# Quantum

Data protection
GCS

Danae Townsend, Jordi Bru, Ignasi Juez, Mariona Jaramillo
April 2023

**1.Introduction** **2**
Why do we need quantum computers? 2
Qubits 2
**2. Quantum computing** **4**
**2. 1 Quantum communication** **5**
Quantum teleportation 5
Entanglement swapping 6
**3.Quantum computing in cryptography** **7**
3.1 Cryptography 7
3.2 Why quantum computers challenge existing cryptography 7
3.3 What is QKD 9
**4.Quantum computing in encrypted data** **11**
4.1 Cryptography and encryption: Quantum security 11
4.2 Homomorphic and quantum encryption 11
4.3 Client-server quantum protocol 12
4.4 Risks 12
4.5 Current developments - Quantum safe TLS: 13
**5.Quantum computing in machine learning** **14**
Quantum Algorithms 14
**6.Conclusions** **15**
**7. References** **16**

# 1.Introduction

Quantum computing is a rapidly evolving field that combines the principles of quantum mechanics with computer science to create a new type of computing technology. Unlike classical computers that use bits to store and process information, quantum computers use quantum bits or qubits. Qubits can exist in multiple states at once, allowing quantum computers to perform complex calculations much faster than classical computers.

## Why do we need quantum computers?

Complex and difficult problems are usually solved with supercomputers, which are very large classical computers with thousands of classical CPU and GPU cores. However, even supercomputers struggle to solve certain problems and this is often due to complexity.

In these cases, we can try to solve the problem using quantum computers, which are elegant and smaller machines requiring less energy than supercomputers.

## Qubits

Qubits, short for "quantum bits," are the basic units of information used in quantum computing. Unlike classical bits which can only exist in one of two states (0 or 1) at any given time, qubits can exist in a superposition of both states simultaneously.

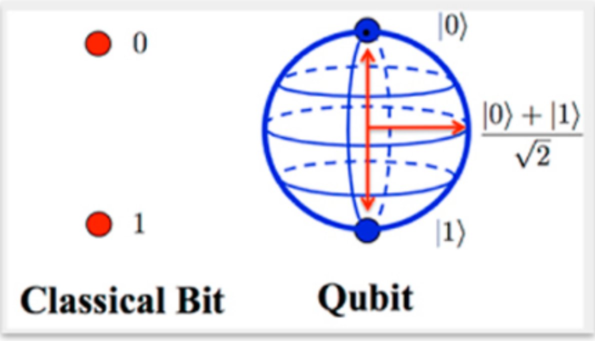

***Figure 1.*** Representation of a classical bit and a qubit. *Source: https://www.bbvaopenmind.com/*

The most important properties of qubits are superposition and entanglement:

- **Superposition**: allows a qubit to exist in a combination of different states simultaneously. For example, a qubit can be in a superposition of both 0 and 1 at the same time. This property allows quantum computers to perform many calculations simultaneously, vastly speeding up certain types of computations.
- **Entanglement**: when two or more qubits are entangled, their states become correlated in a way that is not possible with classical bits. This means that the state of one qubit can instantaneously affect the state of another qubit, even if they are far apart. Entanglement is a key resource for quantum computing, as it allows quantum computers to perform certain types of calculations much faster than classical computers.
- **No cloning theorem:** states that it is impossible to create an independent and identical copy of an arbitrary unknown quantum state.

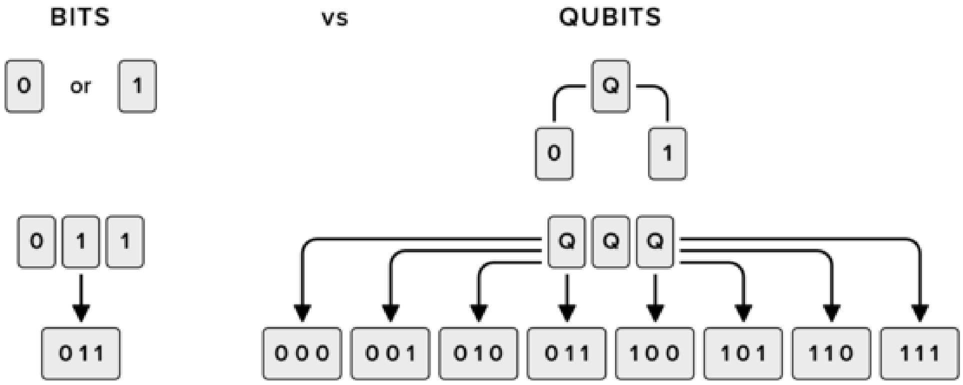

***Figure 2****.* Superposition. On the left, the classical approach, in which each bit exists in just one state, so when three bits are combined, a single state is obtained. On the right, the quantum approach, in which each bit exists in two state, then when three bits are combined, 8 different states are obtained at the same time. *Source: https://openexpoeurope.com/*

# 2. Quantum computing

There is currently a lot of discussion about quantum technology and how it has revolutionized the way we process and transmit information. That is why in this section we will go into depth about the two most outstanding applications of this technology, which are quantum communication and quantum computing. But first of all we must be clear about what quantum computing really is.

Let's start with the basics. As we already know, the bit is the basic unit of information that represents all basic computing processes. Conventional computers contain millions of tiny transistors that, when voltage is applied, conduct a current and represent the digit 1. And 0, in the opposite case [4]. These 0s and 1s are the basis for the creation of complex data strings representing information. However, quantum computing, as we have already introduced, is based on qubits and challenges this binary conception of classical bits. Qubits, which take advantage of the laws of quantum physics, can be in multiple states simultaneously, allowing more efficient or even impossible tasks to be performed with conventional computation. This is the state we have previously called superposition [5].

And now linking with the concept of entanglement introduced in the previous section, we can say that two qubits can be entangled, meaning that they can contain 4 states. And then 3 entangled qubits can contain up to 8 states, and so on. This leads to the conclusion that a machine with n qubits can have up to 2^n states at the same time [5]. Of which, each state can represent a computational operation. From here comes the idea that, with this technology, the computing capacity can grow exponentially and reach the point of being able to solve problems of a very high level of complexity.

This is the key to quantum computing. It is not to create a computer that works the same as a conventional one, but at a higher speed. But the way in which we see things or calculate algorithms is completely new. And in most cases it can become more efficient [6].

To finish clarifying its operation and the concept of superposition, we can put an example where we want to find which is the best route from a point A to a point B. As far as we know, there are a total of 10000 different routes. If we want to calculate the best route with a conventional computer, we can make up to N/2 attempts to find it, i.e. 5000 iterations, as it will go one by one, using the best case algorithm to solve the problem. But on the other hand, with a quantum computer, it is able to go through all the routes and only make approximately 100 attempts [6].

# 2. 1 Quantum communication

With this new technology and the resulting quantum entanglement and qubit concept documented in the previous section, it has been possible to create key protocols and procedures to create a new type of communication: quantum communication. As we will see at this section, this new property allows for a completely new form of information transmission.

This new property stands out from the classical one by the fact that information can be transmitted securely and efficiently over long distances without being affected by interference [7]. Unlike conventional information transmission, which can be altered due to long distances or possible noise much easier.

Taking advantage of these properties, it has been possible to develop technologies that allow the transmission of information through quantum channels that can benefit sectors such as cryptography and cybersecurity [8] since the information transmitted through these channels is immune to eavesdropping by unwanted people, which makes it ideal for applications that require security and privacy. We will go into more detail on the different applications of this technology later on.

This can be made possible thanks to qubit transmission protocols, such as the ones we will see below.

## Quantum teleportation

Quantum teleportation is a process that allows quantum states to be transmitted over long distances. It is notable for its use of the concept of quantum entanglement, which we have already defined, regardless of the distance that separates them. This will be key in the development of quantum networks and distributed quantum computing.

The quantum teleportation process involves two parties intending to share a pair of entangled particles. These particles are usually photons, particles of light that can exhibit both wave and particle behavior. One of the parties then performs a measurement of the quantum state to be transmitted, which causes the entangled particles to correlate in a specific way. The result of the measurement is communicated to the other party via a classical communication channel [9].

The other party uses this information to perform a specific operation on its entangled particle, which causes the original quantum state to be transferred to the other entangled particle [9]. This process "teleports" the quantum state from one place to another without physically moving the particle.

Further on, there is an example between Alice and Bob which will complete the explanation of the behavior of this type of state transmission.

## Entanglement swapping

Having explained the concept of quantum teleportation, we must talk about another quantum phenomenon with a different behavior but with an important relation. This phenomenon is called entanglement swapping.

In the following, we will be able to understand why we have previously been able to affirm that quantum communication is notably superior to conventional communication since it is not really affected by interference at long distances. We will see how this is not really the case, but thanks to different procedures it has been solved.

The field of quantum communication faces a significant challenge in protecting photons against loss during transmission. Unlike traditional digital communication, amplifying the signals is not possible since copying a quantum bit is physically impossible [10]. However, researchers have found a clever solution by using entanglement swapping, which involves entangling photons that have never interacted before [7]. One photon from each pair is sacrificed to establish long-distance entanglement, and this process can be repeated to increase the distance between remote entangled photons.

Despite this, quantum repeating requires precise photon synchronization across the entire network. If photons do not arrive at all stations simultaneously, the entire process needs to be repeated. To address this issue, quantum memories are introduced, which hold one photon from each pair. While the other photon travels to a swapping station upon a successful swap, the memory releases the stored photon for the next swapping step with memories. With this approach, if one block of the chain fails to swap, it is only necessary to repeat that block, making quantum communication more robust and efficient.

To understand how quantum repeaters work, we proceed to prepare a more visual example: in this process, two pairs of entangled particles, which we will call AB and CD, are initially prepared. Now, one particle is chosen from each pair. In this case, we take B and D, and we send them over long distances through fiber optics. However, due to the loss of photons, the entangled state would degrade over long distances, making the communication impossible. Here, quantum repeaters come into play. By using entanglement swapping and quantum memories, we can establish entanglement between B and C, even though they have never interacted directly before. This way, we obtain a last pair resulting from the exchange of entanglements from the two original pairs, and we can extend the entangled distance between A and B. This process can be repeated, and we can create a chain of quantum repeaters to achieve longer distances and enable quantum communication at a global scale.

# 3.Quantum computing in cryptography

## 3.1 Cryptography

We will start with a brief definition of the concept cryptography. "Cryptography is the study of mathematical techniques related to aspects of information security such as confidentiality, data integrity, entity authentication, and data origin authentication. Cryptography is a way of implementing security objectives through the use of algorithms that transform data into a format that is unreadable without knowledge of a secret key. The security of a cryptosystem depends on the secrecy of the key, the algorithm's resistance to attack, and the correctness of the algorithm's implementation." [11]

The field of cryptography encompasses a wide range of techniques, including symmetric and asymmetric encryption, digital signatures, and hashing.

So how does quantum computing pose a challenge to current cryptography?

## 3.2 Why quantum computers challenge existing cryptography

These codes, keys, encryption, and authentication schemes are essentially complex mathematical problems that are purposely designed to be challenging for classical computers to solve. Public key algorithms are particularly effective as they involve math problems that are extremely difficult to crack using classical computers, but their solutions can be easily verified.

Considering the widely-used RSA encryption as an example: the public key consists of a massive 2048-bit integer. The private key comprises the prime factors of that number. It's a straightforward task even for a basic calculator to verify the private key against the public key - just multiply the factors together. However, it would take an incredibly long time for even the most advanced classical supercomputers to decipher the 2048-bit integer into its component factors and decrypt the encoded message. To put it into perspective, every star in the universe would have burnt out and died before such a feat could be accomplished.

Encryption standards such as RSA have proven to be reliable for decades because humans have lacked the necessary tools to crack them. However, classical computers also have their limitations. They can only efficiently run specific algorithms on their binary processors. As time has passed, we've built our society on the belief that if a problem cannot be solved using binary code, it cannot be solved at all.

Quantum computers have ushered in a new era of computing, abandoning the traditional binary bit system in favor of qubits and creating complex computational spaces. This paradigm shift has made it possible to solve problems that were once considered impossible.

However, one of the problems that was once considered impossible to solve, but can now be tackled with quantum computing, is prime factorization. Mathematician Peter Shor demonstrated in 1994 that a quantum computer with sufficient computing power would be able to find prime factors of integers much more efficiently than classical computers. Shor's algorithm was the first-ever developed algorithm for quantum computers, and it will ultimately render every major public-key encryption system in use as of 2022 obsolete.

Symmetric encryption, while less secure against classical attacks, is still used for specific purposes such as credit card transactions. However, even this form of encryption is under threat from quantum computing. While Grover's Search Algorithm may not be the equivalent of a skeleton key for symmetric cryptography in the same way that Shor's algorithm is for asymmetric cryptography, it could significantly aid in brute force attacks, ultimately reducing the security of symmetric cryptography.[12]

So the main reason that quantum computers challenge existing cryptography, as said before,  is the usage of a specific type of algorithm, the Shor's algorithm to efficiently solve certain mathematical problems that classical computers cannot.

However, Shor's algorithm can efficiently factor large numbers on a quantum computer, which means that RSA encryption can be broken using a quantum computer. This could potentially allow an attacker with a quantum computer to decrypt sensitive information that was previously thought to be secure.

Similarly, other widely used cryptographic methods such as elliptic curve cryptography and symmetric key cryptography are also vulnerable to attacks by quantum computers.

Therefore, the development of quantum computers poses a serious threat to existing cryptographic methods, and researchers are actively working on developing new cryptographic methods that are resistant to attacks by quantum computers, known as post-quantum cryptography.

As we can see the huge societal benefits of quantum computing come with a challenge: fully-realized quantum computers will be able to break many of the most widely-used cybersecurity protocols in the world. Data considered secure today may already be at risk, due to the threat of harvest-now-decrypt-later schemes.[13]

## 3.3 What is QKD

Quantum Key Distribution (QKD) [14, 15] is a technology, based on the quantum laws of physics, rather than the assumed computational complexity of mathematical problems, to generate and distribute provably secure cipher keys over unsecured channels. It does this using single photon technology and can detect potential eavesdropping via the quantum bit error rates of the quantum channel. Sending randomly encoded information on single photons produces a shared secret that is a random string and the probabilistic nature of measuring the photon state provides the basis of its security.

A QKD system consists of a quantum channel and a classical channel. The quantum channel is only used to transmit qbits (single photons) and must consist of a transparent optical path (fiber, free-space and optical switches, no routers, amplifiers or copper). It is a lossy and probabilistic channel. The classical channel can be a conventional IP channel (not necessarily optical), but depending on system design it may need to be dedicated and closely tied to the quantum channel for timing requirements.

With the advent of quantum computers, several of the cryptographic constructs underlying the security model of IPsec and TLS will be broken. Breakthroughs in cryptanalysis continue to present a possible threat as well. Quantum-resistant replacements will have to be found for public-key cryptography and for Diffie-Hellman key agreement. Using quantum keying material within these protocols would solve this problem. QKD does not solve the authentication problem and would rely on conventional authentication techniques (public key or pre-shared secret).

The BB84 [16] protocol and its variants are the only known provably secure QKD protocols. The BB84 protocol consists of four stages:

- **The first stage** is the transmission of the randomly encoded single photon stream over the quantum channel from the sender A to the receiver B to establish the initial raw key. A maintains a temporary database of the state of each photon sent.
- **The second stage** is sifting, where B sends a list of photons detected and their basis, but not their value, back to A over the classical channel. There is only one photon and it can only be measured once, so only one basis can be applied. If it’s measured in the correct basis the value measured will be correct. If it’s measured in the wrong basis, the value will be random. Alice retains, from its database, only those entries received by Bob in the correct basis and sends this revised list back to Bob over the classical channel. Bob retains only those entries on this revised list. Alice and Bob now have a list of sifted keys. These lists are of the same length but may have some errors between them. This is the quantum bit error rate and it is an indication of eavesdropping.
- **The third stage** is reconciliation to correct these errors. Cascade [9, 10] and its variants are the predominant reconciliation algorithm that exchange parity and error correcting codes to reconcile errors without exposing the key values. This process

requires a number of communications between Bob and Alice, over the classical channel, and results in a list smaller than the sifted list.

- **The fourth stage** is privacy amplification, which computes a new (smaller) set of bits from the reconciled set of bits using a hashing algorithm and requires no communication between Alice and Bob. Since the reconciled set of bits were random, the resulting privacy amplified set will also be random. Unless the eavesdropper knows all or most of the original bits, she will not be able to compute the new set.

QKD offers several advantages over traditional methods of key distribution, such as public key cryptography. It is theoretically impossible for an eavesdropper to intercept the key without being detected, and the security of the key does not rely on the difficulty of solving mathematical problems, as is the case with public key cryptography. However, QKD is still a relatively new technology and there are practical limitations that need to be addressed before it can be widely deployed.

The benefits of QKD are that it can generate and distribute provably secure keys over unsecured channels and that potential eavesdropping can be detected. QKD is not subject to threats from quantum computers or break through algorithms that can defeat the current computationally complex key exchange methods. Because QKD generates random strings for shared secrets, attaining a QKD system and reverse engineering its theory of operation would yield no mechanism to defeat QKD.

It is important to note that QKD is not a complete solution to the threat posed by quantum computing. While it provides a way to distribute keys that are resistant to attacks by quantum computers, it does not provide a way to protect the data itself from being intercepted or altered. Therefore, QKD is just one piece of the puzzle in developing secure communication systems that are resistant to quantum computing attack.

# 4.Quantum computing in encrypted data

## 4.1 Cryptography and encryption: Quantum security

| Cryptography | Encryption |
|---|---|
| Science of encrypting and decrypting information, including communication practices and techniques. Related to information security terms such as: Data confidentiality, integrity and authentication. | Information converted into a non-public code, whose true meaning cannot be observed, given an unreadable format intended for unauthorized persons. |

Although the terms are used in much the same ways, encryption is a process specific to cryptography that can be used in conjunction with other techniques and protocols to protect sensitive information. Said process uses algorithms that today must be sufficiently robust and capable of supporting quantum-based vulnerabilities, which introduces quantum security.

Quantum security systems use quantum cryptography protocols, which allows the communication and transmission of information in a secure and reliable manner, without the meddling of third parties or alteration of the communication. [19]

## 4.2 Homomorphic and quantum encryption

In April 2011, Sony's Playstation and Dropbox companies were exposed to a security flaw related to encryption. Sony exposed credit card information, passwords, addresses and personal information, while Dropbox was accused of hosting unencrypted files. The problem involves data handling without the information being exposed, which is why homomorphic encryption was introduced. [20]

Homomorphic encryption refers to a cipher operations technique that has the ability to perform specific mathematical operations on previously encrypted data and produce a result that is unreadable unless it is decrypted, in other words, it allows mathematics to be performed on encrypted data without having to decrypt the data in the process. When the result is decrypted, it matches the result of operations performed on the unencrypted data. For example, two numbers could be encrypted and then added, resulting in another recorded number where the identity of the first two numbers is unknown. Upon completion, the result would be deciphered and it would be impossible to know the value of the individual numbers. Homomorphic encryption provides security to user information in external browsing, so the use of logical and arithmetic operations are useful. [21]

Quantum homomorphic encryption is theoretically possible, it is not practical due to limited resources, since one of the restrictions is that the complexity of the operations does not imply a greater use of resources than encryption and decryption, and in this case the use of resources would grow exponentially. Even so, different approaches have been presented that make possible the use of quantum computing in homomorphic encryption. Research papers suggest a trade-off when using photonic quantum processors, thus perfect privacy is not required as long as the maximum amount of information available to an attacker is small enough. The learning technique has practical applications in automatic algorithms, search, boson testing, among others. Security in this context should not be compared to existing classical techniques for classical computing. [22]

## 4.3 Client-server quantum protocol

In general, there is a proposed protocol that involves a client sending its quantum information to a remote server for processing. The client encrypts the input qubits and sends them along with the necessary helper qubits to the server. The server executes the specified quantum gates sequentially, which requires one round of classical communication between the server and the client for each non-Clifford gate, taking into account that such gates are necessary for performing operations universally. Once the computation is complete, the encrypted qubits are returned to the client for decryption. The server does not acquire knowledge about the quantum information processed, but it can choose to perform a different calculation. This protocol would bring benefits such as the use of fewer qubits and fewer rounds of communication between the client and the server. [23]

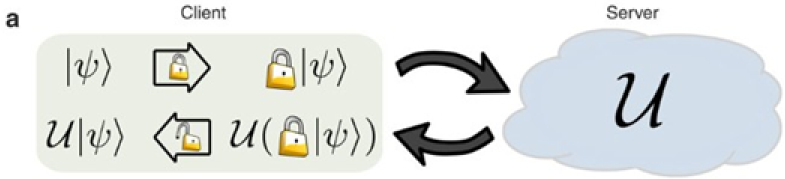

***Figure 3****. A client encrypts a quantum state and sends it to a quantum server, who performs a computation  on the encrypted qubit. The server returns the state which the client decrypts to get. [23]*

## 4.4 Risks

a. **Precision:** It must be taken into account that a quantum computer works with probabilities, so it is low, but there is a possibility of returning the correct solution among 10,000 possibilities within a test. To make the probability less, it would be suggested to carry out several tests when using quantum computing, however, such action would decrease the speed of the tool.
b. **Environmental factors:** Since we work with Qubits (Quantum Bits), slight changes in the environment, magnetic coupling could lead to an alteration in the information stored in them. Therefore, the qubits in its implementation must be isolated and controlled, with a temperature close to absolute 0. Even so, said insulation measure contributes to the contamination of the environment, falling again in the increase in temperature and noise.
c. **Phase Error:** Qubits are susceptible to data shifts where the signal flips incorrectly, causing measurement errors. [24]

## 4.5 Current developments - Quantum safe TLS:

The Transport Layer Security (TLS) protocol is one of the most widely used security protocols on the Internet to protect the privacy and security of online communication. However, the increasing ability of quantum computers to break conventional cryptographic systems poses a threat to the security of TLS-protected communications. As a result, quantum security solutions for TLS, known as quantum secure TLS, are being developed that use quantum cryptography to protect online communications from quantum threats. The current developments are focused on quantum-secure TLS, including public-key protocols based on quantum cryptography, and ongoing efforts to standardize and commercialize these quantum-secure technologies.

Today, the IMB company has contributed a series of resources for the development of quantum computing, including: Key Encapsulation Mechanisms (KEM) and digital signature schemes. [25] Given the advent of quantum computers, encryption such as RSA is believed to be vulnerable. The National Institute of Standards and Technology (NIST) claims that these early IBM cryptography protocols are quantum secure thus solving the problem of information exposure. These algorithms are called “Quantum safe TLS”. [26] [27]

# 5.Quantum computing in machine learning

Quantum computing has the potential to significantly impact the field of machine learning by providing faster algorithms for certain tasks and enabling the development of new machine learning methods.

However, the development of quantum machine learning is still in its early stages, so lots of challenges still have to be faced, such as assuring the reliability and scalability of quantum computing hardware and software, as well as finding ways to mitigate the effects of noise and decoherence in quantum systems.

## Quantum Algorithms

Developing algorithms for a potential quantum computer consists on using gates in order to create a quantum state that has a relatively high amplitude (this means high probability) for states that represent solutions for the given problem. Quantum algorithms are usually repeated a number of times since the result is always probabilistic.

Next, three quantum algorithms will be explained:

1. **Quantum support vector machine (QSVM)**: QSVM can classify data faster than classical support vector machines (SVM) by using quantum interference to perform the classification task in a single step, rather than the iterative process used by classical SVM.
2. **Optimization problems such as Quantum Approximate Optimization Algorithm (QAOA)**: first, it uses a series of quantum operations to prepare a quantum state that encodes the problem, and then measures the state to obtain a classical solution. The classical solution is then used to update the quantum state, and the process is repeated iteratively until an optimal solution is found or some other stopping criterion is met.
   One of the key advantages of QAOA is that it can be implemented using existing quantum hardware, without the need for error correction or fault tolerance. QAOA has been shown to be effective in solving a variety of optimization problems, including the Max-Cut problem, the Traveling Salesman problem, and the Ising spin-glass problem. [17]
3. **Quantum neural networks**: Quantum neural networks use qubits instead of classical bits as the basic unit of computation. They offer an advantage over classical neural networks through a higher effective dimension and faster training ability. In quantum neural networks, information is first encoded into a quantum state via a state preparation routine. Once data is encoded into a quantum state, a variational model containing parameterised gates is applied and optimised for a particular task through a loss function minimisation, where the output of a quantum model can be extracted from a classical post-processing function that is applied to the outcome. [18]

# 6.Conclusions

In conclusion, quantum computing has emerged as a promising field with the potential to revolutionize various aspects of technology.

The introduction highlighted the importance of quantum computers and their unique building blocks known as qubits. Moving forward, the exploration of quantum communication unveiled groundbreaking concepts such as quantum teleportation and entanglement swapping.

Furthermore, the discussion on quantum computing in cryptography shed light on the challenges posed by quantum computers to existing encryption methods, emphasizing the need for Quantum Key Distribution (QKD) to ensure secure communication. Additionally, the exploration of quantum computing in encrypted data touched upon topics such as quantum security in cryptography and encryption, homomorphic and quantum encryption, and client-server quantum protocols. The section highlighted the risks associated with these developments but also presented current advancements like Quantum Safe TLS. Finally, the discussion on quantum computing in machine learning hinted at the potential of quantum algorithms to enhance and transform the field of machine learning.

Overall, these insights demonstrate the vast potential of quantum computing and its imminent impact on various domains.

# 7. References

[1] IBM, Quantum Computing [Online; accessed 17th April 2023 https://www.ibm.com/topics/quantum-computing]

[2] GCS course slides.

[3] Schuld, M., Sinayskiy, I., & Petruccione, F. (2015). An introduction to quantum machine learning. Contemporary Physics, 56(2), 172-185.

[4] Allende, M., 2022. TECNOLOGÍAS CUÁNTICAS: Una oportunidad transversal e interdisciplinar para la transformación digital y el impacto social.

[5] Israel Physical Society. (n.d.). What are Quantum Computing and Quantum Communication? [Online].
Available: https://www.ippi.org.il/what-are-quantum-computing-and-quantum-communication/

[6] S. V. D. Ruiz, B. F. A. Minga, J. D. C. Soto and E. F. M. Zambrano, "Impact of quantum computing on current technologies," 2022 17th Iberian Conference on Information Systems and Technologies (CISTI), Madrid, Spain, 2022, pp. 1-12, doi: 10.23919/CISTI54924.2022.9820248.

[7] S. Ahmed, S. Al Arif, M. Alnaggar, and M. Alam, "Quantum Computing: An Overview," J. Phys.: Conf. Ser., vol. 624, p. 012003, 2015. [Online].
Available: https://iopscience.iop.org/article/10.1088/1742-6596/624/1/012003/pdf

[8]
K. N. Smith, "What Is Quantum Communications?," MIT Technology Review, Feb. 14, 2019. [Online].
Available:
https://www.technologyreview.com/2019/02/14/103409/what-is-quantum-communications/

[9] N. Gisin, "The Principle of Quantum Cryptography," J. Phys.: Conf. Ser., vol. 1865, p. 022008, 2014. [Online].
Available: https://iopscience.iop.org/article/10.1088/1742-6596/1865/2/022008/pdf

[10] Aliro Quantum, "How Do Quantum Repeaters Work?" [Online]. Available: https://www.aliroquantum.com/blog/how-do-quantum-repeaters-work

[11] "Cryptography Engineering: Design Principles and Practical Applications" by Bruce Schneier, Niels Ferguson, and Tadayoshi Kohno

[12] https://www.ibm.com/topics/quantum-safe-cryptography

[13] https://www.ibm.com/quantum

[14] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 Quantum cryptography Rev. Mod. Phys, 4 41.1-41.8

[15] Chou C W, Laurat J, Deng H, Choi K S, de Riedmatten H, Felinto D and Kimble H J 2007 Functional quantum nodes for entanglement distribution over scalable quantum networks Science 316 1316-20

[16] C. H. Bennet and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” in Proc IEEE Intern’l Conf on Computers, Systems and Signal Processing, Bangalore, India, 1984, pp. 175-179

[17] Quantum Approximate Optimization Algorithm (QAOA). Grove. [Online; accessed 17th April 2023 https://grove-docs.readthedocs.io/en/latest/qaoa.html]

[18] Abbas, A., Sutter, D., Zoufal, C., Lucchi, A., Figalli, A., & Woerner, S. (2021). The power of quantum neural networks. Nature Computational Science, 1(6), 403-409.

[19] IMB, "Security in the quantum computing era", *IBM Inst. Bus. Value*, vol. 1, p. 7, 2023.

[20] Yi, X., Paulet, R., Bertino, E. (2014). Homomorphic Encryption. In: Homomorphic Encryption and Applications. SpringerBriefs in Computer Science. Springer, Cham. https://doi.org/10.1007/978-3-319-12229-8_2

[21] M. Ogburn, C. Turner y P. Dahal, "Homomorphic Encryption", Procedia Comput. Sci., vol. 20, pp. 502–509, 2013. [En línea]. Disponible: https://doi.org/10.1016/j.procs.2013.09.310

[22] Zeuner, J., Pitsios, I., Tan, SH. et al. Experimental quantum homomorphic encryption. npj Quantum Inf 7, 25 (2021). https://doi.org/10.1038/s41534-020-00340-8

[23] Fisher, K., Broadbent, A., Shalm, L. et al. Quantum computing on encrypted data. Nat Commun 5, 3074 (2014). https://doi.org/10.1038/ncomms4074

[24] Z. Kirsch, "Quantum Computing: The Risk to Existing Encryption Methods", Tufts univ., p. 8, 2015. [En línea]. Disponible: http://www.cs.tufts.edu/comp/116/archive/fall2015/zkirsch.pdf

[25] "IBM Quantum Computing | Quantum Safe". IBM - Deutschland | IBM. https://www.ibm.com/quantum/quantum-safe

[26] M. Osborne y V. Lyubashevsky. "NIST's quantum-safe standards | IBM Research Blog". IBM Research Blog. https://research.ibm.com/blog/nist-quantum-safe-protocols.

[27] "IBM Cloud Docs". IBM Cloud. https://cloud.ibm.com/docs/key-protect?topic=key-protect-quantum-safe-cryptography-tls-introduction.