Quantum Cryptography and its applications

Omar Naja
DEIB
Politecnico di Milano
Milan, Italy
omar.naja@mail.polimi.it

***Abstract*—Cryptography has always played an important role when it comes to data protection. However, as technology advances and new fields emerge, traditional cryptographic methods are insufficient, and new solutions must be provided. This paper explores one of them, known as Quantum Cryptography (QC), which represents a new approach to cryptography. Providing a complete description of its theoretical principles and practical applications, QC's potentialities and efficiencies in providing new cryptographical solutions designed for the new technologies are presented.**

***Index Terms*—Cryptography, Quantum Communication, Quantum Cryptography (QC), BB84, Quantum Key Distribution (QKD), Post-Quantum Cryptography**

I. Introduction

Even if technology is improving year after year and new, better solutions are provided to well-known problems, management and protection of information and sensitive data is still important.

Cryptography has always played a crucial role in this context. However, the classical, traditional solutions are not well suited to the new technologies. That's why more recent advancements have been introduced, among which Quantum Cryptography (QC) stands out.

QC, as stated in the article *An introduction to quantum computing for non- physicists* [18], represents a new cryptographic paradigm and integrates the classical approach with quantum mechanism in order to enhance communications security.

This paper is made up of seven sections, that are structured as now described:

- Section 2 describes the research methodology adopted, describes which main questions have been considered to conduct the research, and ends with a brief analysis and conclusion regarding the analyzed topic.
- Section 3 offers a full overview of the main physical laws that are the basis of QC's development and introduces the real topic of this paper.
- Section 4 presents a full discussion about QKD, including discussions and analysis on its implementation and on protocol BB84.
- Section 5 focuses on Quantum Key Distribution Network (QKDN), the field for which most of the founded information are related to.
- Section 6 presents the current challenges.
- Section 7 concludes this paper by providing a full summary and some personal analysis.

II. Research Methodology

The approach that has been chosen for developing this research is the EBSE Systematic Literature Review. It aims to identify and analyze the available literature for a given topic.

More in detail, by making some query requests, it provides a large set of articles, books, papers, and so on, that are related to the given input.

The choice of methodology was guided by the paper titled *Systematic literature reviews in software engineering – A systematic literature review* [9]. This approach consists in seven main steps:

- **Research question**: the main questions from which to start to write the article. The questions will bring a sufficient amount of request queries that are made to the chosen tool(s) to conduct the research and find a proper amount of texts.
- **Search process**: manual search of specific journal papers, books, and other relevant sources. In this case, the research took into account papers only because of their formal language and completeness.
- **Inclusion and exclusion criteria**: decision for which findings to consider for the survey and which ones to discard. In this case, papers that don't have lots of citations and that are too old are discarded when looking for detailed, updated information.
- **Quality assessment**: evaluation of the methodological rigor and trustworthiness of the included studies. This step ensures that the founded references are considered reliable.
- **Data Collection**: all the relevant data are extracted from each study, including sources and authors
- **Data Analysis**: data studying for analyzing whether the information answers the research questions.
- **Deviations from protocol**: if needed, it is possible to change the research pattern to find some different results. For this research's purpose, no deviations were necessary.

A. Research Questions

For our specific purposes, the main information that we started looking for is related to quantum cryptography, starting with a general overview regarding the main quantum physical properties that are at the basis of quantum computers and, specifically, on quantum cryptography and, completed with studies related to the classical cryptography, to move to the

current technologies and solutions adopted. In particular, here we list the Research Questions:

RQ1 What are the current paradigms in Quantum Cryptography?

RQ2 What are the main challenges in the field of QKD?

Starting from the Research Questions listed before, there have been performed a series of queries to extract some articles and papers in order to assess them.

The table below illustrates the requests that have been made to the IEE Xplore tool.

After a first analysis, the conclusion is that QKD is, nowadays, the most preferred approach, while post-quantum, for which studies are still ongoing, there is a limited amount of information. For this reason, the decision to focus more on the first approach.

In order to get more details regarding QKD, other requests have been performed to the Scopus tool,

The table below summarizes all the requests, including the tool used and the reason behind the performed queries.

In order to filter the results and have fewer articles from which to study, we decided to look only for articles not older than 8 years (i.e., from 2016 to now) and to look for those with a high number of citations.

An interesting look can be made by studying the main technologies and approaches that have been exploited in 2016 [5] and 2020 [14], noticing that the information that has been collected is complementary, concluding that there are no differences in the actual differences. In fact, the two articles provide different approaches in different contexts (Hardware-Software and QKD Networks, respectively).

In order to make this paper easier to be understood, here is reported a tabel that shows, for each section, the research question that is/are considered and answered.

B. Analysis and discussions

The research revealed the main principles and properties that guide this new technology. While the classical approach to cryptography relies on mathematical rules and functions, Quantum Cryptography is grounded in physical properties, specifically quantum mechanics, which is an important research field in contemporary physics.

Quantum Cryptography solutions encompass two different approaches, that have been identified as **Quantum Key Distribution (QKD)** and **Quantum-Resistant Algorithms**. While the first is closely tied to new quantum computers and their security and, consequently, it guarantees more efficiency while technology advances, the second field focuses more on algorithms and still shares some similarities with the current infrastructures, that can easily integrate the new cryptographic systems.

These two approaches are significantly different and find application in distinct contexts. This research states that QKD has more applications and utilities than post-Quantum cryptography, as demonstrated by the reported examples.

Question	Query	Tool	Rationale
1	quantum AND communication	IEE Xplore	To extract articles related to general concepts of Quantum Communications
1	photon AND polarization AND principle	IEE Xplore	To explore the Photon Polarization Principle in more detail
1	quantum AND cryptography	IEE Xplore	Initial query to gather foundational data
2	(qkd) OR (quantum AND key AND distribution)	IEE Xplore	To obtain further details about Quantum Key Distribution (QKD)
2	post-quantum AND cryptography	IEE Xplore	To gather starting information about Post-Quantum Cryptography
1	(iot OR (internet AND of AND things)) AND (quantum AND cryptography)	IEE Xplore	To search for articles on the application of Quantum Cryptography in IoT
1	cloud AND quantum AND cryptography	IEE Xplore	To find articles on the application of Quantum Cryptography in cloud management
2	quantum AND key AND protocols	IEE Xplore	To search for articles related to Quantum Key protocols
1	cloud AND quantum AND computing AND security	IEE Xplore	To find information about the usage of Quantum Computing in cloud security
2	(properties OR approaches) AND (qkd OR (quantum AND key AND distribution))	Scopus	Looking for more specific informations regarding QKD

TABLE I
PERFORMED REQUESTS

#	RQ1	RQ2
Section 3	x	
Section 4	x	
Section 5	x	x
Section 6		x

TABLE II
CORRESPONDENCES QUESTIONS-SECTIONS

C. Summary

After a first personal research on informal websites and article, queries performed using IEE Xplore tool helped to start building the paper structure. A total of 35 papers and 9 online articles have been found and choosen as initial sources.

Analysing their content, only 26 will be used as actual

sources fot this paper (all of them mentioned in the last, Bibliography section).

First results provided lots of informations on QKD, while for Quantum Resistant Algorithms there have been found few and non detailed papers. Hence, the decision to go deeply inside QKD world, as the queries performed to the Scopus tool suggest. In particular, the main focuses were the analysis of the BB84 protocol, shown to be the main one that is used for contemporary researches, and then moving on to study QKDN (Quantum Key Distribution Network), the main area in which QKD is applied. That is not surpising, considering that quantum communication is mainly applied for faster communications fot network perspectives and how internet is starting to rely on this technology and, hence, suited cryptographic algorithms are needed.

Table III summarizes all the selected articles and their related topics.

#	Premises	Quantum Cryp-togra-phy	Quantum-Resistant Algo-rithms	QKD	QKD main chal-lenges	Real-World appli-cations
[1]	x		x			
[2]			x			
[3]						x
[4]	x					
[5]			x	x	x	
[6]	x					
[7]						x
[8]	x				x	
[9]	x					
[10]	x	x				
[11]	x	x	x			
[12]		x				
[13]			x			
[14]					x	
[15]			x	x		
[2]			x			
[16]			x			
[17]		x				
[18]	x					
[19]						x
[20]	x					
[21]		x				
[22]				x		

TABLE III
CORRESPONDENCES ARTICLES-TOPICS

- Premises: Almost all the concepts included sections 2 and 3: systematic review's approach, all the physical background concepts related to quantum cryptography
- Quantum Cryptography: all the articles that calls the basic concepts that introduce the technology
- Quantum-Resistant Algorithms: All the articles that treat about post quantum cryptography and goes specifically in one of the defined algorithms
- QKD: All the concepts related to QKD and included in section 3
- QKD main challenges: Set of articles used after the decision of going deeply inside the QKD topic
- Real-World applications: section that has not been included since the research didn't provide actual applications, but some interesting studies regarding IoT and Cloud computing, that will be cited as proof of BB84 importance

Lastly, here there is a graphic map that might help the reader understand the paper's structure and the logical schema that has been followed when writing this paper.

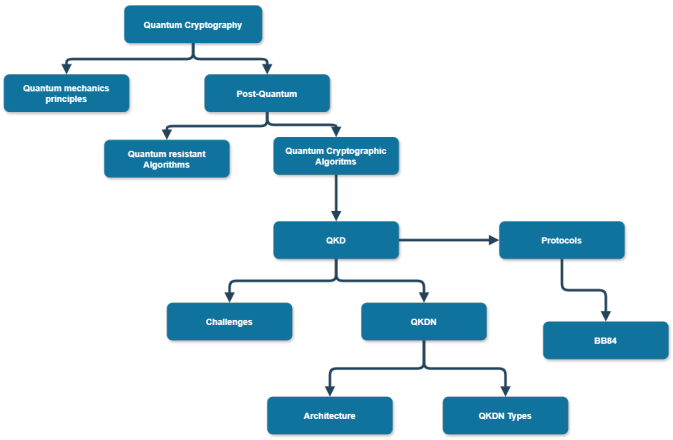

Fig. 1. Guide

III. BACKGROUND

This section aims to provide a general, complete introduction to the classical technologies that are necessary to understand the tools, principles, and algorithms that will be discussed in the article. The first section will briefly describe quantum computing, and the second will introduce the concept of cryptography as known in its historical, mathematical perspective.

In both cases, there will not be an advanced physical or mathematical description; it will be a simple introduction.

A. Quantum computing

The starting point is Richard Feynman's observations in 1982, in which he found out that some quantum mechanisms cannot be simulated on a classical computer, hence the need to build quantum computers capable of performing such operations.

B. Quantum mechanics principles to remind

In order to guarantee a complete understanding of the technologies described, this section will provide a simple recall of the main principles of quantum mechanics.

Photon Polarization Principle

This first principle addresses that photons are polarized using specialized filters and resulting in one of the four possible polarization states, each one corresponding to a specific bit designation as shown in Figure 2:

- *vertical*: 0 qubit;
- *45° right*: 0 qubit;
- *horizontal*: 1 qubit;
- *45° left*: 1 qubit;

A quantum bit, or qubit, is a fundamental quantum information unit. It is represented as a unit vector in the two-dimensional complex vector space, where the basis $\{|0\rangle, |1\rangle\}$ have been fixed. Each qubit can exist in a superposition of the classical states $|0\rangle$ and $|1\rangle$, allowing it to represent multiple quantum states simultaneously. Qubits also encode and manipulate information in quantum computers and quantum communication systems. Photon polarization dictates that when plain polarized light emits a photon-electron pair, the electron is always ejected in a preferred direction, indicative of its wave-like behavior. Consequently, a photon filter can only detect photons with a similar polarization state; otherwise, they will be destroyed. Therefore, the measurement of photons cannot be done in parallel.

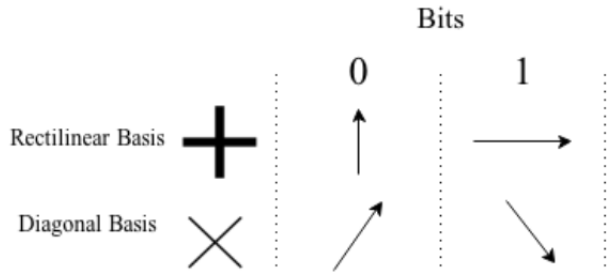

Fig. 2. Photon Polarization [4]

It is interesting to notice that, in Quantum Cryptography, photons are just used for transferring data [8].

Heisenberg Uncertainty Principle

This second principle states that it is not possible to calculate accurately position and momentum, which are two properties of the object used to determine its quantum state.

In other words, it is inevitable to produce changes in the system if we try to calculate the quantum state of an object, and consequently, the polarization of light particles can only be observed when it is measured.

This principle provides great security in the context of Quantum Cryptography, as any malicious attempt to detect the state of data at a particular point will inevitably alter the state itself, making the observation useless. [8].

C. Quantum Cryptography

Classical cryptographic systems are generally based on mathematical approaches. This surely provide, based on the adopted algorithm, a suitable security for most of the existing IT infrastructures, but they are not resilient with the advance of new technologies.

Generally, when referring to systems that have to adopt cryptogtaphic technologies for providing security against advancements in quantum computing we will talk about *Post-quantum cryptography* [12].

Up to now, we can classify the post-quantum approaches in two main categories [12], that are briefly summarized in Figure 3. The first one is based on *Quantum-Resistant Algorithms*, algorithms based on mathematical approaches as the classical cryptographic system does, hence easier to be integrated with the currently existent IT infrastructures althought security cannot be guaranteed when comes to face advancemenents in quantum technologies. Based on the type of computational problem they address, we can categorize Quantum Resistant Algorithms into four main categories [11]:

- Code-based Algorithm: use of error correction codes to generate public keys from private matrices with purposefully injected errors. They are generally fast because of the algorithm's low complexity in encryption/decryption, although they are characterized by relatively high key rate, sometimes requiring even millions of bits[12];
- Lattice-Based Algorithm: based on the difficulty of solving complex mathematical problems, generally based on lattice. For example, given an n-dimensional vector space, finding the closest vector to an arbitrary point in the lattice is difficult [12];
- Hash-based Algorithm: schemes based on hash functions, generally common even in tha classic cryptographic system and, hence, suited for most of the existing IT Infrastructures;
- Multivariate Algorithm: signature and encryption schemes based on multivariate polynomials and the difficulty of solving linear problems;

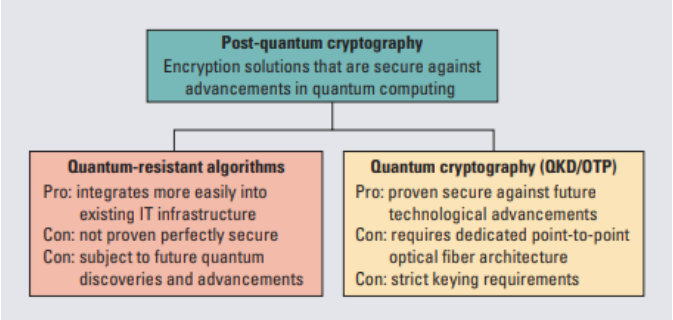

Fig. 3. PQC Fields [12]

On the other hand, Quantum Cryptographic algorithms, which are based on the quantum mechanics that have been called in the previous paragraphs in order to to ensure the security of data transfers, as stated in the article *Quantum cryptography with photon polarization and Heisenberg uncertainty principle*[20], aims to make it possible for cryptography to be suited with the advancements in quantum systems.

This one is widely regarded as the most secure solution, even thought not all the existent infrastructures can adopt it since lots of specific physical requirements to satisfy, as need for dedicated point-to-point optical fibers and, based on various contexes, suited architectures [11].

IV. Quantum Key Distribution

A. Introduction

Quantum Cryptography has emerged as a solution to the imperative need for securing data with unconditional security, leveraging the fundamental laws of physics.

Among the various techniques within Quantum Cryptography, Quantum Key Distribution (QKD) stands out as the most reliable primitive. QKD protocols enable the secure distribution of cryptographic keys between users and applications by encoding information in qubits, facilitating the key establishment over an untrusted networked channel [3]. QKD communications is composed of a transmitter, a receiver, and two communicating networks (a quantum channel connected to the transmission of quantum random-bits signals and a conventional channel). An attacker, which we assume has infinite computing capacity, is able to enter both the quantum and classical public networks without being able to access the encoder and decoder, making it impossible for him to detect the key [3].

The classical channel, which could be an Internet link or a telephone line, serves for the mutual authentication of the parties and the key sifting phase.

Meanwhile, the quantum channel, often employing optical fibers or free space, facilitates the transmission of qubits. Here, the first user randomly selects one of two possible bases to prepare each qubit, which is then sent over the channel. The second user receives these qubits and measures each one using one of the two possible bases. Subsequently, they communicate via the classical channel, discarding qubits for which they did not use the same base during the key sifting phase.

As discussed in the previous section, an adversary attempting to intercept the stream of photons on the quantum channel cannot observe them without altering their state, thereby triggering detection.

It is important to authenticate the classical channel. By checking the change in the threshold calculated before the transmission, the sender and the receiver will detect if an attacker eavesdrops on the quantum channel. If the error exceeds a certain threshold and leads to discarding random bits along those limitations, the sender and the receiver stop producing the secret key. Thus, QKD requires parties to be involved in sharing a secret symmetric key. If an eavesdropper attempts to snatch the key in a QKD protocol, communicators may use applicable quantum laws to observe it, like the known Heisenberg uncertainty theory. On the other hand, the protocol randomly produces long keys as long as the attacker is passive [3].

There are two categories of QKD protocols:

- *Protocols based on Heisenberg's uncertainty principle*: in these protocols, adversaries are detected by comparing the expected amount of error in communications between the two parties with the actual error measured. An example of such a protocol is BB84.
- *Protocols based on Quantum Entanglement*: these protocols involve the use of entangled photon pairs shared between the two parties. Adversaries can be detected because any attempt to measure the photons will inevitably alter the entangled system. Examples of protocols in this category include E91 or BBM92.

B. QKD Implementation

Quantum cryptography encompasses a wide range of specialized QKD protocols, which have garnered significant interest from researchers and specialists in the secure communication field.

Figure 4 shows the layered structure of QKD protocols, consisting of multiple layers.

Those layers are tailored specifically to the unique principles and requirements of quantum communication, reflecting the different approach employed compared to classical communication protocols [20].

The particular nature of QKD protocols underscores the need for dedicated research and development efforts to explore their capabilities, limitations, and potential applications.

By investigating and refining these protocols, researchers aim to advance the field of quantum cryptography and unlock new possibilities for secure communication in various heterogeneous domains.

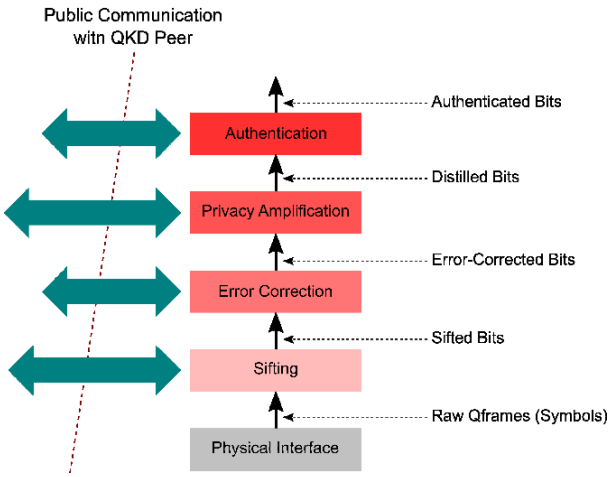

Fig. 4. QKD Protocol [16]

1) Sifting: The process begins when a sender initiates the transmission of a message, which is then received by the desired addressee (addressees).

During this process, any failed bits in the photon series can be attributed to one of the following scenarios: either the sender's photons were not successfully transmitted, or the receiver(s) failed to detect them.

Additionally, this process accounts for all photons emitted by the sender for transmission, even those that were not correctly selected by the receiver.

As part of the complete sifting process, a sift response is executed, resulting in removing the redundant symbols and retaining only the useful ones in order to help optimize memory usage within the database.

2) Error Detection and Correction: During this phase, both the sender and receiver gather all error bits that have been identified.

Those error bits encompass all the sifted bits, as well as any bits that were incorrectly shared between the users. The

objective is to ensure that all of the involved users share identical collections of error-corrected bits.

An error bit is defined as a bit sent by the sender as a 1 but received by the receiver as a 0, or vice versa. This discrepancy can occur due to various factors, such as distortion, noise and so on. Additionally, it could be a result of eavesdropping attempts by an unauthorized party.

Therefore, error detection and correction play a crucial role in mitigating the risk of eavesdropping and ensuring the integrity and security of the QKD process.

By identifying and correcting errors, QKD becomes less susceptible to interferences and more resilient against any potential security threats.

3) Privacy Amplification: In this phase, both the sender and receiver take measures to mitigate the impact of any information that may have been intercepted by a potential eavesdropper. When he attempts to observe data from the stream of photons, their state will surely get altered, hence modifying or, in the worst case, destroying the transmitted data.

To counteract this threat, either party initiates a process known as advantage distillation. In this process, a linear hash function in the Galois Field GF[2n] is utilized to produce values that are multiples of 32, representing the input bits.

Subsequently, the initiating party has four options for transmitting information to the other party:

- shortend bits.
- primitive polynomial of the function.
- input bits as a multiplier.
- an extra bit polynomial to be added to the product.

Both parts then execute the hashing process, and the resulting number of bits retrieved is utilized to perform privacy amplification. This process helps enhance the security of the communication by reducing the potential impact of any information that may have been compromised due to eavesdropping.

4) Authentication: In this final process, both the sender and receiver are safeguarded against Man-In-The-Middle (MITM) attacks, a type of cyber threat where a malicious user intercepts and, possibly, alters communication between the two actual users. MITM attacks pose a significant risk to data security, as the attacker can simulate to be either the sender or the receiver, potentially compromising the confidentiality of the transmitted information.

To mitigate this threat, an authentication process is employed to verify that the real sender is indeed transmitting data to the real addressee and that the receiver is receiving data from a trusted and authenticated source. A proposed, common solution uses families of hash functions to establish the users' authenticity before transferring confidential information.

In this process, both the sender and receiver possess a secret key before initiating communication. This is used to randomly select a hash function from the family of hash functions, which is then employed to authenticate their identities.

Using hashing techniques makes it highly improbable for an unauthorized entity to act as either the sender or receiver and manipulate sensitive information.

Although the secret key is not reusable, a single verified communication session can authenticate many QKD bits. Some of those authenticated bits can be eventually adopted as a secret key, thereby mitigating the non-reusability limitation of the original secret key.

As a result, it becomes virtually impossible for an eavesdropper to impersonate any of the real users, enhancing the overall security of the communication process.

5) Conclusions: Quantum cryptography leverages the principles of quantum mechanics to execute cryptographic operations, with QKD emerging as its most developed application and already embraced in the market.

By exploiting the quantum mechanics properties, those systems enable two distant parts to generate an unlimited supply of secure symmetric keys, ideally suited for OTP applications.

Despite its promise, QKD systems encounter numerous technical limits and face challenges in gaining widespread acceptance.

For instance, to effectively utilize OTP encryption, QKD systems must adhere to stringent keying criteria to ensure the promised level of security. This entails generating symmetric keys that match the length of the message to be encrypted, ensuring they are never reused, and guaranteeing their true randomness.

Furthermore, QKD implementations typically operate as point-to-point solutions, featuring relatively modest key-generation rates. Moreover, many commercial QKD lack formal security certifications, potentially raising user concerns regarding their reliability and trustworthiness.

C. Protocol BB84

We previously saw how protocols based on QKD should be implemented, and we also called in which cases it might be better to exploit one of the various protocols instead of the others. In this paragraph, we will discuss detailedly about the BB84 protocol, since it is adapted in most of the existing QKD systems Moreover, it is common that various fields are trying to integrate QKD systems that are based specifically on BB84. Examples of them are Cloud Computing in which a nowadays theoretical system, CloudQKD [7], and IoT systems, with a look on how it can be adapter for future 6G systems [3].

1) Introduction: The BB84 protocol is a technique used to securely transmit private keys between users, leveraging principles of quantum mechanics to eliminate the possibility of tampering, as dictated by the Heisenberg Uncertainty Principle. It can be considered the most important protocol when comes to Quantum Key Exchange.

One practical application of this protocol is in the secure sharing of private keys between two parts for the online one-time pad (OTP) generation. The two parts can generate and exchange private keys with high security, ensuring confidentiality and integrity in their communications.

Ongoing efforts to enhance the security and efficiency of quantum key exchange have led to the development of upgraded, improved versions of this protocol, such as the B92 and E91 protocols.

2) Mathematical basis: In order to understand how the BB84 Quantum Key Exchange Protocol operates within a Quantum Computing environment, it is essential to introduce two fundamental operations:

- **Unitary transformations**: these transformations preserve energy and are reversible.
- **Measurements transformations**: these transformations involve the loss of energy and are therefore irreversible.

The BB84 protocol distinguishes between four quantum states to represent information used in communication. These information states are further categorized into two alphabets:

- *Alphabet z* that consists of two quantum states, which are $—0\rangle$ and $—1\rangle$.
- *Alphabet x*: that consists of the two quantum states **(+)** and **(-)**, that are represented as **(+)** = $(0)_x = \frac{1}{\sqrt{2}} * (—0\rangle + —1\rangle)$ and **(-)** = $(1)_x = \frac{1}{\sqrt{2}} * (—0\rangle - —1\rangle)$

The BB84 protocol consists of two primary stages:

1) Communication process over the Quantum Channel
2) Process of communicating through the Public Channel. The transmission process is divided into four phases:
   a) *Raw Key Generation*: a phase that removes the position of the error bits (This phase involves the generation of a raw cryptographic key by both parties). Here, any potential error introduced during transmission, including the positions of error bits and the bits at those positions, is identified and removed.
   b) *Error evaluation*: In this phase, both parts evaluate the errors that occurred during the transmission of the raw key. This evaluation helps ensure the accuracy and integrity of the key.
   c) *Synchronization*: The synchronization phase ensures that the users synchronize their cryptographic systems and agree on the final key to be used for encryption and decryption.
   d) *Privacy Amplification*: This final phase involves further enhancing the security of the key by applying privacy amplification techniques. These techniques help mitigate the impact of any potential information leakage or eavesdropping attempts.

3) Communication: Quantum key exchange takes advantage of the quantum mechanics principle to secure cryptographic key transmission. The process involves the exchange of quantum states between the communicating parts, as illustrated in Figure 5. This exchange is facilitated through the adoption of Quantum Superposition (i.e., quantum particles can exist in multiple states simultaneously) and Quantum Entanglement.

The communicating parts exploit those properties to detect any attempted eavesdropping. By encoding information in quantum states and transmitting it over quantum channels, it is easy to detect the presence of a third, malicious part attempting to intercept the communication.

This mechanism relies on the Heisenberg principle that, as previously discussed, dictate that any attempt to observe a quantum state will inevitably disturb it. Thus, if a third party tries to intercept the communication by measuring the quantum states, his actions will inevitably alter the states, making any analysis irrelevant to his purposes.

If the level of eavesdropping is considered to be acceptable, meaning that the disturbance introduced by the eavesdropper falls below a certain threshold, the parties can proceed to generate a secure cryptographic key. This key is guaranteed to be secure against interception by anyone not in possess of the proper quantum information.

However, if the level of eavesdropping exceeds the acceptable threshold, indicating a significant risk of compromise, the parties abort the key exchange process. This ensures that the communication remains secure, as a compromised key could potentially mean an interception of sensitive information [15].

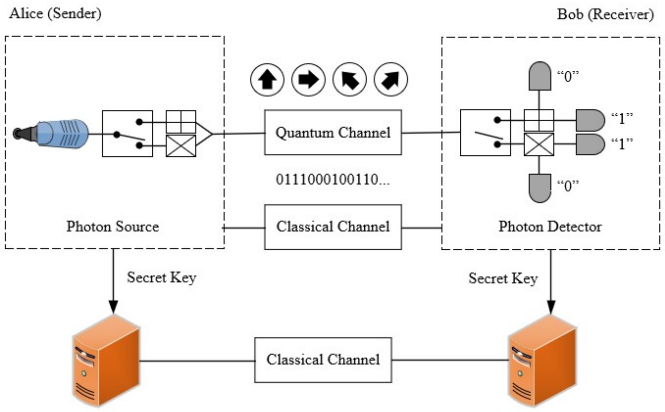

Fig. 5. Quantum Key Exchange [1]

V. Quantum Key Distribution Network (QKDN)

QKDN are networks that consist of nodes (QKD nodes) connected through direct point-to-point connections or intermediate nodes within more complex topologies [11]. Its development is strongly based on the BB84 application [2].

In a QKDN, the quantum and classical channels constitute the physical connection layer, also known as the quantum layer. However, QKDNs require a well-defined functional and organizational architecture to provide secret keys in various contexts. The next paragraph will illustrate the recommended architecture based on International Telecommunication Union – Telecommunication Standardization Bureau, that covers various aspects (describing the architecture and functions, addressing their security concerns etc.). According to those recommendations, QKDNs should have a six-layered structure [13].

Furthermore, to address the limitations inherent in point-to-point connections, QKDNs must incorporate key forwarding functionality facilitated by trusted intermediate nodes.

However, this expanded functionality, along with integrating QKDNs with application-level networks, introduces various security threats that can affect different components of the QKDN.

Many of these threats primarily target the confidentiality and authenticity of key material and necessitate the implementation of appropriate cryptographic mechanisms for mitigation. While encryption schemes. such as the OTP and authentication schemes, offer IT security; their exclusive adoption in a QKDN could ensure its security, providing that QKD devices are securely implemented and operated.

However, these mechanisms may face challenges related to performance and functionality, particularly in meeting the diverse requirements of modern computerized applications.

The practical realization of IT-secure QKDNs is adversely affected by several circumstances, including:

- **Bandwidth Constraints**: limitations imposed by IT-secure encryption schemes and the physics of photonic transmission restrict the bandwidth of a QKDN when employing an OTP-like cipher.
- **Authentication Requirements**: commercial network use cases often involve scenarios where the sender and receiver can share a key without requiring a prebuilt channel. However, IT-secure authentication schemes typically necessitate a short pre-shared secret key.

Indeed, while QKDNs facilitate the distribution of secret keys for encrypting messages using symmetric ciphers, modern cryptography offers a much broader range of capabilities. This includes achieving various advanced features.

A. QKDN Architecture

Currently, as mentioned before, the International Telecommunication Union – Telecommunication Standardization Bureau (ITU-T) is working on defining recommendations for QKDNs. These recommendations cover aspects related to describing the architecture and functions of these networks, as well as addressing their security concerns.

According to these recommendations, QKDNs typically have a six-layered structure, as illustrated in Figure 6 and based on informations collected from *The Rise of Quantum Information and Communication Technologies* [13].

1) Quantum Layer: The level in which secure symmetrical key is established. Here, each pair of QKD modules connected by a QKD link generates symmetric random bit strings.

Each QKD module pushes the (random) bit strings up to a key manager in the same node and send QKD link parameters (e.g., quantum bit error rates—QBERs, etc.) to the QKDN manager.

A QKD Link is a *logical connection between two remote QKD nodes connected by both a quantum channel used for transmitting photons and a public channel used for post-processing the exchanged information, respectively* [14].

Each pair of QKD modules connected by a QKD link generates symmetric random bit strings in its own way. Each QKD module pushes the random bit strings up to a key manager that is in the same QKD node. Each QKD module

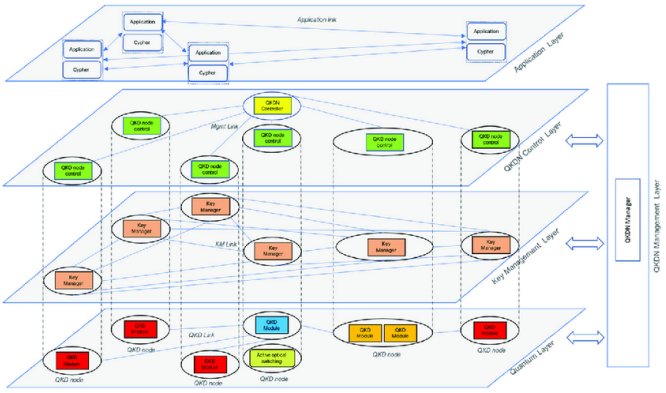

Fig. 6. QKDN 6-layer architecture [13]

can also send QKD link parameters (e.g., quantum bit error rates—QBERs, etc.) directly to the QKDN manager layer.

The disadvantage is the limited quantum channel key generation rate, available to the parties connected by a direct optical fiber or free line-of-sight in a point-to-point (P2P) manner over a certain distance

Moreover, it is necessary to secure key generation. Although fiber is commonly used for transmitting qubits, the installation of dedicated channels for QKD purposes is not practical in all situations.

A free space link is sometimes convenient, although it has its drawbacks since it needs lots of specific external suitable conditions like a visible light path, an acceptable signal-to-noise ratio (SNR) to limit usage time, and so on.

The QKD Link can be designated "currently unavailable" when no available key material in key storage is found, as no cryptographic operations can be performed.

2) Key Management Layer: This layer includes both Key Managers (KMs) and their related links (KM links). Each KM is located in a QKD node.

The KM, connected to each other via KM links, is used to performs key management. Specifically, KM receives random bit strings from the various module(s) located in the same QKD node. The KM synchronizes and re-formats these bit strings and stores them as keys in the storage.

The KM first receives key requests from a cryptographic application, acquires the necessary number of keys from storage, synchronizes and authenticates the acquired keys using a KM link, and supplies them in a format coherent with the cryptographic application. If KMs do not have direct links between them, they should share the necessary number of keys via key relay.

KMs, then, ask the QKDN controller(s) about a proper relay route to use for transfer the keys and finally supplies them to the cryptographic applications.

3) Control Layer: In this layer, control functions are designed in order to control QKDN resources to ensure secure and stable QKDN operations.

QKDN control functions are provided by QKDN Controller(s).

From the various, different functions that can be listed, they should include:

- The key's control relay routes, including rerouting (handle cases when a failure or eavesdropping occurs) between the two end points of the cryptographic application, which require the key
- KMs and KM links control
- QKD modules and QKD links controls
- Authentication and authorization control
- Quality of service and charging policy control

4) Application Layer: Here, QKDN manager monitors and manages the whole QKDN system. The application layer manages different information about QKD modules and links performances in the lower layers. Moreover, the manager interacts with the controller aiming to support the management and control functions of the QKDN.

Here, the main functions found are:

- Fault, accounting, configuration, performance and security (FCAPS) management
- QKDN monitoring
- Support of key life cycle management in KM
- Authentication and authorization management
- Quality of service and charging management

B. QKDN types

This section aims to give a detailed look at the current QKDN technologies that are adopted.

1) Switched QKD Networks: Switched QKDNs consist of nodes connected to a dedicated optical network containing a switching mechanism to establish a direct optical point-to-point QKD connection between any two nodes in the network.

The limitations on distance in point-to-point QKD links restrict these networks to a metropolitan or regional scale. Since every optical switch adds at least several dB of loss to the photonic path, optical switches can significantly reduce a network's range.

The main drawback of switched QKD networks is the requirement of dedicated optical infrastructure for quantum channels, which is often not economically feasible. By contrast, the major advantage of this class of networks is the reliance on an optical switch that allows establishing a connection between two nodes without the active participation of other network nodes.

Another drawback of switched QKD networks is the consistency of the applied QKD technique. Combining different QKD techniques, such as free-space QKD and QKD over fiber, is not possible since no suitable devices that could perform this transformation in the path are available.

2) Security with Trusted Repeater QKDNs: In trusted repeater QKD networks, the security of each node along the transmission path is essential for securely transmitting information. Point-to-point communication between two nodes provides the same key to the nodes, hence enabling secure communication.

Considering the lack of a quantum repeater, nodes are also responsible for routing and forwarding mechanisms. Since the transfer security depends on the security of all the nodes involved in the path, this organization guarantees important advantages.

On the other hand, trusted repeater networks are not limited by distance or node numbers and can be made up of different QKD devices implementing different technologies.

3) Security without Trusted Repeaters: Since the quantum channels can be "given" to the eavesdropper without compromising the QKD security, an ideal attacker would rather target the weaker link, the node. The usual assumption is letting the nodes be our trusted element. This assumption can converge in at least three ways:

- use measurement device independent (MDI) QKD, which is inherently immune to all side-channel attacks targeting the measurement device, usually the most vulnerable part in a QKD system. [5];
- use quantum repeaters;
- relies on multiple paths.

This first and most common approach, which will be described next, considers the second assumption of perfect state preparation achievable by communication parties, although adding a potentially untrusted location to the quantum channel.

The idea behind the second approach, quantum repeaters, is to employ quantum entanglement of photons to communicate over different quantum links.

To recall, with quantum entanglement, we refer to the property that multiple particles are connected together in such a manner that the measurement of one particle's quantum state determines the other particles' possible quantum states. Entanglement fidelity is a property used to describe how well the entanglement between two subsystems is preserved in a quantum process.

The third (and most practical) method resorts to classic technology and employs multiple paths and threshold cryptographic techniques to mitigate the risk of eavesdropping.

Multipath transmission trusts the repeaters for the assumption that the repeater is vulnerable to eavesdropping; the attacker gets forced to intercept many of the intermediate devices to discover the message.

Indeed, it can be shown that, without the "trusted" repeaters, multiple paths are theoretically necessary. Moreover, path redundancy mitigates the problem that all QKD implementations are vulnerable to denial-of-service attacks.

4) QKD Overlay Networks: While the previously described QKDN types relay to the quantum channel organization, the QKD Overlay Network type refers to public channel realization.

The Overlay Network's main purpose is to achieve the higher hierarchy network to provide a better quality of service and use the resources of lower-level networks.

To do so, the overlay network aims to be independent of the paths defined by the known Internet Service Providers (ISP). Finding alternative routes that can provide a service with higher quality degrees and quick rerouting because of interrupt detection or multipath communications are key features of the overlay network approach. Using multipath connections is

often suggested to improve network workloads by protecting against different potential limitations such as network failures and large bandwidth implementation.

The overlay network can help overcome these challenges by establishing the network with a P2P approach. The overlay network connects nodes in different domains and allows the usage of alternative paths by encapsulating traffic in the lower network. When an intermediate node receives the packet, it will be unpacked, and the receiver's IP address is analyzed, re-encapsulated, and forwarded to network nodes that may be in other domains.

Considering the encapsulation principle, overlay nodes can independently perform link state measurements and guarantee fast responses to link congestion by redirecting traffic to other less-congested links. Overlay networks can offer new functionality that is difficult to perform in the lower-layer networks.

VI. Main challenges

A. Accuracy

The two communicating parts must verify that the keys are identical, as even a minimal noise could cause serious issues during data transmission.

To ensure accuracy without revealing the specific bits obtained, the parts can examine the parity (i.e., the remainder when the sum is divided by two). This operation can be performed publicly while keeping individual components secret.

In case groups exhibit inconsistencies, they are either rejected or divided in smaller groups, discarding or correcting at least one of them. After a proper number of repetitions, this procedure ensures that the keys are likely to be considered similar.

This process underscores the importance of precision and security in the cryptographic process [8].

B. Security

The reliance of Quantum Cryptography on quantum physical principles renders it inherently more secure than classical cryptography.

Quantum mechanics enables the transmission of cryptographic keys across highly secure channels, offering a level of security unmatched by traditional methods. The exchanged keys are unique and randomly generated, minimizing the risk of interception by any possible cyber-attacker.

Additionally, during the key exchange process, polarization states are measured by both parts, resulting in the rejection of half of the bits. Furthermore, an error-correcting algorithm is employed to detect eavesdropping attempts and facilitate key regeneration.

As a result, the primary challenge faced by the system is preventing malicious users from intercepting the secret key during the exchange, a highly improbable scenario.

We'll see that QKD does not transmit the message but can produce and distribute keys used to encrypt and decrypt the message transmitted over a standard channel [8].

C. Limitations

Here are described the main properties and limitations that affect Quantum Cryptography's limitation. All those informations are based on the paper *An exploration to the quantum cryptography technology* [8].

1) Intensity of Light: The process of producing the desired polarized photons involves refining a flash source, such as a laser or a Light-Emitting Diode (LED), to ensure that each pulse consists of a single photon.

However, there are limits and challenges to consider when developing the system. In fact, if the pulse intensity is too low, it may be imperceptible to the receiver, while an excessive intensity might make the polarity of the photon discretely identified, allowing a sleuth to read the photon from a beam concerning both the bases without any notable variance in a flash [8].

Both aspects – intensity and polarity – are crucial, and finding the correct balance between them is important.

2) Time: In a cryptosystem based on Quantum Cryptography, the principle that the polarization of light or a photon particle can only be determined at the time of measurement is crucial in thwarting attempts at interception and eavesdropping [8].

D. QKDN Requirements

As stated as a starting point for this analysis, QKD has shown to be more common than Quantum-Resistance Algorithms, and most of the research results provided detailed studies related to QKD rather than post-Quantum cryptography.

However, QKD networks must be integrated into theexisting environment and need to meet certain criteria and conditions. Some of the most common requirements from QKD networks are listed below and based on the papers *Practical challenges in quantum key distribution* [5] and *QuantumKeyDistribution: A Networking Perspective* [14].

1) Key rate: One of the main parameters used to evaluate a QKD network is the average key rate of a QKD link.

Since encryption and decryption operations cannot be performed without sufficient key material, the competition between the rate at which key material is stored in the key storage and the rate at which it is consumed for encryption and decryption operations has an important influence on network performance.

Encryption keys generated by QKD can be used in a symmetric cipher scheme (such as AES, which is quantum resistant) for enhanced security, or combined with OTP encryption scheme for unconditional security. In both cases, it will be achieved higher secure rates, that allows for more frequent updates of encryption keys and proportional increase in the OTP communication bandwidth as this scheme requires the key to be as long as the message.

The obtained key rate depends crucially on the performance of the detectors used. For QKD systems employing single-photon detection techniques, high efficiency and short dead time of the detectors are essential for reaching a high bit rate.

2) Extended distances: The fundamental constraint of a QKD link is the length over which secure key material can be generated (due to various factors, such as scattering and absorption of polarized photons), which limits the ability of quantum channels (direct optical links or free line-of-sight) to a certain distance. Enlarging the communication range is another key aspect for technological.

QKD systems based on single-photon detection champion the point-to-point communication distance.

Quantum Key Distribution (QKD) systems transmitting over optical fiber lines face significant distance limitations compared to standard optical communication systems due to photon properties [8].

To overcome these limitations, researchers are exploring the concept of *quantum repeaters*, designed based on one of the two approaches: quantum error correction techniques or entanglement.

E. Key material protection

Nodes of a QKD network must be secured with a strong probability that the established key material is unique and inaccessible to third malicious users. Key material security is evaluated both when it is established and, most importantly, when managed, stored and used.

It is therefore important to secure each level of the QKDN architecture

F. Costs and robustness

Because of costs and limitations on the implementation, QKDN will slowly be integrate in traditional, everyday environments.

It is important then to ensure robustness, reflected in the gradual and seamless addition of new nodes and establishment of new links. QKDN needs to provide adequate replacement paths to avoid defective, weak nodes.

In order for QKD systems to be used in real-world applications, low cost, and high robustness are also necessary to be gained.

A first property to consider is that QKD systems have been shown to coexist with heavy data traffic, eliminating the need for dark fibers, which are known to be both expensive and often unavailable. Access network architecture allows simultaneous access by many QKD users; moreover, they are compatible with full-power Gigabit Passive Optical Network traffic in the same network.

Room-temperature single-photon detectors are suitable for systems whose fiber length can reach 100 km, thus removing cooling requirements for the entire QKD systems, helping to reduce deployment cost as well as system complexity, footprint, and power consumption.

VII. Conclusion

This paper has provided a detailed analysis regarding Quantum Key Distribution, one of the two main approaches on Post-Quantum Cryptography and, as the various researches demonstrated, the most efficient against the advancements in quantum technologies. Here, classical cryptographic techniques are redesigned in order to re-adapt them for being efficient with quantum computers.

Starting from those premises, the discussion went deeply inside the analysis of QKDN, including the architecture analysis and various types of QKDNs typically adopted nowadays.

Also, particular attention has been dedicated to study the main challenges in this fields.Even thought they are, for now, nothing but theoretical studies, it has been shown how it might be possible to adapt QKD protocols, in particular the BB84, with cloud computing and Internet of Things systems.

References

[1] Adnan, M.H., Zukarnain, Z.A., Harun, N.Z.: Quantum key distribution for 5g networks: A review, state of art and future directions. Future Internet (2022)

[2] Adu-Kyere, A., Nigussie, E., Isoaho, J.: Quantum key distribution: Modeling and simulation throughn bb84 protocol using python3. MDPI (2022)

[3] Al-Mohammed, H.A., Yaacoub, E.: On the use of quantum communications for securing iot devices in the 6g era. 2021 IEEE International Conference on Communications Workshops (2021)

[4] Bhatia, P., Sumbaly, R.: Framework for wireless network security using quantum cryptography. International Journal of Computer Networks and Communications (2014)

[5] Diamanti, E., Lo, H.K., Qi, B., Yuan, Z.: Practical challenges in quantum key distribution. njp Quantum Information (2016)

[6] El-Araby, E., Taher, M., Abouellail, M., El-Ghazawi, T., Newby, G.B.: Comparative analysis of high level programming for reconfigurable computers: Methodology and empirical study. Conference Paper (2007)

[7] G.Murali, Prasad, R.: Cloudqkdp: Quantum key distribution protocol for cloud computing. International Conference On Information Communication And Embedded System (2016)

[8] Jasoliya, H., Shah, K.: An exploration to the quantum cryptography technology. 9th International Conference on Computing for Sustainable Global Development (2022)

[9] Kitchenham, B., Brereton, O.P., Budgen, D., Turner, M., Bailey, J., Linkman, S.: Systematic literature reviews in software engineering – a systematic literature review. Information and Software Technology (2008)

[10] Lakshmi, P.S., Murali, G.: Comparison of classical and quantum cryptography using qkd simulator. International Conference on Energy, Communication, Data Analytics and Soft Computing (2017)

[11] Lella, E., Gatto, A., Pazienza, A., Romano, D., Noviello, P., Vitulano, F., Schmid, G.: Cryptography in the quantum era. IEEE 15th Workshop on Low Temperature Electronics (2022)

[12] Mailloux, L.O., II, C.D.L., Riggs, C., Grimaila, M.R.: Post-quantum cryptography. what advancements in quantum computing mean for it professionals. IEEE Computer Society (2016)

[13] Manzalini, A., Artusio, L.: The rise of quantum information and communication technologies. Quantum Reports (2024)

[14] Mehic, M., Niemiec, M., Rass, S., Ma, J., Peev, M., Aguado, A., Martin, V., ansd Andreas Poppe, S.S., Pacher, C., Voznak, M.: Quantumkeydistribution: A networking perspective. ACMComputing Surveys (2020)

[15] Nguyen, T.T., Khac, T.L.V., Luc, N.Q.: Simulation of the bb84 quantum key exchange protocol. 5th International Conference on Knowledge and Systems Engineering (2023)

[16] Nurhadi, A.I., d Nana Rachmana Syambas: Quantum key distribution (qkd) protocols: A survey. 4th International Conference on Wireless and Telematics (2018)

[17] Perez-Pacheco, P., Caballero-Gil, P.: Mceliece cryptosystem: Reducing the key size with qc-ldpc codes. 19th International Conference on the Design of Reliable Communication Networks (2023)

[18] Rieffel, E., Polak, W.: An introduction to quantum computing for non-physicists. ACM Computing Surveys (2000)

[19] Routray, S.K., Jha, M.K., Sharma, L., Nyamangoudar, R., Javali, A., Sarkar, S.: Quantum cryptography for iot: Aperspective. International Conference on IoT and Application (2017)

[20] Singh, G., Singh, A., M, M.S.N.: Quantum cryptography with photon polarization and heisenberg uncertainty principle. 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (2022)
[21] Yavuz, A.A., Nouma, S.E., Hoang, T., Earl, D., Packard, S.: Distributed cyber-infrastructures and artificial intelligence in hybrid post-quantum era. 4th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (2022)
[22] Zapatero, V., van Leent, T., Arnon-Friedman, R., Liu, W.Z., Zhang, Q., Weinfurter, H., Curty, M.: Advances in device-independent quantum key distribution. njp Quantum Information (2023)