeed the period by verifying $a^r \equiv 1 \mod N$, and check that r is even. If not, repeat the process with a new random a. Indeed:

- If r is odd, it cannot be used to find the factors.
- If $a^{r/2} \equiv -1 \mod N$, then r does not provide useful information.

Otherwise, compute the factors of N using the period r:

- Calculate $x = a^{r/2} \mod N$.
- Compute $\gcd(x-1, N)$ and $\gcd(x+1, N)$. At least one of these will yield a non-trivial factor of N.

3.3.2 Example

Consider an example where $N = 15$ and $a = 2$.

- Compute $a^x \mod 15$ for various values of x to determine the period r.
- Using the quantum period-finding algorithm, suppose we find $r = 4$.
- Compute $2^{r/2} \mod 15 = 2^2 \mod 15 = 4$.
- Calculate $\gcd(4-1, 15) = \gcd(3, 15) = 3$ and $\gcd(4+1, 15) = \gcd(5, 15) = 5$.
- Therefore, the factors of 15 are 3 and 5.

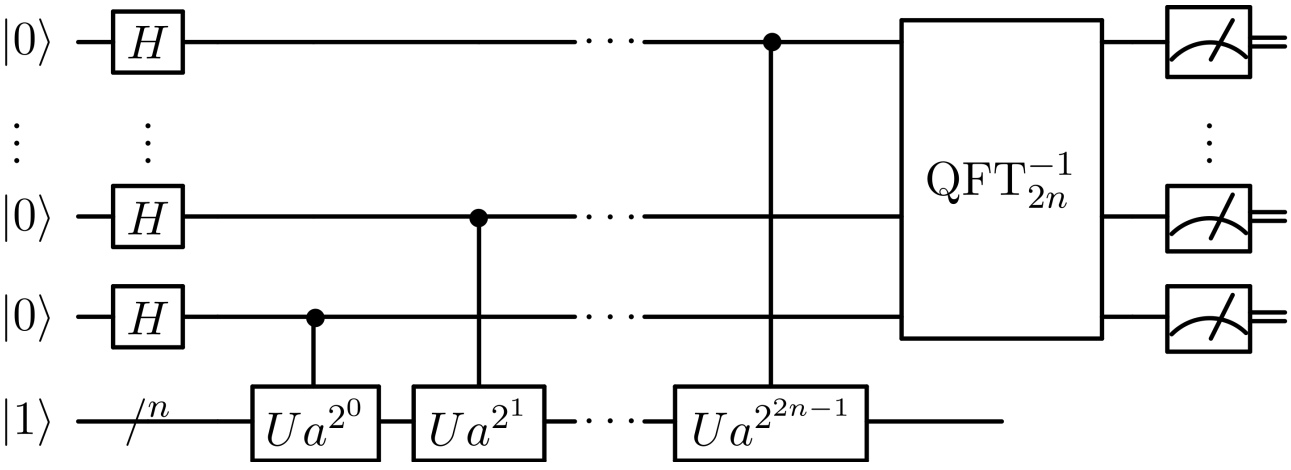


Figure 3.2: Quantum circuit for Shor's algorithm.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

3.3.3 Computational Complexity

The overall number of quantum gates required to run Shor's algorithm is $\mathcal{O}((\log N)^2(\log\log N)(\log\log\log N))$ (or, using n, $\tilde{\mathcal{O}}(n^2)$ where the $\tilde{\mathcal{O}}(\cdot)$ ignores the logarithmic factors, i.e., $\mathcal{O}(f(n)log^k n) = \tilde{\mathcal{O}}(f(n))$), which is exponentially faster compared to the best-known classical algorithms for integer factorization, such as the General Number Field Sieve (GNFS) with a complexity of $\mathcal{O}(\exp((\log N)^{1/3}(\log\log N)^{2/3}))$.

This exponential speedup over classical algorithms demonstrates the potential of quantum computing to solve certain problems much more efficiently than classical computing, highlighting the importance of Shor's algorithm in the field of quantum computation and cryptography.

3.3.4 Conclusion

Shor's algorithm is a groundbreaking quantum algorithm that has a direct impact in cryptography. It leverages the principles of quantum superposition and entanglement to solve the integer factorization problem exponentially faster than classical algorithms. The successful implementation of Shor's algorithm on large-scale QCs would render many current cryptographic systems insecure.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

4 Applications of Quantum Computing to Cryptanalysis

4.1 Introduction

The application of quantum computing to cryptanalysis represents a significant shift in the landscape of digital security. This chapter focuses on the implications of quantum computing for cryptographic systems. We assess the feasibility of implementing Shor's algorithm to break widely used cryptographic schemes and explore the potential challenges posed to lattice-based cryptography. The urgency of transitioning to quantum-resistant cryptographic methods is underscored, highlighting the need for immediate action in the face of advancing quantum technologies.

4.2 Current Feasibility of Shor's Algorithm

While research in quantum computing is more and more focused on finding new computational tasks that can exploit the nature of quantum mechanics to achieve an advantage over the classical counterpart (the so-called "quantum supremacy"), Shor's algorithm (1994) is with no doubt the oldest quantum algorithm with an unmatched improvement with respect to classical computing. Its main result is the ability to find the prime factors of any integer number in polynomial time, instead of the exponential time that a classical algorithm takes. Nowadays, computer security mainly relies on secret-key cryptography algorithms such as RSA, that rely on the very fact that the key cannot be found by brute force since it is necessary to find the prime factors of integers that range from 2048 to 4096 bits, and the exponential nature of the task makes it unfeasible with a classical computer. Shor's algorithm overcomes this barrier by theoretically being able to find the prime factors with a number of computations that is polynomial with respect to the number of bits. This allows to make it much easier to break RSA and similar algorithms.

Despite being an algorithm with polynomial complexity, the actual implementation requires a quantum circuit with a number of gates in the order of $\tilde{\mathcal{O}}(n^2)$, where n is the number of bits of the integer number. This means that breaking a 4096 bit RSA key takes $4096^2 = 2^{24} = 16\ 777\ 216$ gates. The number of necessary qubits, instead, is $\mathcal{O}(n)$. Current technologies that realize QCs, of which the main ones are superconducting, photonic and neutral atom qubits, have two problems:

- They have a limited number of qubits: even though in the best case they are in the order of thousands, they still are subject to errors that require error correction techniques. These techniques make use of other qubits to compensate for these errors, to the point where the actual number of qubits that are actually available for computation, called logical qubits, can be from 0.1% to 1% of the physical qubits. Despite the number of required qubits in Shor's algorithm is linear in n, this is a problem anyway, since for 1024 bits we would need a million of superconducting qubits, and IBM has yet to deliver a 1121 qubit processor.
- The errors reflect in the fact that only a maximum circuit size is allowed. The main physical error is decoherence, where the state of a qubit tends to lose coherence after a certain number of manipulations since they involve in part an interaction with the external environment, to the point where in the end it does not bring any information any longer.

Given the first point and the exponential number of gates required for Shor's algorithm, it is evident that we are still far from being able to implement such an algorithm. In a recent paper [11] it was shown how the complexity can be reduced to just $\tilde{\mathcal{O}}(n^{\frac{3}{2}})$ but, despite being a good improvement, the current technology can not cope with an actual implementation.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

In conclusion, although we are far from being able to break Rivest–Shamir–Adleman (RSA) and other cryptographic algorithms such as Elliptic Curve Digital Signature Algorithm (ECDSA), it is worth noting that we should expect to do so within a decade. Therefore, it makes sense to start transitioning to other types of cryptography that are immune to Shor's algorithm as soon as possible (see the blog post [12]) for two main reasons: the transition to PQC is not easy and involves many layers, processes, and standards in an a priori unknown cascade of dependencies, and the "store now, decrypt later" attack is a threat today.

4.3 Breaking Lattice Cryptography

The paper [13] initially claims a breakthrough: a polynomial time quantum algorithm for breaking lattice cryptography. If this were true, it would imply that many lattice-based cryptographic systems, which are considered secure against quantum attacks, could be broken. This would have profound implications, potentially undermining the security of current and future cryptographic protocols, including those considered for PQC standards by NIST. The paper claims to have developed a polynomial time quantum algorithm for Learning With Errors (LWE). By leveraging reductions from LWE to lattice problems, this would translate to efficient quantum algorithms for critical lattice problems like the Decisional Shortest Vector Problem (GapSVP) and the Shortest Independent Vector Problem (SIVP). If valid, this would mean that encryption schemes based on lattice problems, such as fully homomorphic encryption and certain NIST PQC candidates, could be vulnerable to quantum attacks. It would call into question the security assumptions of many cryptographic protocols that rely on the hardness of lattice problems. However, a significant bug was identified in Step 9 of the algorithm. The authors admitted they do not know how to fix this bug, rendering the main claim of the paper invalid. In summary, while the paper initially presents a groundbreaking quantum algorithm that could potentially disrupt current cryptographic systems, it ultimately fails to deliver on this promise due to a critical bug in the algorithm. The implications of the algorithm, if it had worked, would have been profound, but as it stands, lattice-based cryptographic systems remain secure against this proposed quantum attack.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

5 Quantum Computing Impact in the Security of Communication Protocols

In this chapter, we will present and evaluate the current and expected impact that quantum computing technologies have on the communication industry.

5.1 Impact of Quantum Computing Algorithms

As it was previously pointed out, quantum computing has been shown to have an impact in the communication industry due to its ability to break some of the main cryptosystems that are currently in use. The threat is two-pronged, as both public key cryptography – due to Shor's algorithm [9, 10] – and symmetric one – using Grover's algorithm [8] – can be targeted.

On the one hand, Grover's algorithm for searching unstructured databases allows for a quadratic speed-up over the classical exponential situation. This can mainly be used to target symmetric cryptosystems such as AES, but it also has an impact on the security offered by hash functions. However, it has been shown that Grover's algorithm is optimal [14], i.e., there is no quantum algorithm that improves on it, so this threat can be easily solved by doubling most key sizes in the worst case scenario.

On the other hand, Shor's algorithm solves the discrete logarithm problem for integer numbers in polynomial time using the quantum model of computation. This may seem to only have an effect on the ElGamal public key cryptosystem, which is the one based on this problem and has seen almost no use, but this is not the case, as further generalizations extend the solution to any abelian group, and thus Elliptic-Curve Cryptography (ECC) can be broken. Furthermore, the integer factorization problem can be reduced in polynomial time to the discrete logarithm one, which also allows QCs to target the RSA cryptosystem.

Similar threats apply to any cryptographic scheme that uses the described building blocks, such as the Diffie-Hellman key exchange method, which is based on the discrete logarithm problem, or digital signature schemes based on either ECC or RSA cryptosystems. However, signature schemes based on hash functions do not fall into this category.

What is the solution to this threat? Michele Mosca famously analyzed the situation in [15], where he proposed what has been called the Mosca's theorem. There are two possible solutions to the issue: using cryptography resistant to quantum computing techniques, known as PQC, or via cryptography of a quantum nature itself, more particularly Quantum Key Distribution (QKD).

Mosca's theorem deals with the timetable for the migration into these new tools by defining three magnitudes. The first of them is security shelf-life, x, which is the amount of time you need your keys to be secure (for instance, x might not be zero for national security information or health information), the second, y, is the time needed to fully complete the migration, and, thirdly, z is the collapse time, i.e., the time before a QC – or any other method – breaks the current security schemes. The key point is that, if

$$x + y > z,$$

then, attacks will be feasible and data will be exposed. Many guesses at what a realistic value for z might be have been made, but a general consensus on the margin of 15 to 20 years is commonly accepted [16].

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

5.2 Impact in Protocols

As it should be expected, any protocol that makes use of any of the previously enumerated cryptographic methods is at risk when faced with a Cryptographically Relevant Quantum Computer (CRQC). What follows is an analysis of the main communication protocols affected by this new sort of technologies, focusing specially in those based in asymmetric cryptosystems, as threats to symmetric ones have already been discussed to be less relevant. It is not the focus of this document to depicts all existing vulnerable protocols, but the most relevant and widely used.

The first affected protocol is Transport Layer Security (TLS) which employs public key cryptography during the Handshake Protocol both to establish a shared secret using either some manner of Diffie-Hellman or RSA key exchange and in using digital signatures. This, in turn, affects the Hypertext Transfer Protocol over Secure Socket Layer (HTTPS), which is based in TLS security and is paramount in web browsing and a lot of other protocols protected with TLS, such as the secure version of Simple Mail Transfer Protocol (SMTP), Internet Message Access Protocol (IMAP) or Post Office Protocol version 3 (POP3). Similarly, the Secure Shell protocol (SSH) is also affected, as it uses Diffie-Hellman to exchange keys in the Transport Layer Protocol and may use digital signatures in the User Authentication Protocol, so file transfer or any services based on SSH tunneling – including legacy non-secure protocols that delegate their security to the SSH – are also susceptible to quantum attacks.

Secondly, regarding wireless communications, the IEEE 802.11i protocol (the Wi-Fi family) includes the usage of an authentication Extensible Authentication Protocol (EAP) method in its authentication phase. Some versions of the EAP employ asymmetric cryptography, either by employing TLS (EAP-TLS), Diffie-Hellman (EAP-FAST) or digital certificates (EAP-IKEv2). Furthermore, Wi-Fi Protected Access 3 (WPA3) substitutes the 4-Way Handshake with Simultaneous Authentication of Equals (SAE), which uses Diffie-Hellman over ECC (ECDH), and allows for Opportunistic Wireless Encryption (OWE), which also makes use of Diffie-Hellman. Other similar example of wireless protocols vulnerable is Bluetooth that also involve Diffie-Hellman in the pairing process.

Thirdly, IP Security (IPsec) is also affected. Although, once again, authentication may be based on Pre-Shared Keys (PSK), Internet Key Exchange (IKE) can make use of digital certificates or asymmetric cryptography. Similarly, IKE utilizes some version of Diffie-Hellman for key exchange. Any service based on IPsec – such as Virtual Private Network (VPN) – is thus potentially weak in the presence of quantum techniques.

It should be noted that pre-shared keys – which are employed for instance in TLS or IPsec – are only quantum safe when we are referring to pre-installed information, but not in the context of pre-established secrets which were exchanged in a previous session using a public key protocol.

Regarding the security of mobile networks – particularly 5G networks – any service that makes use of any of the aforementioned protocols (TLS, SSH, IPsec) is weak in the presence of quantum techniques. The account of affected services is quite long, so [17, 18] can be consulted for a more exhaustive analysis.

What follows is a list of the main services that use each protocol.

- IPsec: 4G/5G radio fronthaul/backhaul network to security gateway connection or Software-Defined Wide Area Network (SD-WAN) services.
- TLS: internal and roaming 4G/5G Core control plane communications based on Service Based Architecture (SBA), and OSS/OAM system management in 4G/5G or provisioning profiles in eSIMs.
- SSH: operator administrative access to network components, for instance.

Of course, there are many more, e.g., Internet of Things and Customer Premise Equipment (CPE) devices, SIM card services, VPNs, privacy of costumer personal data. For example, 5G SUbscription Concealed Identifier (SUCI), that provides privacy for the SUbscription Permanent Identifier (SUPI), depends on Elliptic Curve Integrated Encryption Scheme (ECIES) [19].

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Finally, we will note the implications this has on network programmability. Regarding Network Functions Virtualization (NFV), the abandonment of hardware specific elements and the security they may provide (e.g., PSK), forces the use of protocols which rely on public key cryptography for authentication and privacy [20]. For instance, live migration of NFVs currently makes use of TLS protocols to provide confidentiality and authentication. The same happens with Software-Defined Networking (SDN), for example, OpenFlow prescribes the use of TLS for communications between network controllers and switches. Another example is the usage of Cloud-native Network Functions (CNF) in container platforms, where several tools using digital signatures – such as DSA or ECDSA – to sign and verify software images.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

6 Conclusions

In this deliverable, we have provided a comprehensive overview of the expected capabilities of QCs. We began by exploring various quantum computing technologies, including superconducting qubits, photonic qubits, trapped ions, and neutral atoms. Each of these technologies presents unique advantages and challenges, which we discussed in detail.

We then reviewed the main quantum algorithms, such as Grover's algorithm and Shor's algorithm, which exemplify the potential power of quantum computation. These algorithms highlight the significant speed-ups that QCs can achieve compared to classical computers.

Furthermore, we delved into the applications of quantum computing to cryptanalysis. The implementation of Shor's algorithm demonstrates the urgent need for transitioning to quantum-resistant cryptographic methods, as it poses a threat to widely used cryptographic systems. We also examined the potential of QCs to challenge lattice-based cryptography, which is considered one of the most promising PQ cryptographic schemes.

The impact of quantum computing on the security of communication protocols was also assessed. Quantum computing algorithms have profound implications for protocols relying on public key cryptography, necessitating updates to ensure security in a PQ world.

In summary, while quantum computing holds tremendous promise, it also presents significant challenges that must be addressed to fully realize its potential and ensure secure implementation. Continued research and development in quantum technologies, algorithms, and cryptographic methods are essential to navigate the transition from classical to quantum paradigms effectively.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].

Bibliography

[1] IBM, "IBM Quantum System Two: the era of quantum utility is here — ibm.com," https://www.ibm.com/quantum/blog/quantum-roadmap-2033.

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

[3] Aquila, "256-qubit Quantum Computer — quera.com," https://www.quera.com/aquila.

[4] IonQ, "IonQ Forte — ionq.com," https://ionq.com/quantum-systems/forte.

[5] Alfonso de la Fuente Ruiz, "Quantum Annealing," https://arxiv.org/pdf/1404.2465, 2014.

[6] D-Wave, "How Quantum Annealing Works in D-Wave QPUs," https://docs.dwavesys.com/docs/latest/c_gs_2.html#how-quantum-annealing-works-in-d-wave-qpus.

[7] D-Wave, "The Advantage™ Quantum Computer — dwavesys.com," https://www.dwavesys.com/solutions-and-products/systems/.

[8] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, 1996, pp. 212–219.

[9] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *35th annual IEEE symposium on foundations of computer science*, Santa Fe (NM, US), 1994, pp. 124–134.

[10] ——, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, p. 1484–1509, Oct. 1997.

[11] O. Regev, "An efficient quantum factoring algorithm," https://arxiv.org/pdf/2308.06572, 2023.

[12] QUBIP, "New Problems Become Post-Quantum Solutions — qubip.eu," https://qubip.eu/new-problems-become-post-quantum-solutions/.

[13] Y. Chen, "Quantum algorithms for lattice problems," https://eprint.iacr.org/2024/555.pdf, 2024.

[14] M. Boyer, G. Brassard, P. Høyer, and A. Tapp, "Tight Bounds on Quantum Searching," *Fortschritte der Physik: Progress of Physics*, vol. 46, no. 4-5, pp. 493–505, 1998.

[15] M. Mosca, "Cybersecurity in an Era with Quantum Computers: Will We Be Ready?" *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.

[16] M. Mosca and M. Piani, "Quantum Threat Timeline Report: Global Risk Institute," https://globalriskinstitute.org/publications/2021-quantum-threat-timeline-report/, 2021.

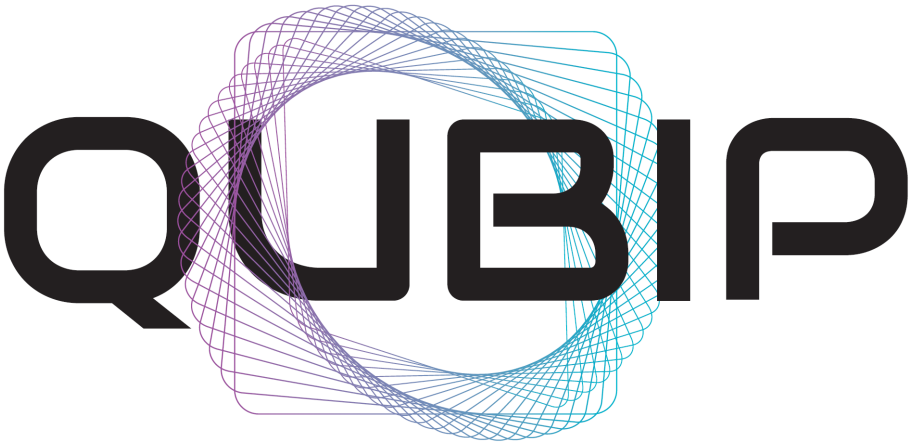
[17] GSMA, "Post Quantum Telco Network Impact Assessment. Whitepaper Version 1.0," https://www.gsma.com/newsroom/wp-content/uploads/PQ.1-Post-Quantum-Telco-Network-Impact-Assessment-Whitepaper-Version1.0.pdf, 2023.

[18] ——, "Post Quantum Cryptography – Guidelines for Telecom Use Cases Version 1.0," https://www.gsma.com/newsroom/wp-content/uploads//PQ.03-Post-Quantum-Cryptography-Guidelines-for-Telecom-Use-v1.0.pdf, 2024.

[19] 3GPP, "Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 18)," https://www.3gpp.org/ftp/Specs/archive/33_series/33.501/33501-i50.zip, 2024.

[20] M. Daghmehchi Firoozjaei, J. P. Jeong, H. Ko, and H. Kim, "Security challenges with network functions virtualization," *Future Generation Computer Systems*, vol. 67, pp. 315–324, 2017.

This project has received funding from the European Union under the Horizon Europe framework programme [grant agreement no. 101119746].



Quantum-oriented Update to Browsers and Infrastructures for the PQ transition (QUBIP)

https://www.qubip.eu

D1.1 – Expected capabilities of Quantum Computers

Version 1.0

Horizon Europe