IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 October 2024, accepted 15 November 2024, date of publication 22 November 2024, date of current version 9 December 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3504815

SURVEY

Quantum Cryptography for Future Networks Security: A Systematic Review

DURR-E-SHAHWAR[1], MUHAMMAD IMRAN[2], AHMED B. ALTAMIMI[3], WILAYAT KHAN[3], SHARIQ HUSSAIN[1], AND MOHAMMAD ALSAFFAR[4]

[1]Department of Software Engineering, Foundation University Islamabad, Islamabad 44000, Pakistan
[2]National Centre for Physics, Islamabad 44000, Pakistan
[3]Department of Computer Engineering, University of Ha'il, Ha'il 55473, Saudi Arabia
[4]Department of Information and Computer Science, University of Ha'il, Ha'il 55476, Saudi Arabia

Corresponding author: Durr-E-Shahwar (durre.shahwar_se@fui.edu.pk)

This work was supported by the Scientific Research Deanship at the University of Ha'il, Saudi Arabia, under Project RG 23-187.

ABSTRACT Quantum Cryptography (QC) revolutionizes network communication – harnessing principles of quantum mechanics to enable the exchange of encrypted messages – for enabling secure data transmission in an era of quantum information processing. With a significant rise in quantum computing research and development efforts, there is an increasing interest in exploring QC (e.g., Quantum Key Distribution (QKD) and Quantum Secured Encryption (QSE)) against a multitude of security threats in futuristic networks for quantum information processing. The objective of this study is to review the existing research i.e., consolidating the published evidence, that streamlines and documents the predominant challenges, recurring solutions, security threats, and their counter-measures against the outlined research questions in the context of QC. To conduct this study, we followed the guidelines and method of Systematic Literature Reviews (SLRs) to answer seven research questions. These questions investigate the proposed solutions for state-of-the-art QC and its impact on future network security. Based on the seven (7) outlined research questions, this study systematically selected and reviewed one hundred and thirty four (134) research studies published from 2016 to 2023 with a focus on QC for quantum information processing. The results of this SLR establish a knowledge base for modern QC applications to guarantee network security in quantum-enabled network communications. The review reveals that though still in the phase of its inception, the research on QC is progressing rapidly, highlighting the necessity for network protocol and frameworks to cater for quantum network security. The SLR also highlights the challenges encountered while designing or implementing the QC systems, pinpointing the significance of keeping abreast of QKD networks and addressing possible ramifications for internet security in the future. The SLR provides theoretical foundations and evidence-based guidelines to tackle emerging and futuristic challenges of security in the context of QC and QKD for quantum information processing.

INDEX TERMS Quantum cryptography, systematic literature review, quantum computing, cryptographic protocols, quantum key distribution.

I. INTRODUCTION

In the current era, network security plays a pivotal role in safeguarding information transmitted over various communication channels. With the proliferation of digital data and the increasing sophistication of cyber threats, traditional cryptographic methods face significant challenges in providing robust protection. Classical encryption techniques were used (and are still in use) to encrypt data in the earlier eras [1]. Classical cryptography, usually referred to as conventional cryptography, is the umbrella term encompassing the encryption and decryption methods that have been extensively employed for protecting information and communication networks for many years. It uses mathematical formulas

The associate editor coordinating the review of this manuscript and approving it for publication was Alessio Giorgetti.

and keys to convert plaintext (the original communication) into ciphertext (the encrypted message) and the other way around. Initially, classical cryptography primarily focused on securing communication. However, with the advent of modern cryptography, its scope has broadened significantly. Presently, modern cryptography addresses a large number of applications, including digital signatures, digital currency, secure voting systems, and more. The security of conventional cryptographic algorithms relies on mathematical problems like factorization of large numbers and discrete logarithms but quantum computers can break this [2]. With adequate computational power on a quantum computer implementing Shor's algorithm [3], all these math problems can be easily solved. Quantum computers are computational devices that leverage principles of quantum mechanics to tackle complex mathematical challenges that are difficult or computationally infeasible for classical computers to solve [4]. If high-capacity quantum computers are ever developed, many of the current cryptosystems will become susceptible to cracking. Quantum computers are a great danger to modern cryptography that pose a serious threat to the confidentiality and integrity of communications within networks [5].

A. RESEARCH CONTEXT - CONVENTIONAL CRYPTOGRAPHY SCHEMES AND THEIR LIMITATIONS IN NETWORKS

Conventional cryptography schemes can be generally classified into two categories namely, the symmetric and asymmetric cryptography. The same key is used for encryption and decryption in symmetric cryptography [1]. It uses algorithms like Advanced Encryption Standard (AES) [6], the Rivest Cypher (RC) [7], and Data Encryption Standard (DES) [6]. The confidentiality of the key determines the security of the symmetric key cryptography. The ciphertext can be decrypted by an attacker if the key is compromised. A pair of keys i.e., a combination of public key and a private key, are used in asymmetric key cryptography. The private key is kept confidential and is used for decryption, while the public key is used for encryption. Digital signatures and safe key exchange are made possible by asymmetric key cryptography. Elliptic Curve Cryptography (ECC) [8] and Rivest-Shamir-Adleman (RSA) [9] are popular public key algorithms. Symmetric key encryption surpasses asymmetric key cryptography in efficiently encrypting large data volumes due to its faster processing speed and lower computational overhead [5], [10]. On the other hand, key distribution is the major problem in symmetric encryption. To achieve a balance of security and usability, a combination of symmetric and asymmetric encryption is used in the current era. Asymmetric key cryptography is used for symmetric key exchange and once the key is exchanged safely then the symmetric key is used for encryption/decryption for the rest of the communication between sending and receiving entities. Quantum computer attacks are a threat to conventional cryptography, with the potential to compromise widely used cryptographic methods like RSA and ECC. The security of the encrypted data is now seriously threatened by quantum computer attacks. Securely sharing the secret key between the two communication parties is one of the main issues in conventional cryptography, in particular, in large-scale systems. Updating and managing keys securely is difficult, especially when there are many people or devices involved. As the number of keys grows, the danger of key compromise and unauthorized access rises. Over time, the security of traditional cryptography may deteriorate if new algorithms or attack methods are developed. To fend off changing threats, it needs constant upgrades and enhancements. Symmetric key cryptography puts all the past and future communications encrypted with the secret key at risk if it is compromised. Conventional encryption does not, by default, offer perfect forward secrecy which assures that the loss of long-term keys will not preserve the confidentiality of previous conversations [5].

Table 1, which was modified from the National Institute of Standards and Technology (NIST) [3], displays how quantum computing would affect current cryptography techniques. NIST predicts that by increasing the key size twice would be sufficient to ensure security of symmetric key systems in quantum era [3]. Additionally, research has shown that it is not possible to accelerate search algorithms exponentially [5]. As mentioned above, the security of public key cryptography schemes depends on complex mathematical problems that can be solved by quantum computers [5]. These drawbacks of the existing key encryption schemes have led researchers, academics, and professionals to consider alternate strategies [11]. Post Quantum Cryptography is also considered as a solution to this problem [5], [12]. NIST report on Post Quantum Cryptography shows that in the context of a quantum age, symmetric algorithms and hash functions should continue to be feasible and useful [3]. According to Shor's [13] and Grover's [14] algorithms, the mathematical problems which conventional encryption techniques depend on can be solved by future quantum computers as a result the existing public key encryption systems will become obsolete [11]. NIST recommends increasing key sizes to mitigate the impact of large-scale quantum computers on conventional encryption algorithms [3], [11]. Quantum cryptography is also considered as a solution for secure network communications in quantum era [11]. By utilizing the foundational ideas of quantum cryptography (QC), the maximum level of communication security in quantum era is reasonably guaranteed [11]. It is important to distinguish between post-quantum cryptography and quantum cryptography, quantum cryptography uses the concepts of quantum mechanics to create a secure communication channel [3], [11]. By switching to QC, it may be possible to get beyond the drawbacks of traditional encryption and address the new problems in network security [15]. This paper's goal is to examine the current state of knowledge about quantum key distribution, quantum cryptography, and

TABLE 1. Analysis of quantum computing on conventional encryption techniques [3].

Encryption Algorithms	Category	Function	Quantum Era Impact
AES-256	Symmetric Key	Encryption	Larger Key Size Needed
SHA-256,SHA-3	Hashing	Hash Function	Larger 0utput Needed
RSA	Public Key	DS, Key Establishment	Not Secure
EEC	Public Key	DS, Key Exchange	Not Secure
DSA	Public Key	DS, Key Exchange	Not Secure

quantum communication, including their constituent parts, applications, and recent developments.

B. QUANTUM CRYPTOGRAPHY IN THE ERA OF QUANTUM INFORMATION PROCESSING

QC is an emerging field that utilizes the ideas of quantum physics to increase the security of cryptographic protocols rapidly. QC achieves unparalleled levels of security by making use of basic aspects of quantum mechanics as opposed to traditional encryption which is based on mathematical algorithms and keys. QC provides special benefits that might revolutionize network security by taking advantage of quantum events. During the early 1970s, As mentioned in [16] Stephen Wiesner [17] was the pioneer who introduced the concept of QC. Quantum cryptography [18] is founded upon the basic principle of quantum physics, specifically Heisenberg's uncertainty principle [16]. This principle serves as the basis for the concept of QC. By leveraging quantum phenomena, such as QKD and quantum-resistant encryption algorithms, QC offers enhanced security features that are resistant to attacks based on computational power [19].

C. THE NEEDS, FOCUS, AND CONTRIBUTIONS OF THE SYSTEMATIC LITERATURE REVIEW

Despite all the research work in the subject of QC, there are still some issues and challenges related to its development and implementation. These issues include quantum channel noise, security and resilience of the quantum devices, protocol distance limitations, practical implementation complexity, and so on [20]. In this study, the research done in the field of QC along with the challenges it faces and how researchers hope to enhance the reliability, scalability, and applicability of QC for future networks are discussed.

1) RESEARCH PROBLEM

Development in quantum technology has made QC a viable method for boosting network security. However, making the transition from classical to quantum encryption presents several difficulties and needs considerable thought. To thoroughly assess the existing level of knowledge, surrounding the process of switching from conventional to QC for future network security, is the research challenge addressed in this literature review. The primary objective of this research is to *'investigate the published literature - i.e., conduct evidence-based findings via the SLR - to consolidate existing research and document the predominant challenges, recurring solutions, security threats, and their counter-measures in the context of QC'*.

2) RESEARCH CONTRIBUTIONS

In a Systematic Literature Review, secondary data are gathered, research studies are critically reviewed, and qualitative or quantitative conclusions are synthesized. As QC is an emerging field and considerable research work is underway in this area, there is a need for a comprehensive and up-to-date systematic literature review that discusses the development in the field of QC over the past few years. This SLR focuses on quantum cryptography as a means to enhance future network security. With the growing threats to information transmission and the limitations of classical cryptographic methods, QC has appeared as a viable candidate. We outlined 7 research questions and reviewed 134 research studies as proposed solutions of QC to document this SLR. The primary focus and main contributions of this SLR are to document:

- *Applications of QC in Networks:* Based on a synoptical view of quantum cryptography solution, the SLR highlights the application domains of QC in computer networks.
- *Principles of QC in Networks:* Exploring the principles and techniques that are being used to implement QC.
- *Challenges of QC in Networks:* Identify and streamline the predominant challenges and issues in the implementation of QC.
- *Strategies of QC in Networks:* Explore the strategies and approaches that exploit QC to enhance network security.
- *State-of-Research on QC in Networks:* Assess the current state of research on QC, its potential, and limitations in real-world network security.

By achieving these goals, this literature review will offer insightful information about the process of switching from conventional to QC, giving data scientists, researchers, and practitioners thorough information on the state-of-the-art knowledge, difficulties, and potential solutions for enhancing network security in the future [21].

D. PAPER ORGANIZATION

The structure of this paper comprises several sections that guide the reader through the research process and findings. Section II provides research context in terms of the principal concepts in QC. Section III serves as a brief description of the related work, offering an overview of the existing literature and studies relevant to the subject

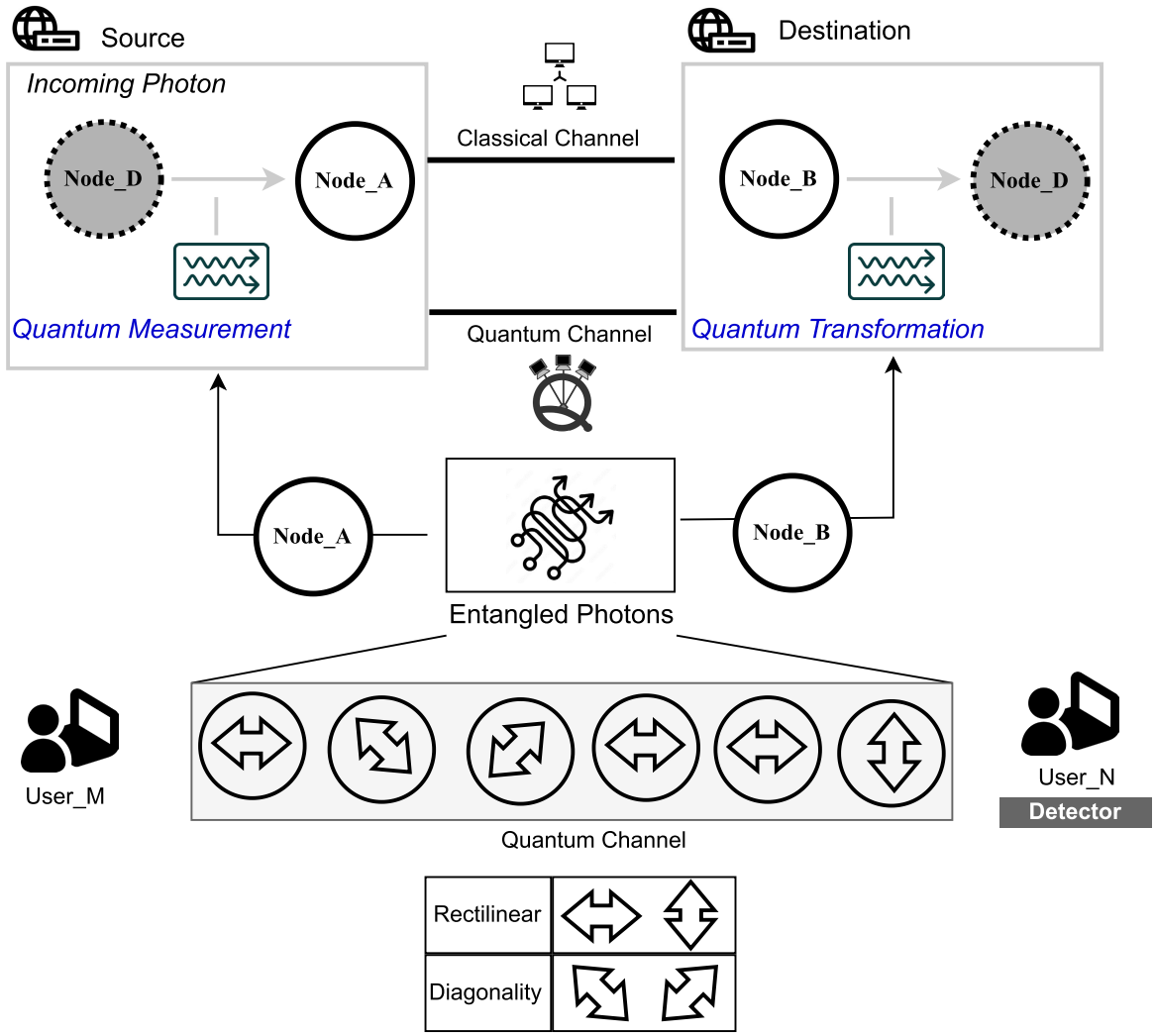


FIGURE 1. Overview of classical and quantum communication channel.

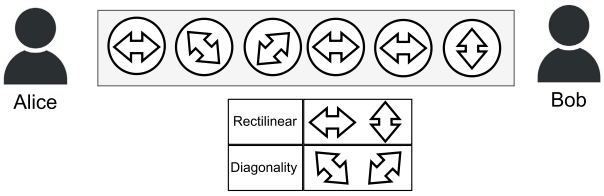


FIGURE 2. A scenario of the quantum coin flipping.

matter. It provides a foundation for the current research by exploring the work that has been previously conducted in the field. Section IV describes the research method to perform the SLR study. The methodology section helps to establish the credibility and rigor of the research by explaining the procedures and tools employed. Section V of the paper is dedicated to the discussion and presentation of the results and offers a comprehensive analysis of the findings obtained from the research. This section aims to describe a detailed understanding of the research outcomes and their significance within the broader context of the study. Concerns about internal, external, concept, and conclusion validity are discussed in Section VI along with other possible threats to the study's validity. Section VII concludes the paper with a synopsis of the SLR and highlights the key findings of the study.

II. RESEARCH CONTEXT

This section contextualizes the technical details of QC and quantum networks that are visually illustrated using Figure 1 and Figure 2.

A. PRELIMINARIES

In this section, key concepts in QC are discussed which includes quantum entanglement, quantum measurement, and quantum teleportation [22]. In a quantum system as shown in

Figure 1, the traditional methods of duplicating or moving data from one point to another are impractical because quantum bits (basic unit of quantum information) cannot fully capture the state information at the destination due to the limited coherence times in quantum states. Quantum teleportation is employed to transmit quantum information between different systems as an alternative approach. Quantum mechanics is best described as the following.

- In the quantum world, a phenomenon known as quantum entanglement [22] takes place when two minuscule particles that share a source interact. No matter how far apart they may be physically, when the state of one particle changes, the state of the other particle also instantly changes in a connected way.
- We may retrieve information that is encoded in a quantum state using a fundamental procedure known as quantum measurement [22]. It is a dynamic process that can discriminate between several quantum states and record how these states change over time. Since measurement directly affects how quantum states are manipulated, quantum measurement and state development are related.
- Through the use of their mutual entanglement, quantum teleportation entails sending unknowable quantum information to a faraway light quantum. The quantum information is not physically transported, but rather stays on its original physical carrier.

B. QKD PROTOCOLS

Two disciplines of photon behavior can generally be used to classify quantum key distribution protocols: the first one is based on superposition states (orthogonal/nonorthogonal), and the second one is based on entangled states [23], [24]. According to the size of the source code space, conventional QKD protocols may be classified into two classes with respect to discrete and continuous variables. These protocols may further be classified into two classes: prepare-and-measure protocols and entanglement-based protocols, depending on whether or not the entanglement is present in the light source. The details about these protocols can be found in [22] and [25]. A thorough review of many QKD protocols is provided by the authors in the study [23], [24], [26], [27].

C. QUANTUM COIN FLIPPING

A procedure, called quantum coin flipping [28], was created for two parties who don't trust each other. Quantum coin flipping includes communication over a quantum channel where qubits are communicated between the parties, in contrast to the QKD which focuses on the safe key exchange. Due to their shared skepticism of one another, the two parties Alice and Bob expect each other to act dishonestly. As a result, further precautions must be taken to guarantee that neither Alice nor Bob can use the protocol to their advantage and get the result they want. Bias is the term for the manipulation or influence over a certain outcome. A lot of effort is put into designing methods that decrease the bias of any dishonest participant [29]. Figure 2 illustrates the information exchange between Alice and Bob through quantum coin flipping.

D. QUANTUM BIT COMMITMENT

Quantum commitment protocols are used in cases when there is a lack of confidence between the parties in addition to quantum coin-flipping. A commitment scheme ensures that the receiver, Bob, stays unaware of the value until Alice decides to divulge it. It enables one person, Alice, to securely bind a particular value without the ability to change it (i.e., ''commit''). This protocol ensures the consistency of the committed value and maintains the information's secrecy up to the reveal phase [29].

E. DEVICE INDEPENDENT QUANTUM CRYPTOGRAPHY

When a QC system's security is not reliant on the reliability or honesty of the quantum devices it uses, then protocol are termed as device-independent. This implies that even in cases where the devices may be flawed or purposefully exploited by malevolent people, the protocol is still safe. To ensure the protocol's resistance to such threats, a variety of conceivable situations involving flawed or dishonest devices are taken into consideration in the study of device-independent protocols. Device-independent quantum cryptographic methods provide a greater degree of security by removing the dependency on device trustworthiness, making them appropriate for situations where the integrity of the devices cannot be guaranteed [29]. Recently, in a research work [30], a fully device-independent QKD scheme is proposed.

F. QUANTUM AUTHENTICATION PROTOCOLS

QC has a branch called quantum authentication that focuses on securely verifying the identities of communication parties. Quantum authentication is sometimes known as quantum authentication protocols or quantum authentication methods. Verifying an entity's stated identity and making sure it is who it says it, is the process of authentication. Quantum identity authentication and quantum digital signatures are two schemes used in quantum authentication. Over conventional communication techniques, quantum communication protocols provide considerable security advantages. However, in real-world situations, its actual execution presents difficulties. To fully utilize the potential of these techniques, research on bias reduction and cheating prevention is still active. The foundation of effective quantum communication systems, integration with current network infrastructures, and scalability are only a few of the difficulties that face QC despite its immense promise. QC is still an interesting field for study and development because of the potential benefits, and it might open up new ways to improve future network security.

III. RELATED WORK

A considerable amount of work has been done in the past that highlights the development of QC. Gisin et al. [16] conducted an initial review on QC. Several researchers, including Alleaume et al. [31], Giampouris [32], Diamanti et al. [33], Long [34], Zhou et al. [15], Li, Jian and Kumar [35], Alvarez [10], Na Li [22], Hong [36], and Kaushal Shah [37] conducted review studies on the same subject. In their work, Gisin et al. [16] conducted an initial assessment of the advancements made in, both theoretical and experimental, studies of QKD. Alleaume et al. [31] began their work by conducting a comprehensive review and comparison of various key establishment techniques with a specific focus on QKD. Subsequently, they delve into the examination of two distinct practical scenarios concerning the application of QKD. Throughout their study, the authors analyze the constraints and advantages associated with employing QKD in these specific contexts. Additionally, they provide an overview of the challenges that pertain to the advancement of QKD technology which also present possible areas for further research in the domain of cryptography.

Giampouris [32] presents fundamental definitions and examines significant theoretical progress about the BB84 and E91 QKD protocols. Additionally, it seeks to present an overview of essential advancements in the realm of QKD, specifically associated with the two protocols mentioned above. Diamanti et al. [33] discuss the real-world obstacles encountered in QKD and explore the current strategies being implemented to tackle them. Long [34] provides a concise introduction to the fundamental concepts of Quantum Secure Direct Communication (QSDC), outlines the key protocols, presents the current status, and offers a perspective on the field. Zhou et al. [15] examine the features of QC and investigate its potential benefits in the future Internet. Their analysis primarily revolves around the QKD protocol, exploring its behavior in both noise-free and noisy communication channels to simulate real-world scenarios in the future Internet. Kumar [35] explore various experimental endeavors within the field of QC, analyze different attacks, and address the challenges associated with transitioning from classical to quantum. Alvarez [10] discusses the evolution of QC and explores its practical applications.

Na Li [22] begins by clarifying the definition of QC. It then proceeds to present the current understanding of QC, covering various aspects such as quantum information processing, QC protocols, and potential attacks. Lastly, the paper discusses the challenges and opportunities that lie ahead in this promising field. Hong [36] examines the current trends and addresses the challenges encountered in the QKD. Kaushal Shah [37] conducts an in-depth exploration of QC and QKD, covering their fundamental elements, implementation methodologies, and the latest advancements in the research. Furthermore, it comprehensively analyzes the vulnerabilities and security concerns related with the Internet of Things (IoT) infrastructure, while evaluating the effectiveness of the classical cryptographic algorithms currently in use. B. Harish Goud. [38] encompasses the fundamental terminology and concepts of QC, explores the emerging trends in this field, provides a detailed examination of various QKD protocols, highlights their vulnerabilities, and provides guidance for potential future research areas. Aji [39] examined several modern quantum cryptographic-based networks and simulation frameworks for QKD. Their objective is to perform a comprehensive and methodical assessment of how these experimental platforms and functionalities are implemented. Hasan [40] explored the foundational aspects of quantum communication. This includes an in-depth discussion of its vision, the objectives guiding its design, techniques for processing information, and the various protocols involved.

A detailed and comprehensive overview of quantum cryptography's developments is given by the authors in paper [41], who address satellite difficulties, device independence, and discrete and continuous-variable quantum key distribution methods. They discuss how quantum repeaters can expand private communications beyond their current boundaries. They also go through the uses of quantum cryptography, including digital signatures and random number generators. The writers of [42] went over the basic ideas of quantum mechanics, including entanglement and superposition, which are the cornerstones of quantum computing and cryptography. Additionally, they investigated quantum encryption methods, stressing the potential of post-quantum cryptography and Quantum Key Distribution (QKD) protocols for secure communications in the quantum era. The influence of quantum cryptography on US national security in the context of developing quantum technology is reviewed in study [43]. It investigates how quantum cryptography techniques might be used to produce unbreakable encryption and improve digital security in the future. The examination of reports and literature from 2013 to 2023 is the systematic basis for the analysis. In a recent study [44] authors emphasizes the importance of quantum-safe solutions to protect current data and reviews advances in integrating Quantum Key Distribution, Post-Quantum Cryptography, and classical cryptography to ensure secure key exchange in the face of future quantum threats.

These surveys have offered a range of point of views on QKD technologies for future internet security. However, our paper aims to complement these surveys by providing an updated overview of recent developments in quantum networks, field trials, and demonstrations that have emerged since these publications. Furthermore, like the methodology in [43], we employed systematic literature review techniques to perform our survey. Nevertheless, our analysis addresses quantum cryptography's worldwide implications, whereas [43] concentrated on how it can affect US national security in the context of developing quantum technology. Most of them have not addressed the specific topic of QKD networks and applications of quantum cryptography.

The exploration of QKD networks and its applications as a critical dimension in the realm of QC for ensuring secure communication over the internet are also explored in this SLR. Our emphasis is on Quantum Communication within the broader context of quantum cryptography.

A. NEEDS FOR THIS SLR

With the increasing potency of quantum computers, they pose a substantial risk to the security of traditional cryptographic systems. So, there is a dire need to explore and understand the potential of QC as a solution to address these emerging security challenges. In contrast to prior survey papers, this SLR comprehensively covers the details of QC, encompassing protocols, techniques, implementations, QKD networks, threats, attacks, current advances, limitations, and future directions. To the best of our knowledge, this survey stands as the first comprehensive and up-to-date SLR of quantum cryptography, making it unique in the existing literature. Role of QC to implement network security is also highlighted in this paper. Examining the current level of knowledge about quantum key distribution, quantum cryptography, and quantum communication as well as their constituent elements, uses, and latest advancements is the aim of the SLR. This survey serves as a valuable resource for the researchers, offering insights into the application and understanding of existing protocols, current research trends, and exploring various open problems in the field.

IV. RESEARCH METHOD

By systematically reviewing the literature, this study aims to present an overview of the existing knowledge, research trends, and potential avenues for future research in this domain. The review process involves a comprehensive search of academic databases, selection of relevant articles based on the predefined criteria, extraction and analysis of data, and synthesis of findings. The results of this SLR will be helpful in understanding the current state of QC in the context of future network security, highlight its strengths and limitations, and guide researchers and practitioners in further exploration and implementation of advanced cryptographic techniques for robust network protection. Figure 3 gives an illustrative view of the steps of research methodology, detailed in this section.

Within the research design, the careful selection of suitable research methods can contribute to exploring the potential aspects associated with advancements in QC for future network security. This study employed the exploratory research method to gain a comprehensive and well-rounded understanding of the subject matter. By employing an inductive approach, this study thoroughly analyzes all aspects of the research topic and draws comprehensive conclusions from the collected data.

A. FRAMING RESEARCH QUESTIONS FOR A REVIEW

The research questions (RQs) that guide this SLR are shown in Table 2. These questions aim to investigate quantum cryptography solutions, with a particular emphasis on quantum key distribution (QKD) and quantum communication, while addressing current and emerging security issues. Each question is formulated on the basis of some objectives to achieve. These objectives are listed below:

- RQ1: Understanding the challenges and constraints that must be addressed for quantum cryptography to be successfully adopted and implemented is the goal of this research question.
- RQ2: The goal is to investigate and comprehend quantum attacks' characteristics and how they affect QKD systems security.
- RQ3: The objective is to discover the primary causes of the failure of conventional cryptographic schemes and how quantum cryptography ensures the secured network communications in the quantum era.
- RQ4: To provide insights into the different techniques employed in quantum cryptography and shed light on their practical implementation in real-world scenarios.
- RQ5: By addressing this question, the SLR will provide valuable insights into the role of Quantum networks in enhancing internet security and the potential avenues for further research and development to meet the evolving security requirements of future networks.
- RQ6: To give a thorough grasp of the state of knowledge in the area today, this research question attempts to collect and synthesize the knowledge and insights produced by earlier studies.
- RQ7: To provide insights into the potential avenues for future research and development in quantum cryptography to address the evolving security landscape and ensure the resilience of cryptographic systems in the quantum era.

B. DEFINING PICOC CRITERIA

Table 3 showcases the adoption of the Population, Intervention, Comparison, Outcomes, and Context (PICOC) criteria, initially proposed by [45], as a framework for structuring the research question. This approach enables the identification and understanding of specific findings about the topics addressed in the papers under review.

C. IDENTIFYING RELEVANT WORK

Defining the search technique and search string comes after the research questions have been developed. Finding research papers on QC that focus on network security is the main objective of the search procedure. The search strategy comprised an automated search given by the digital libraries using a search string that is often used by scholars on this subject.

1) STEP1: SEARCH STRATEGY

This strategy aims to identify relevant studies from various electronic data sources (EDS), including IEEE Xplore, ACM Digital Library, ScienceDirect, Springer Nature, Semantic

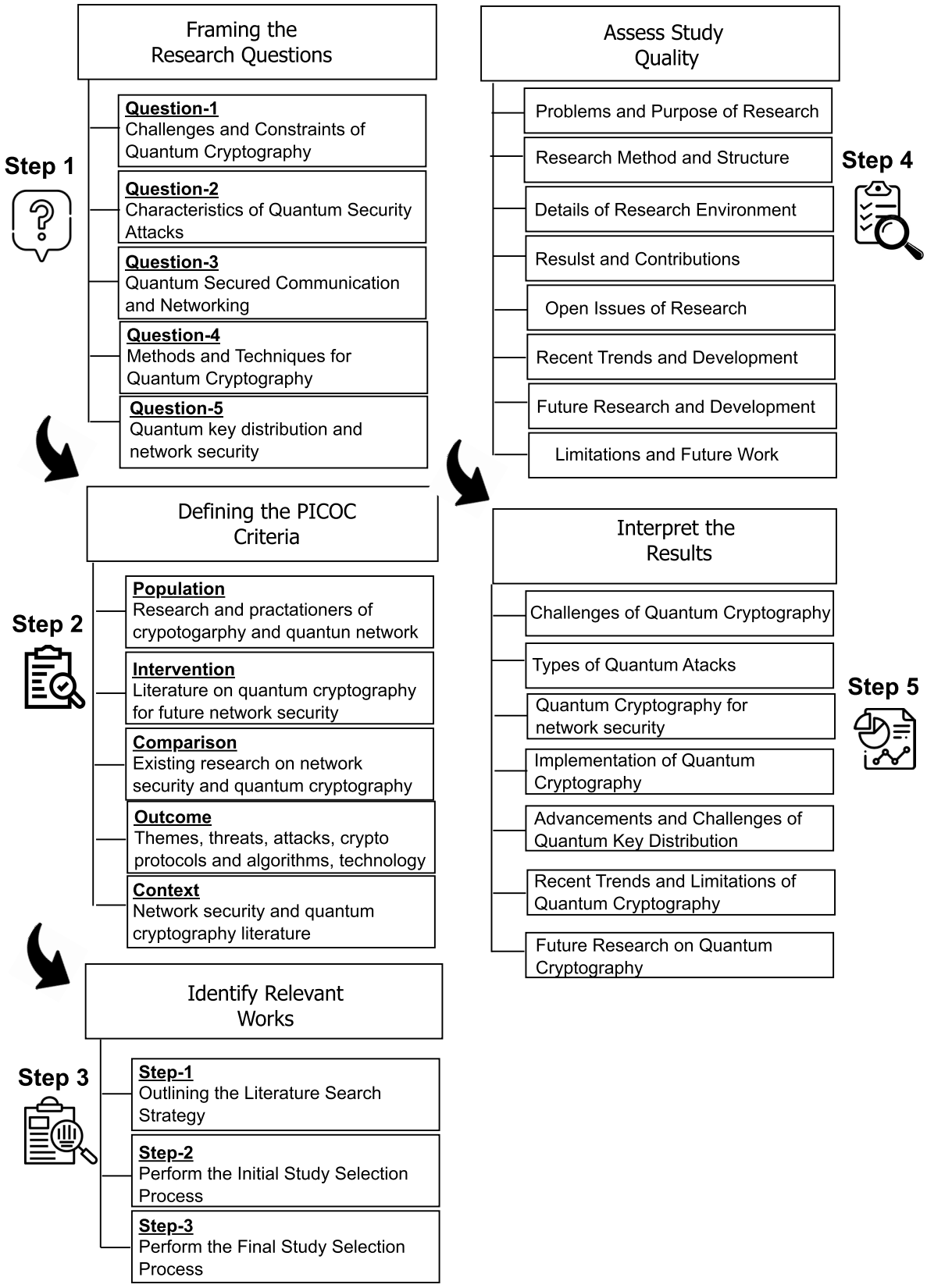


FIGURE 3. An overview of the steps of research method.

TABLE 2. Research questions.

RQ1	What are the issues and challenges faced by Quantum Cryptography?
RQ2	How quantum attacks will affect the security of future network communications?
RQ3	What are the applications of Quantum Cryptography for ensuring network security in the quantum era?
RQ4	What are the techniques exist related to quantum cryptography and how these are implemented?
RQ5	What are the current advancements and challenges in Quantum networks and their potential implications for ensuring future internet security?
RQ6	What are the findings based on the existing research work?
RQ7	What are the future research directions for quantum cryptography?

TABLE 3. PICOC criteria for SLR.

Population	The population of interest for this SLR includes researchers, practitioners, and educators interested in advancements in network security and cryptography.
Intervention	The intervention in this SLR is the research studies and literature on Quantum Cryptography for future network security.
Comparison	No specific comparison is required for this SLR, as it is focused on synthesizing the existing research on network security and quantum cryptography.
Outcome	The SLR aims to synthesize the findings of studies on quantum era network security and quantum cryptography and identify the major research themes, threats and attacks, cryptographic protocols and algorithms, and emerging technologies and trends in this field.
Context	The context of this SLR is the field of evolution in network security and quantum cryptography, including research studies and literature from various disciplines, such as computer science, electrical engineering, mathematics, and information security.

TABLE 4. Composition of the search string for literature search.

("Network Security" OR "Information Security" OR "Cyber Security" OR "Internet Security") AND ("Cryptographic Algorithms" OR "Conventional Cryptography" OR "Quantum Cryptography" OR "Quantum Key Distribution" OR "QKD" OR "QKD Networks") AND ("Techniques" OR "Methods" OR "Algorithms" OR "Protocols") AND ("Implementation" OR "Implementation Details" OR "Practical Application" OR "Experimental Setup") AND ("Network Attacks" OR "Quantum Attacks" OR "Threats" OR "Vulnerabilities") AND ("Potential Advancements" OR "Recent Developments" OR "Emerging Trends" OR "Future Research Directions" OR "Future Research" OR "Future Prospects) AND ("Challenges" OR "Limitations" OR "Issues" OR "Obstacles" OR "Implications")

Scholar, and Google Scholar, based on recommendations from [46]. The search terms selected are based on a combination of keywords and controlled vocabulary as shown in Table 4. With the help of the aforementioned search phrases, we define the search strings and apply them to online literature databases to identify and gather pertinent documents. We only consider studies published in English-language peer-reviewed journals and conference proceedings from 2016 to 2023, using the search string in Table 4:

2) STEP2: INITIAL STUDY SELECTION

Figure 4 shows the original search turned up 282 publications, as demonstrated by SLR methodology, but many of them were duplicates, of poor quality, or unrelated to the study goals. For the reasons listed above, further filtration is performed using the study selection process. The study selection process consists of two phases: title/abstract screening and full-text review. In the first phase, the screening of titles and abstracts of identified studies is performed and in the second phase, the full text of the potentially relevant studies is retrieved and reviewed based on the inclusion/exclusion criteria to determine their eligibility for inclusion in the SLR. Inclusion/Exclusion criteria are given in Table 5 and 6 respectively.

TABLE 5. Summary of the inclusion criteria for literature selection.

I1	Articles published in English language peer-reviewed journals or conference proceedings from 2017 to 2023.
I2	Articles related to conventional cryptography and quantum cryptography in the context of network security
I3	Studies that discuss technologies related to QC
I4	Studies that mention the issues or challenges of QC
I5	Studies that proposed some techniques related to QC and provided with implementation

TABLE 6. Exclusion criteria.

E1	Articles that are not relevant to QC and its applications for network security
E2	Non-English language studies
E3	Studies that are not peer-reviewed, including book chapters, editorials, thesis, and technical reports
E4	Studies that conduct survey on same topic

3) STEP3: FINAL DATA SELECTION

A data extraction form is designed to capture relevant information from the included studies, such as, title, publication year, citations, research question(s), methodology, findings, and implications. 134 research articles are selected from the database of 181 publications after final selection. These selected papers were then evaluated based on the quality evaluation criteria.

D. ASSESSING QUALITY OF STUDIES

The quality of the included studies is assessed using a standardized procedure given in Table 7, and any discrepancies will be resolved through discussion or consultation with the supervisor.

V. RESULTS OF THE SYSTEMATIC LITERATURE REVIEW

Table 9 offers a comprehensive overview of past eight years (2016-2023) research publications selected for the purpose

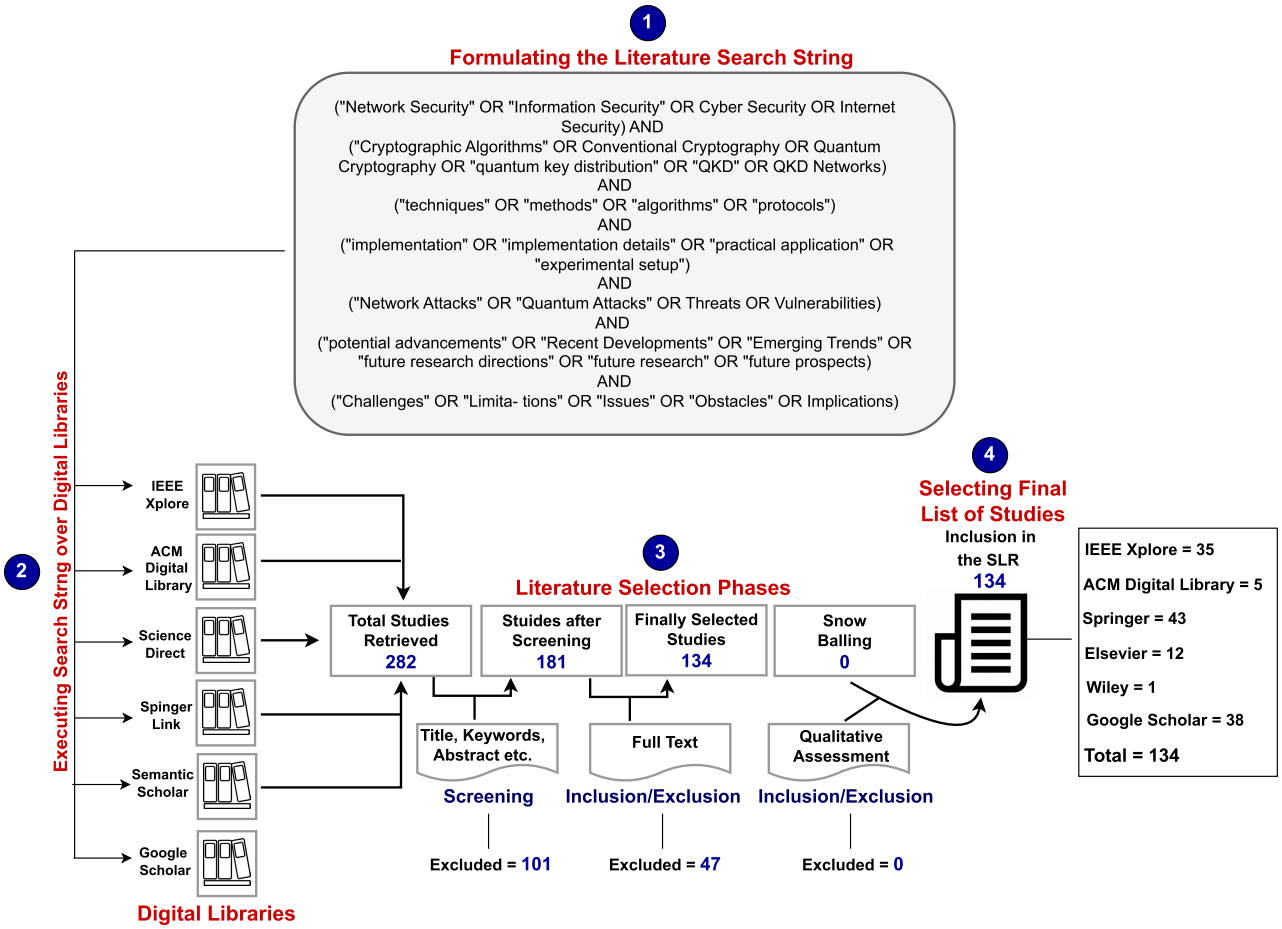


FIGURE 4. Literature search and selection process.

of conducting SLR. In addition to the aforementioned publications, other relevant research papers are also referenced within the article, and their corresponding citations can be found in the References section of this paper. This section includes an in-depth analysis and conclusive insights drawn from the chosen articles, aligning with the research questions at hand.

A. RQ1: ISSUES AND CHALLENGES OF QUANTUM CRYPTOGRAPHY

Despite several improvements [47], quantum cryptography is still seen as a developing technology that must overcome a number of technical obstacles. Unintentional polarisation shifts, short transmission lengths, and the need for specific channels are a few of the difficulties that must be overcome. Despite QKD's intrinsic security, there are certain difficulties with its actual application. Particularly, when the transmission distance grows, restrictions in the key generation rate occur [48].

Theoretically, QC seems to provide a major advance in the realm of data security. However, no cryptographic technique can guarantee complete security. QC relies on a certain set of presumptions in order to be conditionally secure in practice. QKD typically uses weak laser sources due to the difficulty in constructing single-photon sources, paired with multiple single-photon detectors, one for each party, designed to capture photons within a brief time frame. However, the detection windows of the detectors may show minor changes as a result of manufacturing differences. A listener by the name of Eve can intercept Alice's qubit, measure it, and then transmit Bob a ''fake state'' by taking advantage of this flaw in the system. Eve can avoid Bob seeing that she is an eavesdropper by changing the phase and time of the fake photon. Since manufacturing tolerances can cause variations in optical path length, wire length, and other faults, eliminating this vulnerability involves minimizing discrepancies in photodetector efficiency [49].

The systematic grouping of challenges in the field of QC is depicted in Table 8. These difficulties may be roughly divided into three categories: hardware difficulties, performance and cost difficulties, and difficulties related to the design of the quantum paradigm. The hardware difficulties include problems related to experimental settings, where the use of particular hardware components has a direct influence on the system's performance.

TABLE 7. Check list for the literature quality assessment criteria.

Characteristics for Quality Assessment	Score		
	Yes=2	Particularly=1	No=0
Are the problem statement and the purpose of the study clearly stated?			
Are the research's methods and structure thoroughly described?			
Is the study's research environment well described?			
Are the research's stated results consistent with its contributions?			
Has the research successfully described the limitations of traditional/conventional cryptography in the context of network security?			
Does the research effectively investigate the recent developments and trends in QC?			
Does the study efficiently show that QC is the solution for future network security?			
Are the current research's limitations made clear?			

TABLE 8. Quantum cryptography challenges [29], [49], [50].

Performance & Cost Challenges	Design Challenges	Hardware Challenges
Reduces the usage of expensive material. For example, dark fibers. Use techniques that enable concurrent access to multiple users in QKD. Follow those procedures that remove cooling requirements, system complexity and power consumption, etc. Compact and lightweight solutions should be proffered. For example, lowloss planar lightwave circuits, chip-scale QKD, etc	To prevent attacks, keys should be updated frequently. Designing robust error correction and accurate estimation techniques. Designing quantum protocols to transfer quantum information over longer distances. Design techniques for fault-tolerant architecture for real-time systems. To get accurate results, experiments should consider finite data limitations and design for entanglement using appropriate measures.	Hardware that supports large qubits (64 to 1024) are required. Hardware that communicates millions of qubits at high speed is required. Hardware with a lower error rate needs to be designed. Hardware that can hold information longer and allows complex calculations (i.e. large circuit depth) can increase the speed of quantum operations.

The emphasis now switches to finding the best balance between cost-effectiveness and enhanced performance characteristics as we move on to difficulties connected to performance and cost. The design problems include tackling the complexity of real-time experiments while developing novel quantum protocols, tools, or procedures [51]. The goal is to provide solutions that not only advance quantum capabilities but also successfully solve the practical difficulties brought on by current experimental configurations [33], [47]. Quantum Cryptography is plagued by numerous vulnerabilities highlighted in different research work. Photons have the capacity to alter in polarization while being transmitted. Such modifications may be caused by non-homogeneous transmission medium or malicious hacker involvement. It is a challenging effort for engineers to implement algorithms in QC, sometimes at the expense of essential features like digital signatures. The algorithm becomes more vulnerable as a result of this compromise. Due to its extraordinary sensitivity, meeting the strict design specifications of the photon emitter in QC proves to be quite difficult. It is possible to hack the method via a time-shifting assault [40], [47]. The possibility to use stimulated emission or the light's clustering features to create exact copies of an unidentified quantum state. It is extremely difficult to implement multiplexing in a quantum channel since each individual photon needs its own high-quality channel. It is pricey due to the necessity's huge cost increase. In addition, there are certain extra barriers that prevent the broad use of QKD, in addition to the general difficulties connected with it. First of all, the cost of the optical components used in QKD makes its implementation prohibitively expensive [20]. Further restricting the system's accessibility is the fact that using it requires users to have a foundation in physics due to its intricacy. Thirdly, consumers need to feel confident that the equipment they buy from sellers has been set up securely for QKD purposes, which makes the lack of security standards for QKD equipment a concern. Last but not least, QKD is only useful for short transmission lengths, which continues to be a major impediment to its wider application across greater distances. In conclusion, there are several issues with QC that are outside the scope of the rules of physics. As a result, there is still a long way to go before QC completely replaces traditional encryption in the sphere of information security [52], [53]. In [54] the authors highlight a range of challenges associated with QKD networks that extend beyond hardware issues. The advancement of quantum cryptography has been hindered by the need to grasp the intricate rules of quantum physics. To simplify quantum cryptography and promote its broader adoption, it is crucial for computer science researchers to develop a thorough understanding of these fundamental principles. The issues and challenges discussed in this section are derived from various sources, including [20], [40], [47], [48], [49], [52], and [53]. Overcoming these obstacles will be

TABLE 9. List of selected research articles (2016-2023).

Ref. No.	Study Ref.	Publication Channel	Year	RQs	Citations
S1	[56]	Springer	2021	RQ3, RQ6	21
S2	[26]	Elsevier	2022	RQ3, RQ4	229
S3	[57]	ACM	2020	RQ3, RQ2, RQ4, RQ6	101
S4	[27]	IEEE	2022	RQ3, RQ2, RQ4, RQ6	65
S5	[5]	Elsevier	2017	RQ2	40
S6	[58]	IEEE	2018	RQ3	44
S7	[49]	Springer	2017	RQ1, RQ3, RQ4, RQ6	20
S8	[12]	IEEE	2022	RQ3	2
S9	[50]	Elsevier	2020	RQ2, RQ1	8
S10	[59]	ACM	2019	RQ3	590
S12	[40]	Elsevier	2016	RQ3, RQ4, RQ6	11
S13	[60]	IEEE	2019	RQ3	33
S14	[41]	Springer	2019	RQ1, RQ3	43
S15	[61]	Springer	2018	RQ3, RQ4, RQ6	32
S16	[48]	IEEE	2019	RQ1	-
S17	[53]	IEEE	2018	RQ1, RQ2, RQ6	19
S18	[62]	ACM	2020	RQ3, RQ4, RQ6	6
S19	[54]	ACM	2022	RQ1, RQ3, RQ4, RQ6	4
S20	[63]	Springer	2020	RQ2, RQ4	8
S21	[64]	Springer	2020	RQ2, RQ4	3
S22	[65]	IEEE	2019	RQ2, RQ4	6
S23	[34]	nature	2016	RQ3, RQ4, RQ6	570
S24	[66]	Springer	2021	RQ2, RQ4	19
S25	[67]	Elsevier	2021	RQ2, RQ4	11
S26	[68]	Springer	2016	RQ2, RQ4	54
S27	[69]	Nature	2018	RQ2, RQ4	37
S28	[70]	Springer	2021	RQ2, RQ4	4
S29	[71]	Springer	2023	RQ2 ,RQ4	-
S30	[72]	IEEE	2021	RQ2, RQ4	3
S31	[73]	Elsevier	2022	RQ3, RQ4	48
S32	[29]	Springer	2020	RQ3, RQ4	21
S33	[74]	Springer	2023	RQ3, RQ4	5
S34	[75]	Springer	2018	RQ3, RQ4	3
S35	[76]	Springer	2016	RQ3, RQ4	16
S36	[77]	nature	2018	RQ3, RQ4	22
S37	[78]	Springer	2022	RQ3, RQ4	12
S38	[79]	Elsevier	2018	RQ3, RQ4	64
S39	[80]	Sprirnger	2021	RQ3, RQ4	-
S40	[81]	Elsevier	2016	RQ3	15
S41	[82]	Springer	2019	RQ3, RQ4	5
S42	[83]	IEEE	2021	RQ3	1
S43	[84]	IEEE	2017	RQ3	74
S44	[85]	Elsevier	2019	RQ3	7
S45	[86]	IEEE	2016	RQ3	20
S46	[87]	IEEE	2018	RQ3	11
S47	[88]	Springer	2021	RQ3	7
S48	[89]	IEEE	2019	RQ3	14
S49	[90]	Springer	2023	RQ3, RQ4	-
S50	[91]	Elsevier	2021	RQ3	60
S51	[92]	Springer	2021	RQ3, RQ4	11

TABLE 9. *(Continued.)* **List of selected research articles (2016-2023).**

S52	[51]	Springer	2022	RQ1, RQ3	-
S53	[93]	Springer	2018	RQ3, RQ4	48
S54	[94]	Wiley	2020	RQ3, RQ4	35
S55	[95]	IEEE	2017	RQ3, RQ4	7
S56	[96]	Elsevier	2023	RQ3	7
S57	[97]	IEEE	2017	RQ3	3
S58	[98]	Springer	2017	RQ3	24
S59	[99]	IEEE	2023	RQ2, RQ4	-
S60	[100]	IEEE	2021	RQ4, RQ5	51
S61	[101]	Springer	2017	RQ4	57
S62	[102]	IEEE	2022	RQ4, RQ5	14
S63	[103]	IEEE	2021	RQ4, RQ5	51
S64	[104]	nature	2020	RQ4, RQ5	554
S65	[105]	IEEE	2020	RQ2, RQ4	-
S66	[106]	Springer	2023	RQ4	1
S67	[107]	nature	2018	RQ3, RQ4	28
S68	[108]	nature	2017	RQ4	15
S69	[109]	Springer	2021	RQ4	14
S70	[110]	Nature	2018	RQ4	253
S71	[111]	Nature	2017	RQ5, RQ6	1403
S72	[112]	Springer	2020	RQ4	12
S73	[113]	Nature	2019	RQ5	121
S74	[114]	IEEE	2021	RQ5	1
S75	[115]	IEEE	2016	RQ5	26
S76	[116]	IEEE	2019	RQ5	32
S77	[117]	Nature	2019	RQ5	63
S78	[118]	IEEE	2020	RQ5	33
S79	[119]	IEEE	2020	RQ5	12
S80	[120]	IEEE	2020	RQ5	16
S82	[121]	IEEE	2019	RQ5	7
S83	[122]	nature	2017	RQ5	15
S84	[123]	IEEE	2019	RQ5	48
S85	[124]	Elsevier	2022	RQ5	3
S86	[125]	IEEE	2022	RQ5	3
S87	[126]	Nature	2021	RQ5	455
S88	[127]	Nature	2021	RQ5	153
S89	[128]	IEEE	2021	RQ5	33
S90	[129]	Springer	2023	RQ1	-
S91	[130]	IEEE	2023	RQ5	-
S92	[131]	IEEE	2023	RQ5	1
S93	[132]	IEEE	2023	RQ5	1
S94	[133]	Nature	2019	RQ5	125
S95	[134]	IEEE	2022	RQ5	12
S96	[55]	ACM	2019	RQ1,RQ5	100
S97	[135]	ACM	2023	RQ5	-
S98	[136]	DTIC	2023	RQ5	1
S99	[137]	ULOOP Inc.	2022	RQ5	-
S100	[138]	Quantum World Congress	2022	RQ5	-
S101	[139]	IEEE	2016	RQ5	28
S102	[140]	Arxiv.org	2021	RQ5	22
S103	[141]	CRC Press	2021	RQ5	111
S104	[142]	Arxiv.org	2022	RQ5	5
S105	[143]	IEEE	2021	RQ5	47

TABLE 9. *(Continued.)* **List of selected research articles (2016-2023).**

S106	[144]	MDPI	2023	RQ5	3
S107	[145]	ACM	2019	RQ5	239
S108	[146]	quantum-journal.org	2023	RQ5	23
S109	[147]	APS	2021	RQ5	18
S110	[148]	IEEE	2017	RQ5	200
S111	[149]	Nature	2022	RQ5	373
S112	[150]	APS	2016	RQ5	93
S113	[151]	Springer	2021	RQ5	43
S114	[152]	American Association for the Advancement of Science	2017	RQ5	63
S115	[153]	Nature	2017	RQ5	440
S116	[154]	IOP Publishing	2018	RQ5	83
S117	[155]	Nature	2021	RQ5	111
S118	[156]	Optica Publishing Group	2020	RQ5	31
S119	[157]	Università degli studi di Padova	2023	RQ5	-
S120	[158]	Wiley	2023	RQ5	55
S121	[159]	IEEE	2023	RQ4,RQ5	4
S122	[160]	IEEE	2021	RQ4	9
S123	[161]	IEEE	2022	RQ4	16
S124	[162]	IOP Publishing	2019	RQ4	34
S125	[163]	APS	2020	RQ4	79
S126	[164]	Nature	2015	RQ6	611
S127	[165]	APS	2018	RQ6	691
S128	[166]	ITUAJ	2019	RQ6	1
S129	[167]	Publications Researchgate	2019	RQ5,RQ6	23
S130	[168]	ACM	2018	RQ5,RQ6	3
S131	[169]	Nature	2017	RQ5	949
S132	[170]	American Association for the Advancement of Science	2017	RQ5,RQ6	1469
S133	[171]	Nature	2021	RQ5,RQ6	781
S134	[172]	IEEE	2021	RQ5	13

key to bridging the gap between the theoretical foundations of quantum cryptography and its practical applications.

B. RQ2: QUANTUM ATTACKS AND THEIR IMPACT ON NETWORK SECURITY

The security of cryptographical protocols is significantly at risk due to the advancement in quantum computers. Specific cryptographic techniques, deemed secure against classical attacks, can be compromised by quantum computers. The security assurances offered by QKD methods could be at risk if a sufficiently strong quantum computer becomes available, making them vulnerable to possible assaults. A particular danger from quantum assaults exists for the security of QKD methods. These assaults target weak points in the quantum communication system by taking use of the laws of quantum physics. As a result, there is a serious risk to the overall security of the cryptographic keys created using QKD techniques' secrecy and integrity [56].

Rapid development in recent years has allowed quantum technologies to steadily take the place of more traditional information security techniques [167]. They provide noticeable advantages including higher security levels and special qualities that outperform traditional information security techniques. Notably, eavesdropping efforts may be continuously and extraordinarily detected by quantum technology. The capacity to detect eavesdropping without the use of data encryption is the main benefit of quantum secret-sharing systems. They differ from traditional secret-sharing algorithms because of this. Comparable to their classical counterparts, quantum stream cipher and quantum digital signature both provide increased security [26].

By using quantum one-way functions, the quantum digital signature in particular achieves information-theoretic security. The actual use of these quantum technologies, however, faces a number of technological obstacles. Researchers have done a preliminary classification of attacks aimed at QKD channels using scientific literature analysis. assaults against

qubits, the fundamental building blocks of quantum binary systems, and assaults that take advantage of flaws in the quantum system's components may be divided into two primary groups. Furthermore, based on the difficulty of the equipment needed to carry out such attacks, several research groups have developed a fundamental categorization of attacks on QKD protocols. An enhanced categorization for assaults on QKD systems has recently been developed, separating active from passive attacks [49].

In the world of QKD systems, this new categorization offers a more thorough framework for classifying various attack types. Several types can be found within the realm of classical attacks: Intercept-resend attacks and semi-transparent assaults are examples of non-coherent attacks. DOS and Man-in-the-middle attacks are some examples of attacks brought on by flaws in the protocol [20]. Collective assaults and joint attacks are the two subcategories of coherent attacks. Collective assaults and joint attacks are the two subcategories of coherent attacks. Exploiting flaws in quantum systems or technologies to undermine their security is known as quantum hacking. It includes employing quantum ideas, methods, or tools to launch assaults on quantum-based systems or cryptographic protocols. Quantum hacking tries to gain unauthorized access, get private information, or impair the regular operation of quantum systems by making use of the specific properties of quantum mechanics i.e., quantum superposition and entanglement [52]. Right now, the most successful QKD attack is thought to be the Photon Number Splitting (PNS) attack. This attack is examined in [134] within a specific framework designed to model and simulate QKD systems. Table 10 provides the summary of different research work related to attacks on quantum protocols. According to an article [62], since the eavesdropper (referred to as Eve) may be able to indirectly access the transceiver by using probing radiation, QC systems are typically thought of as open systems assaults against technical implementation or Trojan horse assaults are frequent names for these kinds of attacks. It is impossible to guarantee the privacy of distributed keys without a system that is resistant to such assaults. The situation that arises in the face of such assaults is fundamentally unique, making it impossible to directly use the traditional techniques for assessing the cryptographic robustness of QKD systems. Reference [101] documents an experiment in which an attacker's attempt to retrieve the key distributed through the BB84 QKD protocol was simulated within a controlled environment. New methods must be created to identify both known and unknown assaults, as well as varied combinations of both known and unknown attack kinds. Traditional classifications divide all attacks on QC systems into four categories mentioned in [5] and [48]. Research is now focused on improving and securing QKD protocols as well as investigating post-QC algorithms that are impervious to attacks from both classical and quantum computers to lessen the impact of these quantum attacks. To defend against new dangers and guarantee the long-term security of quantum communication networks, it is crucial to continuously assess and improve QKD techniques. This section is extracted from [5], [20], [26], [29], [48], [49], [52], [56], [62], [63], and [64] research papers.

C. RQ3: APPLICATIONS OF QUANTUM CRYPTOGRAPHY IN NETWORK SECURITY

The science of cryptography deals with encrypting and decrypting data in order to protect it and enable safe transmission over the network. To do this, encryption is carried out by using a key, and the encrypted data is returned to its original state by carrying out decryption on it. Traditional cryptography has the benefits of offering safe communication over great distances, the ability to be implemented in software or hardware, and the presence of various effective algorithms. Despite the resilience and effectiveness of Classical Cryptography, the dependence on untested computational assumptions has spurred academics to look at alternate approaches to solving security problems. As a result, one important effort in this endeavor was the creation of QC. In conventional cryptography, keys are created randomly and are employed for this purpose, but they are susceptible to eavesdropping and other quantum attacks. However, by using quantum communication, or using key distribution carried out by QC, we may solve the issue. Thus, QC involves the key distribution process rather than the communication itself. Utilizing the concepts of quantum physics to increase network security, QC has several uses and advantages over traditional cryptography. A completely secure communication channel is made possible by QC, which is distinguished by its extraordinary speed [55], [168].

The fundamental ideas of QC stem from the Heisenberg Uncertainty Principle and the polarisation of photons, two fundamental ideas in QC. It is difficult for eavesdroppers to decrypt QC-based cryptosystems because of the Heisenberg Uncertainty principle. On the other hand, the capacity to polarise light photons in certain directions is explained by the photon polarisation principle. A photon filter must also match the exact polarisation of a polarised photon in order to detect it since any incompatibility would cause the photon to be destroyed. The no-cloning theorem, another principle of quantum mechanics, denies the production of exact duplicates of an unknown quantum state. QKD is the most well-known of the many cryptographic applications that quantum mechanics has to offer. Establishing a safe key for use in encryption methods is the main goal of QKD. Bennett and Brassard first devised the BB84 and B92 protocols, which are two well-known QKD methods, in 1984 and 1992, respectively [11], [25].

Quantum cryptography has the transformative capacity to redefine many aspects of our daily routines. While still in its nascent stage of development and integration, QC is actively being investigated and integrated into real-world contexts. Table 11 presents relevant studies and prominent examples that illustrate its tangible applications. The creation of secure

TABLE 10. Research work related to attacks on quantum protocols.

Quantum Attacks	Attack Summary	Relevant Studies
Side Channel Attack	Exploiting unintended information leakage from a system to gain unauthorized access or information.	[63] [64] [67]
Detector Blinding Attack	Manipulating a quantum detector's response to extract sensitive information.	[70]
Intercept Resend Attack	Intercepting and re-transmitting quantum signals to gain unauthorized access to data	[71]
Gaussian Attacks	Employing Gaussian noise to compromise the security of quantum communication systems.	[72]
Man-in-Middle Attack	Inserting oneself between communication parties to intercept and potentially alter data.	[69] [99]
Trojan Horse Attack	Introducing malicious code or components into a system to compromise its integrity.	[63] [71]
Participant Attack	A network participant intentionally disrupting or compromising the security of the communication.	[66]
Collusive Attack	Coordinated efforts among multiple attackers to compromise a system's security.	[68]
Canonical Attack	Exploiting fundamental vulnerabilities in a system to compromise its security.	[72]
Photon Number Splitting (PNS) Attack	A theoretical technique that seeks to retrieve all of the information on the shared secret key bits that QKD generates while avoiding any errors that can be detected.	[139]

communication networks is one of the primary applications of QC. QKD methods make it easier to create encryption keys that cannot be cracked, ensuring the privacy of sensitive data sent via networks. The protection of confidential government communications, the safety of financial transactions, and the defense of vital infrastructure all depend on this. Research conducted in references [20], [25], [28], [30], [33], [56], [72], [73], [74], [75], [76], [77], [78], [79], and [93] demonstrates the utilization of QC in the context of secure network communication. Interestingly, QC holds promise for enhancing the security of financial services. Concerns regarding the susceptibility of conventional cryptography methods to possible assaults have been raised by the development of quantum computers. Financial organizations may strengthen the defense of critical data, assure the security of transactions, and effectively combat new security risks by implementing quantum-resistant encryption approaches like QKD. The utilization of QC in the domain of secure financial services is highlighted in research undertaken in [80], [81], and [82]. The handling of substantical volume of sensitive data in data centers and cloud computing settings is a crucial challenge. The potential for QC to play a significant role in enhancing the security of these infrastructures is great. Organizations can efficiently protect the privacy and authenticity of their data within cloud environments by integrating quantum-resistant encryption algorithms and using QKD to create secure channels connecting data centers and users. The study done in [84], [85], [86], [87], [89], [94], and [124] emphasizes the use of QC in the area of Data Centers and Cloud Computing security. Concerns about the IoT devices' vulnerability to cyber attacks are increased by their fast proliferation. In order to provide safe key distribution and encryption procedures specifically designed for IoT devices, QC offers a viable solution. The purity and privacy of IoT data may be protected, successfully limiting potential vulnerabilities, by using quantum-resistant algorithms and building reliable communication routes. The research conducted in [59], [83], and [88] places a strong emphasis on the application of QC to the security of the IoT. The administration of very private patient information and medical records is crucial in the healthcare industry. The addition of a second layer of security using QC might strengthen the protection of electronic medical records. This technology can ensure patient privacy, prevent unauthorized access, and stop any tampering with medical records. QC is used in the context of healthcare and the security of medical data, as shown by research in references [90], [91], and [50]. By using QC, authentication and identity management systems may be improved. Digital identities may be strengthened using cryptographic algorithms that are resistant to quantum hazards, reducing identity theft and maintaining the validity of user authentication processes. Research work presented in [81], [89], [92], [94], and [103] illustrates the application of QC within the realm of authentication and identity management. QC has the ability to address concerns about security in voting processes and systems. The avoidance of manipulation, preservation of vote secrecy, and protection of the veracity of election results become attainable with the deployment of encryption techniques resistant to quantum threats and the development of secure communication paths. The utilization of QC within the scope of Secure Elections and Voting Systems is demonstrated by research presented in references [95], [96], and [97].

Network security may one day be future-proofed by QC. The weaknesses of traditional encryption techniques become increasingly obvious as quantum computers develop. Organizations may reduce the hazards posed by quantum computing and guarantee that their data and communication will be safe in the face of upcoming technological advancements by switching to QC. [20]

All the information in the above section is extracted from the analysis of the following research articles referenced as [11], [18], [19], [20], [25], [55], [57], and [168].

Quantum Cryptography for Future Networks:

As from the literature review QC guarantees the absolute secrecy of cryptographic keys, it provides an unparalleled degree of security. This indicates that the keys continue to be 100 percent safe regardless of the computing power or resources that prospective enemies may possess. This absolute anonymity is predicated on a few requirements being followed, though. In particular, it is assumed that the

TABLE 11. Studies on applications of quantum cryptography.

Applications of QC	Relevant Studies
Secure Communication	[26] [57] [34] [21] [31] [73] [29] [74] [75] [76] [77] [78] [79] [80] [94]
Financial Services	[81] [82] [83]
Data Centers and Cloud Environment	[85] [86] [87] [88] [90] [95] [129]
Internet of Things Security	[60] [84] [89]
Healthcare and Medical Data	[91] [92] [51]
Authentication and Identity Management	[82] [90] [93] [95] [107]
Secure Elections and Voting Systems	[96] [97] [98]

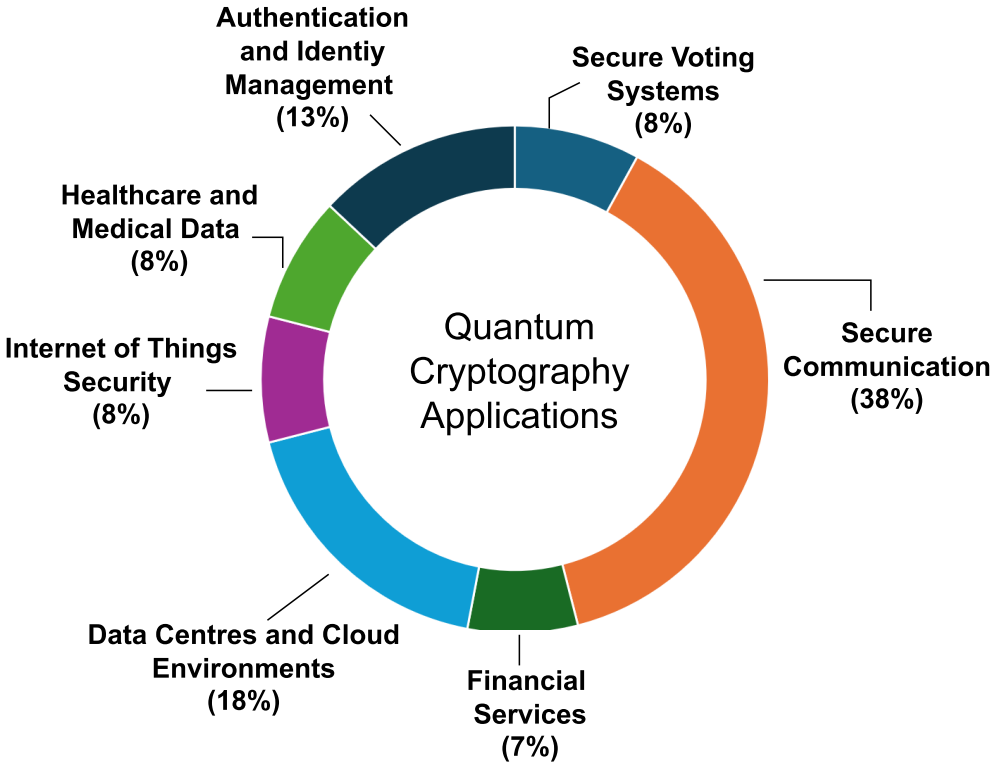


FIGURE 5. Applications of quantum cryptography.

eavesdropper has no direct or indirect access to the sender and receiver and that the assaults are purely directed at the transmitted quantum states. In other words, by solely taking into account assaults on the quantum states occurring during transmission, QC protects the confidentiality of keys. It is based on the supposition that any possible listener lacks access of any kind to the quantum communication channel or the transmitting and receiving stations. This level of security is unmatched by conventional encryption, which is based on computational presumptions and vulnerable to algorithmic or processing power advancements [25], [168].

QC offers a strong barrier against listening in and unauthorized access to cryptographic keys by utilizing the fundamental ideas of quantum physics. It takes advantage of the special qualities of quantum states to create secure communication channels that are impervious to monitoring and manipulation. The communication system's total security is increased since the keys created through quantum processes are resistant to assaults that aim to compromise the transmitted quantum states, guaranteeing their complete confidentiality. It is crucial to remember that although providing this high degree of security, QC still necessitates careful implementation and adherence to established protocols and best practices. The security assurances of QC may be jeopardised by any potential flaws or weaknesses in the underlying hardware, software, or development procedures. To maintain the integrity and secrecy of the quantum communication system, it is imperative that all required precautions be taken [26], [56].

A team from the Institute of Information Engineering led by Tianqi Zhou [15] revealed that QC is derived from the idea of quantum money, which Wiesner put forward in 1969 [17]. The uncertainty principle, the quantum no-cloning theory, the quantum teleportation, and the hidden properties are the key aspects of quantum information. Quantum teleportation

and quantum direct communication are two different types of quantum communication. With a quantum computer, the well-known discrete logarithm issue will be solved easily [48], [57]. Examining QC methods will be a crucial component of future Internet security concerns. The results of the experimental investigation show the absolute security and efficiency of QC in spotting sniffer efforts. Due to these characteristics, QC is a good candidate for Internet-related applications in the future. Future networks should be secured since they will house all information systems and the environment necessary for communication and data sharing. QC is now the first solution to the network security issue that is becoming more and more of a problem [18], [39], [59]. The main use of QC is QKD, which has seen substantial development. It includes using quantum communication to create a shared key between two individuals, such as Alice and Bob while making sure that any third person, such as Eve, is kept in the dark about the specifics of the key even if she intercepts all conversation between Alice and Bob. Any attempt by Eve to learn more about the key results in contradictions that let Alice and Bob know something is up. The established key is then often used for encrypted communication with conventional techniques like symmetric cryptography, such as the one-time pad [40], [60]. In terms of security, QKD has a distinct advantage since, unlike traditional key distribution techniques, its mathematical proof may demonstrate its resilience without placing restrictions on the capacities of prospective listeners. This asset is frequently referred to as ''unconditional security,'' but with a few small presumptions. These presumptions include the use of quantum physics rules, Alice and Bob's capacity to verify one another, preventing Eve from posing as them, and reducing the likelihood of a man-in-the-middle assault [53], [58], [61].

These explanations are gathered from thorough analysis of [18], [25], [26], [39], [40], [48], [53], [56], [57], [58], [59], [60], [61], [168] articles mentioned in references.

D. RQ4: TECHNIQUES FOR IMPLEMENTING QUANTUM CRYPTOGRAPHY

Several techniques exist within the domain of quantum cryptography, each aiming to utilize the distinct qualities of quantum mechanics to improve the security of communication and data transmission. An overview of recently developed and tested QC methods is listed in Table 12. These methods are arranged according to a number of factors, such as their use in communication protocols, how they are implemented, simulation techniques, the use of quantum-based mechanisms for authentication, encryption and decryption operations, key distribution, the detection and analysis of quantum attacks, the consideration of entanglement scenarios over various distances, and the investigation of various quantum attack types.

QC encompasses an extensive array of cryptographic methodologies and protocols as shown in Figure 6. Quantum Communication Protocols encompass a range of strategies and techniques designed to facilitate secure transmission of information using quantum principles. QKD, examined in studies [20], [86], [87], [95], [101], [108], [110], [111], [112], [114], [116], [118], [119], [120], [123], [124], [125], [126], [127], [129], [135], [144], [159], [160], [161], [162], [169], [170], [171], [172], stands as a prominent protocol within Quantum Communication Protocols.

Another crucial protocol is Mistrustful QC, scrutinized in research [28], [73]. The exploration of the Bounded- and noisy-quantum-storage model is observed in the context of [73] and [76]. Position-based QC has been investigated extensively by researchers [77], [78], [147]. Lastly, the protocol of Device-independent QC has garnered attention and insights from studies [58], [72], [79], [142], [143], [176]. The realm of QC witnesses diverse implementation techniques explored in a series of studies. These works, such as [48], [50], [52], [60], [138], [150], [151], [177], and [178], contribute to the understanding and advancement of practical applications in quantum cryptographic systems. By investigating a wide spectrum of methods, these studies shed light on the intricacies of translating theoretical principles into real-world implementations, fostering the advancement of robust and secure quantum communication technologies.

The exploration of simulation-based QC techniques is a dynamic area of research, as evidenced by studies conducted in [39], [61], [91], [93], [96], [96], [97], [99], [99], [113], [131], and [134]. These investigations delve into the realm of virtual experimentation, where intricate quantum phenomena are simulated within controlled environments. Through these studies, researchers gain insights into the behavior of quantum cryptographic protocols under varying conditions, paving the way for a deeper comprehension of their strengths, weaknesses, and potential vulnerabilities. By harnessing the power of simulations, these endeavors contribute to the refinement and optimization of QC methodologies, ensuring their effectiveness and security in real-world applications.

Quantum Encryption techniques stand as a captivating domain within the realm of QC, with notable explorations presented in studies [40], [60]. These investigations delve into the intricacies of leveraging quantum principles to create unbreakable encryption methods, enhancing data security in the quantum realm. By delving into the specifics of quantum encryption methodologies, researchers aim to harness the distinct characteristics of quantum states, such as superposition and entanglement, to ensure data confidentiality and integrity in a manner that traditional encryption mechanisms cannot match.

The insights gained from these studies provide valuable building blocks for the future development of quantum cryptographic systems, with potential applications ranging from secure communication to advanced data protection across various sectors. The exploration of techniques related to Quantum Authentication represents a compelling frontier in the realm of QC, as evident from the comprehensive investigations conducted in studies [74], [75], [81], [82], [84], [89], [90], [92], [94], [103]. These studies delve into the intricate landscape of quantum-based authentication

TABLE 12. Quantum cryptography techniques.

S.No	Quantum Cryptography Techniques	Relevant Studies
1	Quantum Key Distribution	[21] [87] [88] [96] [105] [112] [114] [115] [116] [118] [120] [123] [124] [125] [128] [129] [130] [131] [132] [134] [175] [176] [177] [140] [178] [149] [159] [160] [161] [162] [163] [164] [165] [166] [167]
2	Quantum Communication	[81] [86] [89] [90] [98] [111] [113] [119] [121] [122] [126] [127] [133] [55] [135] [137] [138] [141] [179] [142] [144] [145] [146] [154] [158] [180] [181] [168] [169] [172]
3	Mistrustful Quantum Cryptography	[29] [74]
4	Bounded & Noisy Quantum Storage Model	[77]
5	Position-Based Quantum Cryptography	[78] [79] [152]
6	Device-Independent Quantum Cryptography	[59] [73] [80] [182] [147] [148]
7	Quantum Cryptography Implementation	[49] [61] [53] [51] [183] [143] [155] [156] [184]
8	Simulation Based Quantum Cryptography	[62] [40] [92] [94] [97] [100] [101] [102] [103] [117] [136] [139]
9	Quantum Authentication	[75] [76] [82] [83] [85] [90] [91] [93] [95] [107]
10	Quantum Attacks	[5] [63] [65] [66] [67] [68] [69] [70] [71]
11	Quantum Attack Detection & Analysis	[54] [31] [64] [72] [84] [99] [106]
12	Long & Short Distance Entanglement	[104] [108] [109] [110] [150] [151] [153] [157] [170] [171]

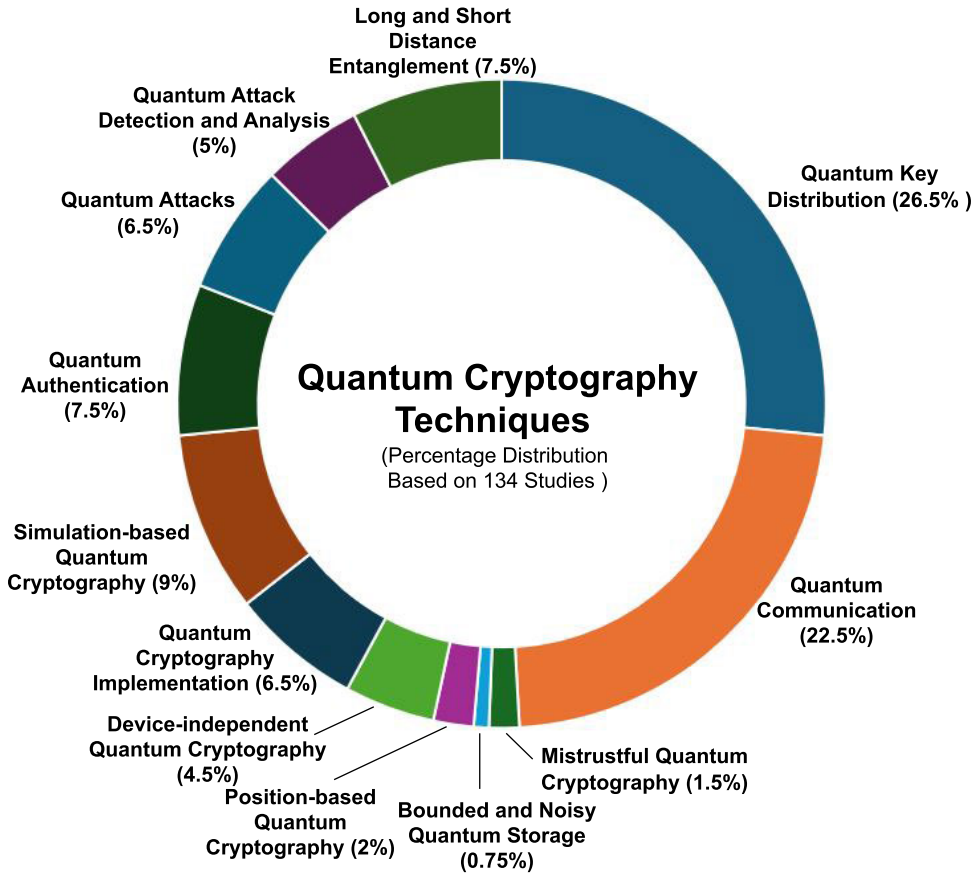


FIGURE 6. Quantum cryptography techniques.

methodologies, aiming to leverage the inherent properties of quantum mechanics to enhance the security of authentication processes.

A significant body of research has been dedicated to techniques for the exploration of Quantum Attacks, as evidenced by the extensive investigations conducted in studies [5], [62], [64], [65], [66], [67], [68], [69], [70]. These studies delve into the intriguing domain of exploiting vulnerabilities within quantum cryptographic systems, aiming to uncover potential weaknesses and devise countermeasures to bolster their resilience. In reference [100], a remarkable advancement in the field of QC is detailed. The study showcases the successful implementation of entanglement-based QKD between two ground stations situated 1,120 kilometers apart. What makes this achievement stand out is that it was accomplished without the necessity of trusted relays. The

researchers achieved a finite secret-key rate of 0.12 bits per second, underscoring the potential for establishing secure long-distance quantum communication without relying on intermediary components. This breakthrough signifies a significant stride towards the practical utilization of QC for ensuring secure communication across extensive geographical distances. Entanglement-based techniques are also presented in [100], [104], [105], [106], [121], [145], [146], [148], [152], and [165].

Quantum information can be encoded in discrete time intervals using time-bin encoding techniques. This technique enhances quantum communication's resilience to noise and works especially well for long-distance transmission [154]. Time-bin encoding techniques for quantum communication are proposed in [154], [155], [156], [157], and [158]. Researchers used high-dimensional arrival-time encoding in conjunction with wavelength multiplexing to create a multi-user QKD network in [154]. Utilizing wavelength-multiplexed time-bin encoding, [155] experimentally demonstrated high-dimensional quantum key distribution. Using a two-photon interference technique, [157] propose and experimentally show a novel scheme for measuring high-dimensional phase states that we call quantum-controlled measurement. An efficient time-bin encoding for practical high-dimensional quantum key distribution is presented in [158]. In summary, QC techniques offer a promising avenue for future network security to provide fundamentally secure communication. These techniques address vulnerabilities present in classical cryptographic methods.

E. RQ5: ADVANCEMENTS AND CHALLENGES OF QUANTUM NETWORKS

The creation of quantum networks, which use the principles of physics to provide increased safety and allow secure communication and transfer of quantum states, is the primary use of quantum technology. Even though this field's study is still in its infancy, a number of organizations have begun building quantum testbeds in order to explore and develop quantum networks. The most common use case for quantum networks at the moment is Quantum Key Distribution (QKD), which is the focus of most testbeds. Future uses, on the other hand, may involve more intricate systems with new capabilities and technical developments, such as distributed quantum computing, blind quantum computing, and quantum sensor networks [179]. Global Quantum Intelligence's "Quantum Safe Outlook" study offers further in-depth information about quantum networking [180].

In table 13 List of a few quantum networks has been compiled to follow the development of quantum network testing on a global scale. While some testbeds for quantum networking are operating or have /blen retired, others are still in the research stage. QUANT-NET is introduced in article [130], which also describes its creation, design, and key technology. By 2025, it is anticipated that the US will have connected many national laboratories over a quantum internet, per research reported in [131]. The Chicago network is currently in use and employs Toshiba technology together with quantum security mechanisms, as detailed in the published article [132]. Other Quantum Testbeds include DC-QNet [133], SECOQC [169], IEQNET [135], DARPA Quantum Network [136], QuTech [173], China Mobile Ltd QKD Network [172], EPB Quantum Network [137], Quantum Scientific Computing Open User Tested (QSCOUT) [138], Satellite Quantum Network [107]. Many organizations like IBM, Google, Amazon, Azure, Microsoft, Alibaba etc., are working on providing cloud bases services using quantum network and resources [181]. An IoT Quantum Network has been proposed in [139].

Since Quantum Key Distribution (QKD) is the most common use case for quantum networks, as previously indicated, our main focus is on highlighting the developments and challenges in QKD networks. As discussed earlier a number of QKD networks have been proposed, helping to test the use of various practical solutions. In contrast to the current reliance on public-key cryptography, which relies on complex computational challenges, the proposal of a QKD network seeks to establish QKD protocols as the fundamental framework for the Internet [132], [133]. This would provide unconditional security key distribution. Correlation studies on QKD networks have received significant funding from several countries and academic institutes.

1) QKD NETWORKS

The specific features of QKD networks and the unusual organization of network architecture are the main reasons why QKD networks differ from traditional telecommunication networks. QKD nodes and QKD links are the fundamental building blocks of the QKD network [182]. Figure 7 shows that three layers are used in the QKD network's structure. The quantum layer is devoted to creating a reliable symmetric key. Layer of key management is used to validate and manage the key that was earlier created and the communication layer is used to protect data in transit. In [109] three-layer QKD network architecture is proposed. In the ITU-T Y.3800 guideline [182] the conceptual frameworks of both a QKD network and a user network are shown. QKD network architecture recommended in [182] consists of six layers. In [110] an architecture for the control and management of Quantum Key Distribution Networks (QKDN) is put forth, aiming to fulfill the requisite functionalities and validate its proof of concept implementation. A different architecture for optical networks secured by QKD, introducing the concept of Key as a Service, has been suggested in [118]. This architecture aims to overcome the challenges of robust deployment and utilization of keys effectively.

2) ADVANCEMENTS IN QUANTUM NETWORK

A link layer protocol for quantum networks has been proposed in [140]. This paves the way for platform-independent

TABLE 13. Quantum networks.

Quantum Networks	Title
QUANT-NET [135]	A testbed for quantum networking research over deployed fiber
LIQuIDNET [136]	Brookhaven National Laboratory Quantum Network Facility and The Long Island Quantum Information Distribution Network (LiQuiDNET) Testbed
Chicago Quantum Exchange + Toshiba [137]	Quantum security trials with Toshiba have begun on 124-mile quantum network; open soon to industry and academics for testing
DC-QNet [138]	Washington Metropolitan Quantum Network Research Consortium, DC-QNet Overview, Developing a Quantum Network Infrastructure
SECOQC [175]	The SECOQC quantum key distribution network in Vienna
IEQNET [140]	Illinois Express Quantum Network (IEQNET): Metropolitan-scale experimental quantum networking over deployed optical fiber
DARPA [141]	DARPA QUANTUM NETWORK
QuTech [179]	QuTech, Eurofiber and Juniper Networks partner to deploy a Quantum testbed in The Netherlands
China Mobile Ltd QKD Network [178]	Field and long-term demonstration of a wide area quantum key distribution network
EPB Quantum Network [142]	Architecture of a First-Generation Commercial Quantum Network
QSCOUT [143]	Engineering the quantum scientific computing open user testbed
IoT Quantum Network [144]	Using Quantum Nodes Connected via the Quantum Cloud to Perform IoT Quantum Network
Satellite Quantum Network [111]	Satellite-relayed intercontinental quantum network
Quantum Satellite Communication [168]	Quantum communication at 7,600 km and beyond
Ground to Satellite Communication [169]	Ground-to-satellite quantum teleportation
Satellite-Based Quantum Communication [170]	Satellite-Based Entanglement Distribution Over 1200 kilometers
MEO Satellite to Ground Station [150]	Exchange of single photons between a medium Earth orbit satellite and the ground station
Integrated Space-to-Ground Quantum Communication Network [171]	An integrated space-to-ground quantum communication network over 4,600 kilometres
QKD Networks in Europe [172]	Deployed QKD networks in Europe

software to be designed and implemented with scalable control and application protocols [140]. A technique for determining resource states that are optimized while requiring the least amount of storage was presented in [141], providing an entanglement topology that is customized for a particular quantum network operation. In [142], a realistic strategy for multidimensional quantum networks is put out. The authors show that basic quantum optical resources, such as weak coherent states, weak compressed states, and linear optics, can be used to address these difficulties. A routing protocol for optimal routing for quantum networks has been proposed in [143]. The problem of increasing the accessibility of Quantum Key Distribution (QKD) as a consumer technology is tackled by the work in [153]. It creates the first-ever quantum network connecting three separate countries by utilizing optical fibers installed by telecommunications firms throughout several European countries [153]. Techniques for improving Quantum network routing algorithms have been proposed in conjunction with the addition of quantum link evaluation criteria [111], [112], [113], [114]. A QKD network-based method for ensuring the security of electricity microgrids was described in references [115] and [116]. Simutation-based software frameworks for quantum networks are also presented in [97] and [99]. In the year 2020, a scientific experiment took place involving the ground stations located in Delingha and Nanshan. These stations were separated by a considerable distance of 1120 kilometers, as documented in reference [100]. An effort to develop a quantum access network that enables multimedia services linking optical network units (ONUs) was described in [117]. Through the use of a "N:N" splitter arrangement, this network permits direct quantum and conventional connections between ONUs at the same time. A theoretical investigation and proposal for multi-users utilizing the idea of entanglement have been provided in [104]. In order to smoothly integrate QKD into optical networks and hence increase their security, a research project proposed a Key as a Service architecture in [29].

The framework's capability as a workable and realistic candidate for the seamless incorporation of QKD into optical networks was highlighted by the performance evaluation that followed. A secret key assignment priority ordering policy is suggested in [119]. This increases the likelihood that quantum lightpaths will succeed in lessening the effects of blocking in QKD optical networks. For QKD in Space-Air-Ground Integrated Networks, [120] offers a resource allocation strategy utilizing stochastic programming. An integrated quantum communication network that stretches from orbit to the earth is demonstrated in [121]. This network combines a vast fiber network with more than 700 QKD links as well as two quick satellite-to-ground free-space QKD links. To achieve twin-field QKD, the sending-or-not-sending protocol described in [122] is used. This eliminates the need for a reliable repeater and enables the distribution of safe cryptographic keys over a prolonged 511 km long-haul fiber link that connects two faraway metropolitan areas. In [144], a mechanism for distributing quantum keys over an 830-kilometer cable using twin fields is described. A stable and effective 1,000 km-long terrestrial quantum-secure network is demonstrated in this paper. For QKD across optical backbone networks, a novel network topology incorporating a hybrid mix of trustworthy and untrusted relays is explained

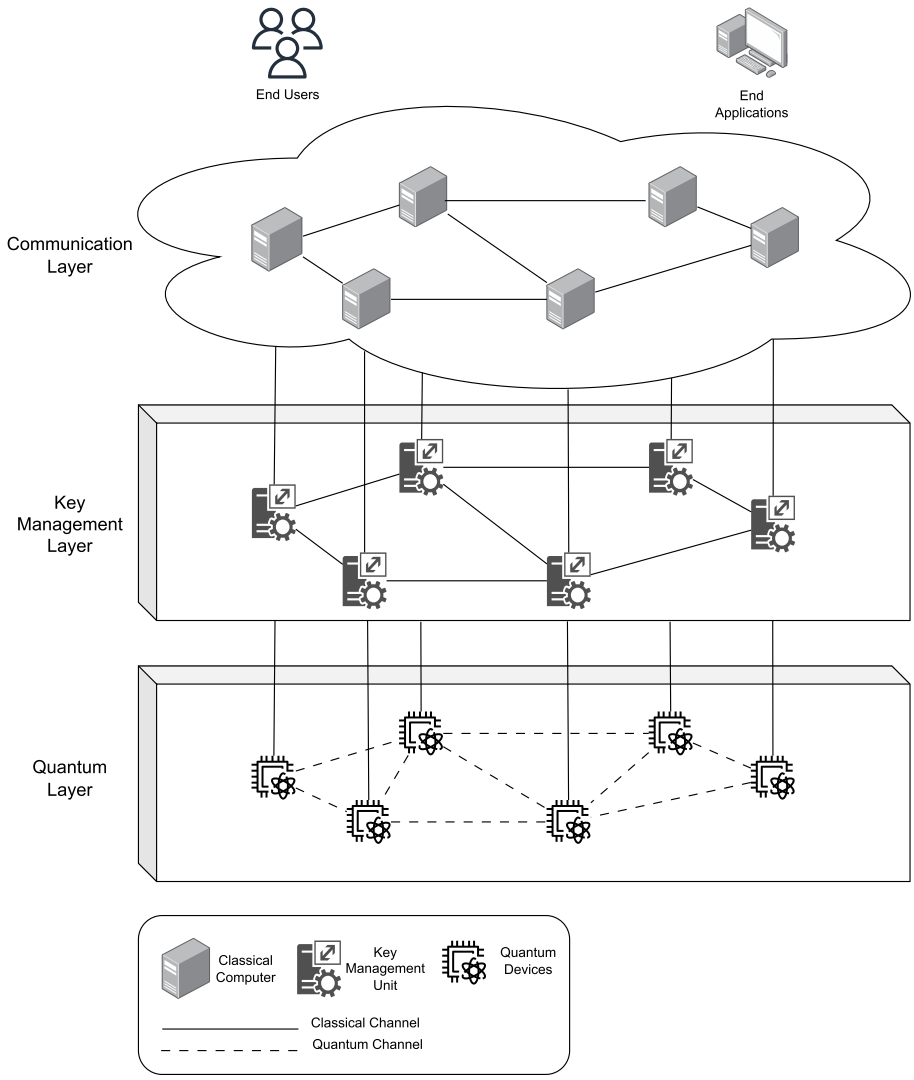


FIGURE 7. QKD network architecture.

in [123]. In addition to describing the architectural makeup of trustworthy and untrusted relay nodes, this article also develops corresponding models for network architecture, expenses, and security. A software-defined network (SDN) is used to implement a QKD network in [125], taking advantage of its advantages such as resource conservation through the identification of alternate routes and the monitoring of links to ascertain whether router network conditions are compatible with the requirements. The size of the changeable quantum key pool must take into account a number of things. In the beginning, security and accessibility must be balanced. Larger key pools can support a wider range of requirements, but they also increase security risks and add complexity to resource management. As a result, it is vital to balance security and accessibility, assuring both the appropriateness of the necessary pool size and the skillful administration and protection of keys [126]. [127] addresses the problem of guaranteeing safe packet routing in QKD networks at the highest achievable pace. This article introduces Tandem Queue Decomposition, a novel safe, and throughput-optimal method for the quick and secure routing of data in QKD networks. Using wavelength multiplexing and high-dimensional encoding based on arrival timings, [154] created a multi-user Quantum Key Distribution (QKD) network. For the widespread implementation of QKD networks, a variety of technologies are available, including i) trusted relays [129], ii) untrusted relays [123], iii) optical switches [117], [119], [126], iv) quantum relay [128]. A Model-Driven Satellite Quantum Communication Simulator has been developed recently as a result of research work [183], and it is intended to give flexibility and evolution in supporting new satellite quantum communications situations. Research work [121] that the network can be extended to a remote node more than 2,600 kilometers away by merging fiber and free-space QKD lines. This enables every user in the network to

communicate with others across a maximum distance of 4,600 kilometers.

Free-Space and Satellite Quantum Communication: It is imperative that space-based quantum networks are developed in order to enable worldwide secure communication. These networks overcome the restrictions of terrestrial infrastructure by ensuring safe and dependable data transfer over great distances through the use of satellites and other space technology [121], [163]. Communication may be shielded from interference, interception, and other weaknesses by using space-based technologies, which makes it an essential part of global safe data transmission [146]. A thorough framework for the conception, creation, application, and use of quantum technology in space is presented in [146]. Intercontinental quantum communication over a distance of 7,600 kilometers was demonstrated between Beijing and Vienna in 2017 [163]. The quantum teleportation of independent single-photon qubits over distances of up to 1,400 kilometers via an uplink channel between a ground observatory and a low-Earth orbit satellite is presented in research work [164]. The exchange of single photons between a medium Earth orbit (MEO) satellite and the ground station at the Matera Laser Ranging Observatory over a distance of 7000km is reported by the authors in [145]. The work in [147] uses multiple photon degrees of freedom to create new possibilities for the application of quantum physics to space communications. Studies like [148] and [150] show that satellite-based quantum communication is possible even in the daytime. The experiment in [149] shows that it is possible to identify individual photons that satellites broadcast. A Stable, low-error, and calibration-free polarization encoder for free-space quantum communication is proposed in [151]. At Padova, optics for free-space quantum communication is now being studied [152]. Eagle-1 is an experimental QKD system that will be sent into orbit by the European orbit Agency in late 2025 [184].

3) DEPLOYED QKD NETWORKS

Several QKD networks employing fiber-based configurations have been implemented in real-world scenarios. Examples encompass the DARPA [177], SECOQC [169], Tokyo QKD Network [170], SwissQuantum [171], Beijing-Shanghai QKD [162], Madrid quantum network [185], and Cambridge Quantum Network [109] QKD networks, space-to-ground QKD network [121]. The deployment of quantum key distribution (QKD) networks throughout Europe is covered in the research article [166], which includes various use-case examples. It describes testing carried out with commercial QKD systems at end-user sites, under real-world settings. An overview of global quantum key distribution (QKD) deployments is given in the report, [162] with a focus on important initiatives, innovations in technology, and partnerships. It addresses issues including scalability, infrastructure, and laws, as well as the reasons for using QKD to protect communications from potential dangers posed by quantum computing in the future. Important case studies from QKD hotspots including Europe, North America, and Asia highlight practical uses and advancements in QKD integration into current networks [162]. Table 14 presents the summary of deployed QKD networks.

4) CHALLENGES OF IMPLEMENTING QKD NETWORK IN A LARGE SCALE

While there exists a limited number of extended-range QKD implementations, a comprehensive knowledge of the weaknesses of these networks to different forms of attacks remains necessary. Prior to incorporating QKD networks into key infrastructure sectors, this understanding may be improved by adopting regulated benchmarking and analyzing methodologies. In [54], certain challenges related to QKD networks are outlined that go past hardware considerations. These challenges encompass the intrinsic disparities inherent in quantum communication and the efforts to address the constraints and flaws existing at the physical level. Although substantial advancements have been made in past years, some prominent challenges persist when it comes to the establishment of large-scale QKD networks. Within an article, an exploration is conducted into primary challenges associated with the large-scale implementation of QKD networks, encompassing aspects such as distance constraints, scalability, and interoperability, security, and resilience, as well as cost-effectiveness and accessibility. The article delves into how researchers are striving to address and surmount these challenges [186].

5) FUTURE PROSPECT

Despite above mentioned difficulties, the QKD network has made significant advancements recently, demonstrating its viability and potential in a variety of situations and applications. The future landscape of quantum communication and information security is poised to be significantly influenced by the QKD network, offering new opportunities and perspectives in a variety of industries and fields. The QKD network is dynamically and continuously changing, navigating new opportunities and difficulties.

F. RQ6: STATE-OF-THE-ART ON QUANTUM CRYPTOGRAPHY

QC, which is a ground-breaking method in the realm of cryptography, draws on the ideas of quantum physics and classical encryption. When compared to traditional encryption, it has certain significant benefits, especially in terms of unconditional security and the capacity to spot eavesdropping efforts [55]. These qualities address important communication security issues, offering substantial possibilities for protecting the future network. For assuring the security of numerous applications QC is particularly beneficial. Experimental research supports QC's capability for sniffer detection and unconditional security, indicating

TABLE 14. Summary of a few QKD networks.

Network	Project Year	QKD Network Type	QKD Protocol	Max. Key Rate	Longest Link Length	Node No.
DARPA [183]	2002 - 2006	Optical switch + trusted relay	BB84 Protocol	400 bps	29 km	10
SECOQC [175]	2004-2008	trusted relay	5 QKD protocols	3.1 kbps	33 km	6
TOKYO QKD [176]	2010	trusted relay	BB84, BBM92	304 kbps	90 km	6
Swiss Quantum [177]	2011	trusted relay	SARG04	2.4 kbps	17.1 km	3
Beijing Shanghai QKD [167]	2017	trusted relay	BB84	250 Kbps	43 km	32
Cambridge QKD [113]	2019	trusted relay	BB84	2.58 Mbps	10.6 km	3
Space-to-Ground Quantum Network [126]	2021	trusted relay	-	47.8 kbps	46000 km	32

its applicability for securing future networks [55], [168]. With the use of quantum physics and cryptography, it is possible to achieve theoretically perfect security. Because of its fundamental nature, any eavesdropper will be quickly identified before any critical information is sent [57]. The necessary technology is still being developed, though, so that its promise may be fully realized. Although certain hardware parts may already be available commercially, they are still regarded to be at a developing stage, and the protocols used to perform secure communications with this hardware still have space for development [47]. The study of QC relies heavily on simulations, which give researchers a useful tool to learn at a minimal cost. Researchers can gain valuable information from simulations that can help direct future developments in the subject [61]. This information supports the creation of novel communication protocols and assists in the continual improvement of real hardware systems [52]. Researchers may explore novel ideas and improve current procedures through the iterative simulation-based research process, ultimately paving the road for QC's future [25], [56]. The lack of urgency that is perceived, the practical difficulties that come with QKD, and the lack of widespread knowledge of its unique advantages are barriers to QKD's commercialization [192]. Given the potential uses for QKD in political and military settings, overcoming these difficulties necessitates critical government backing [53]. A collection of policy proposals for promoting the growth of QKD are presented in the study paper [178]. The foundation for a future quantum internet will be laid by creating a strong backbone QKD network, which will open up a variety of uses beyond secure communications and greatly increase the value of the network as a whole [15]. According to [193] there are various QKD solutions in use right now. The BB84 protocol was successfully deployed across a 100 km fiber link in 2008 by the University of Cambridge and Toshiba [168]. For lengths above 100 kilometers, the University of Geneva and Corning Inc. in 2015 achieved the longest distance and maximum bit rate [159]. Secure quantum key distribution over 421 km of optical fiber is presented in [160]. The Defence Research and Development Organisation in India tested its in-house QKD system in 2020 [174]. Although it is impractical to build optical linkages between all communication parties, attempts have been made to carry out QKD across empty space [146], [163], [165]. However, the signal-to-noise ratio may occasionally be too low for practical use, thus this means of communication is dependent on favourable air conditions. However, successful free space QKD tests have been carried out in China and Los Alamos [39], [60]. The QKD network is expanded to a remote node more than 2,600 kilometers away by merging the fiber and free-space QKD link, according to study in [121].

Several governments and academic institutions are presently using QC for safe key distribution [162]. To make this procedure easier, several organizations have created specialized quantum networks [161]. For Quantum Communication, a broad range of protocols have been put forth, and a lot of study has been done globally to evaluate and confirm their security [40]. KEEQuant in Germany [175] have introduced QKD systems to the commercial sector. Other businesses are actively working on research and development to produce QKD systems [161]. Quantum Communication systems have also been commercially implemented and demonstrated to show how useful this technology is [161]. These initiatives are intended to mitigate possible weaknesses brought on by advancing quantum computing [61]. Table 15 shows the existing research work in the field of QC technology [161], [194]. The market for QC is now estimated to be worth $128.9 million globally as of 2022, and by 2026, it is expected to grow dramatically to a revised size of $291.9 million, representing a strong Compound Annual Growth Rate (CAGR) of 20.8%. Notably, the United States now controls the greatest market share, accounting for 37.5% of the worldwide market, with China expected to surpass it in 2026 with a predicted market value of $40.6 million USD [194]. By 2030, the QC Market is expected to reach a worth of USD 455.3 million, according to research done by Fortune Business Insights. Within the forecast period of 2023 to 2030, its growth trajectory is expected to advance at a Compound Annual Growth Rate (CAGR) of 19.8% [195]. Researchers from China and Austria made history in 2017 when they successfully created the first international video connection using quantum encryption [187]. China and Austria set up a satellite link in January 2019 to allow for the exchange of quantum-encrypted data, including

TABLE 15. Existing research work in quantum cryptography.

Industry	Reference	Year	Quantum Cryptography Technology
USTC (China)	[111]	2017	Satellite to ground QKD
Chinese and Austrian research and Technology	[194]	2017	first-ever intercontinental, quantum-secured video call
Chinese and Austrian research and Technology	[195]	2018	quantum-secured messaging and video
Verizon	[196]	2020	trial of QKD was conducted
BT and Toshiba	[197] [198]	2022	first trial of a commercial quantum-secured metro network
Chicago Quantum Exchange + Toshiba	[197] [137]	2022	Quantum security trials with Toshiba have begun on 124-mile quantum network

photos and a video feed. This was a major first step towards the creation of a safe "quantum internet" [188]. Research documented in reference [107] disclosed the pioneering achievement of conducting a satellite-to-ground quantum communication experiment, spanning a distance of over 1200 km. In 2020 Verizon achieved the milestone in future-proofing data from hackers [189]. The first commercial experiment of a quantum-secured metropolitan network was presented by BT and Toshiba [190], [191]. Businesses are realizing more and more how important it is to use these solutions [181], QC becomes increasingly important in protecting our data and communications in the future. Findings related to this section are gathered from the analysis of these [5], [20], [25], [26], [30], [33], [39], [48], [52], [53], [55], [56], [60], [168] research work in literature.

G. RQ7: FUTURE RESEARCH ON QUANTUM CRYPTOGRAPHY

Future Implementation of QC:

The remarkable advantage of QC over conventional techniques has become more and more clear as it continues to be improved and developed. QC is still a relatively new and developing idea for many people and companies in the current environment. For their security requirements, most consumers continue to rely on non-quantum technologies. But this young technology is developing really quickly, with constant innovations. The need for increasingly advanced and reliable security solutions grows in tandem with these developments. Quantum computing's upcoming general use is anticipated to spark a paradigm change in the field of cryptography. One of the most sought-after technical developments in both the public and commercial sectors is likely to be QC. It is becoming increasingly clear that this cutting-edge sector has the capability to reform data security and transport. The emergence of QC and quantum computing holds the possibility of leading in a new age of security when encryption techniques are essentially impermeable to traditional computing approaches. QC's uses are expected to grow in the near future as it develops, touching on everything from financial organizations and political organizations to regular technological contacts. The security environment will change as organizations work to exploit QC's unprecedented capacity to protect sensitive data from an ever-evolving range of cyber threats. In conclusion, QC is still in its early phases but already shows incredible promise and supremacy. QC will surely become a crucial pillar of the digital future as the combination of quantum computing and encryption redefines security paradigms and raises protection to previously unheard-of heights.

Some of the other future research directions are listed below.

- QKD Protocols
- Quantum Repeaters
- Post-Quantum Cryptography
- Quantum Network Architectures
- Quantum Entanglement
- Quantum Hacking and Countermeasures
- Quantum Cryptographic Protocols for New Technologies
- Quantum Communication in Space
- Quantum Cryptography Standards
- Quantum-Secured Multi-Party Computation
- Quantum Cryptographic Hardware
- Quantum Cryptography in Cloud Computing

VI. THREATS TO VALIDITY

The validity of this study could be compromised by a number of possible dangers. We adhered to Kitchenham and Charters' SLR criteria [45] in order to reduce these hazards. The four primary categories of validity threats—construct validity, external validity, internal validity, and conclusion validity—are used to evaluate the risks that have been identified [196], [197].

A. INTERNAL VALIDITY

The degree to which particular circumstances affect the outcomes and analysis of the retrieved data is referred to as internal validity. Internal validity risks in this study could materialize in the following stages of the SLR:

1) SEARCH STRATEGY

As mentioned by [198], there is a chance that pertinent primary studies could be missed because of the search strings chosen and the overlap between the studies that were chosen. This is especially true when employing the snowballing approach. In Section IV-C, we outlined the search technique in detail to address this. The final search string was created using search phrases that were further improved via consensus sessions once a complete grasp of the research questions was obtained.

2) STUDY SELECTION AND QUALITY EVALUATION

The most pertinent studies were found by applying the inclusion and exclusion criteria described in Section IV-C to the search results. Next, each chosen study's quality was assessed based on the evaluation standards outlined in Section IV-D.

Data extraction: In SLR studies, personal bias presents a serious risk to data extraction. In Section IV-C, we developed a data extraction technique to guarantee consistency in the extraction of pertinent information in order to lessen this. As advised by [196], all writers took part in discussion meetings to clear up any ambiguities and confirm the information.

3) DATA SYNTHESIS

Improper categorization and mapping of data might lead to biased conclusions. Following the theme classification standards supplied by [199] allowed for the mitigation of this hazard. Furthermore, the acquired data was analyzed using a combination of quantitative and qualitative techniques.

B. EXTERNAL VALIDITY

The degree of generalizability of the study's findings is referred to as external validity. We attempted to improve generalizability, albeit we do not claim complete generalizability, by giving a concise summary of quantum software architecture, rationally arranging the data, and adhering to a strict SLR procedure. In order to choose the most pertinent peer-reviewed research and digital repositories, we followed the recommendations provided in [46]. Together with the SLR methodology and data extraction mechanism, the methodological features presented in Section IV and Figure 3 can aid in the identification of new studies and research issues. The goal of this strategy is to reduce risks to external validity.

C. CONSTRUCT VALIDITY

Making sure that the "data items" chosen from research appropriately reflect the material under examination is known as construct validity. There is a chance that data extraction was done incorrectly, maybe as a result of using the wrong search terms or omitting pertinent publications. In order to reduce this, we conducted research quality evaluations, developed inclusion/exclusion criteria, held group meetings to finalize the search string, and used a data extraction form to reduce interpersonal bias. To increase relevancy, the search term was additionally modified to fit the unique qualities of each database that was chosen.

D. VALIDITY OF CONCLUSION

The study's conclusions' level of plausibility and credibility is referred to as conclusion validity. As stated in Section IV, we used stringent selection criteria to guarantee that only high-quality studies with distinct objectives and assessments were included for analysis [45]. Even though this SLR offers insightful information, more work will be needed to modify the findings if new research becomes available, going outside the purview of the study at this time.

VII. CONCLUSION

Quantum cryptography has a greater impact than public key encryption technology. It has the ability to do what traditional encryption cannot, which is important since we expect the future development of quantum computers with super-computing powers. QC distinguishes itself with two key benefits: First off, it gives authorized communicators the ability to quickly identify possible buggers and take the necessary precautions. Second, QC makes sure that, despite their enormous processing power, eavesdroppers cannot compromise the quantum key. QC therefore becomes a vital technique for ensuring the communication security of upcoming networks. Both theoretical developments and experimental achievements have advanced significantly in recent years. With the help of these developments, QC will soon be widely used in network communications, ushering in a new era of quantum information. The ongoing development of QC gives reason to believe that the protection of communication security is about to undergo a revolution as we approach the dawn of the quantum communication era. In conclusion, this thorough systematic literature review has explored the complex world of QC. It has methodically investigated a variety of important research issues, starting with the investigation of the many uses of QC to guarantee network security in the quantum age. Additionally, it has looked at how quantum attacks can affect the future security of network communications. The review has not only pointed out and analyzed the difficulties and problems that QC faces, but it has also uncovered the complex methods that are used in this area. Additionally, it has examined the dynamic environment of QKD networks, highlighting the most recent developments and difficulties that will influence the direction of internet security. The review has carefully examined previous studies during this study, offering insightful analysis and discoveries that advance our understanding of QC's importance in the field of network security. As we come to a close, this literature analysis has also cast its eyes ahead, providing a glimpse of prospective research avenues that still need to be explored in the constantly developing field of QC. We aspire to open the door to a more safe and reliable digital future in the quantum age by combining our expertise and research in this manner.

REFERENCES

[1] A. Sarkar, S. R. Chatterjee, and M. Chakraborty, "Role of cryptography in network security," in *The 'Essence' of Network Security: An End-to-End Panorama*. Singapore: Springer, 2021, pp. 103–143.

[2] Y.-F. He and W.-P. Ma, "Three-party quantum secure direct communication against collective noise," *Quantum Inf. Process.*, vol. 16, no. 10, pp. 1–21, Oct. 2017.

[3] L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, "NIST: Report on post-quantum cryptography," NIST, Gaithersburg, MD, USA, Tech. Rep. NISTIR 8105, 2016.

[4] A. A. Khan, A. Ahmad, M. Waseem, P. Liang, M. Fahmideh, T. Mikkonen, and P. Abrahamsson, "Software architecture for quantum computing systems—A systematic review," *J. Syst. Softw.*, vol. 201, Jul. 2023, Art. no. 111682.
[5] J.-P. Aumasson, "The impact of quantum computing on cryptography," *Comput. Fraud Secur.*, vol. 2017, no. 6, pp. 8–11, 2017.
[6] J. Daemen and V. Rijmen, *The Design of Rijndael*, vol. 2. Cham, Switzerland: Springer, 2002.
[7] R. L. Rivest, "The RC5 encryption algorithm," in *Proc. Int. Workshop Fast Softw. Encryption*. Cham, Switzerland: Springer, 1994, pp. 86–96.
[8] N. Koblitz, "Elliptic curve cryptosystems," *Math. Comput.*, vol. 48, no. 177, pp. 203–209, 1987.
[9] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 26, no. 1, pp. 96–99, Jan. 1983.
[10] D. Alvarez and Y. Kim, "Survey of the development of quantum cryptography and its applications," in *Proc. IEEE 11th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Jan. 2021, pp. 1074–1080.
[11] E. Lella, A. Gatto, A. Pazienza, D. Romano, P. Noviello, F. Vitulano, and G. Schmid, "Cryptography in the quantum era," in *Proc. IEEE 15th Workshop Low Temp. Electron. (WOLTE)*, Jun. 2022, pp. 1–4.
[12] D. J. Bernstein and L. Tanja, "Post-quantum cryptography," *Nature*, vol. 549, no. 7671, pp. 188–194, 2017.
[13] P. W. Shor, "Algorithms for quantum computation: Discrete logarithms and factoring," in *Proc. 35th Annu. Symp. Found. Comput. Sci.*, 1994, pp. 124–134.
[14] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 212–219.
[15] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum cryptography for the future Internet and the security analysis," *Secur. Commun. Netw.*, vol. 2018, pp. 1–7, Jun. 2018.
[16] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography review mod," Group Appl. Phys. (GAP), Univ. Geneva, Geneva, Switzerland, Tech. Rep., 2002.
[17] S. Wiesner, "Conjugate coding," *ACM SIGACT News*, vol. 15, no. 1, pp. 78–88, Jan. 1983.
[18] W. N.-U. Ain, M. A.-U. Rahman, M. Nadeem, and A. G. Abbasi, "Quantum cryptography trends: A milestone in information security," in *Proc. Hybrid Intell. Syst., 15th Int. Conf. HIS 2015 Hybrid Intell. Syst.*, Seoul, South Korea. Cham, Switzerland: Cham, Switzerland: Springer, 2015, pp. 25–39.
[19] B. A. Alhayani, O. A. AlKawak, H. B. Mahajan, H. Ilhan, and R. M. Qasem, "Design of quantum communication protocols in quantum cryptography," *Wireless Pers. Commun.*, vol. 2023, pp. 1–18, Jul. 2023.
[20] S. Mitra, B. Jana, S. Bhattacharya, P. Pal, and J. Poray, "Quantum cryptography: Overview, security issues and future challenges," in *Proc. 4th Int. Conf. Opto-Electron. Appl. Opt. (Optronix)*, Nov. 2017, pp. 1–7.
[21] A. Ahmad, M. Waseem, P. Liang, M. Fahmideh, M. S. Aktar, and T. Mikkonen, "Towards human-bot collaborative software architecting with ChatGPT," in *Proc. 27th Int. Conf. Eval. Assessment Softw. Eng.*, Jun. 2023, pp. 279–285.
[22] J. Li, N. Li, Y. Zhang, S. Wen, W. Du, W. Chen, and W. Ma, "A survey on quantum cryptography," *Chin. J. Electron.*, vol. 27, no. 2, pp. 223–228, 2018.
[23] A. A. Abushgra, "Variations of QKD protocols based on conventional system measurements: A literature review," *Cryptography*, vol. 6, no. 1, p. 12, Mar. 2022.
[24] H. Shu, "Quantum key distribution based on orthogonal state encoding," *Int. J. Theor. Phys.*, vol. 61, no. 12, p. 271, Dec. 2022.
[25] Y.-B. Sheng, L. Zhou, and G.-L. Long, "One-step quantum secure direct communication," *Sci. Bull.*, vol. 67, no. 4, pp. 367–374, Feb. 2022.
[26] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, and L. Hanzo, "The evolution of quantum key distribution networks: On the road to the qinternet," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 839–894, 2nd Quart., 2022.
[27] A. Trizna and A. Ozols, "An overview of quantum key distribution protocols," *Inf. Technol. Manage. Sci.*, vol. 21, pp. 37–44, Dec. 2018.
[28] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," 2020, *arXiv:2003.06557*.
[29] Wikipedia. (2010). *Quantum Cryptography*. Accessed: Jun. 5, 2023. [Online]. Available: https://en.wikipedia.org/wiki/Quantum
[30] M. Barbeau, E. Kranakis, and N. Perez, "Authenticity, integrity, and replay protection in quantum data communications and networking," *ACM Trans. Quantum Comput.*, vol. 3, no. 2, pp. 1–22, Jun. 2022.
[31] R. Alléaume et al., "Using quantum key distribution for cryptographic purposes: A survey," *Theor. Comput. Sci.*, vol. 560, pp. 62–81, Dec. 2014.
[32] D. Giampouris, "Short review on quantum key distribution protocols," in *GeNeDis 2016: Computational Biology and Bioinformatics*. London, U.K.: Nature Publishing Group, 2016, pp. 149–157.
[33] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *npj Quantum Inf.*, vol. 2, no. 1, pp. 1–12, Nov. 2016.
[34] G.-L. Long, "Quantum secure direct communication: Principles, current status, perspectives," in *Proc. IEEE 85th Veh. Technol. Conf. (VTC Spring)*, Jun. 2017, pp. 1–5.
[35] A. Kumar and S. Garhwal, "State-of-the-art survey of quantum cryptography," *Arch. Comput. Methods Eng.*, vol. 28, no. 5, pp. 3831–3868, Aug. 2021.
[36] K. W. Hong, O.-M. Foong, and T. J. Low, "Challenges in quantum key distribution: A review," in *Proc. 4th Int. Conf. Inf. Netw. Secur.*, 2016, pp. 29–33.
[37] H. Jasoliya and K. Shah, "An exploration to the quantum cryptography technology," in *Proc. 9th Int. Conf. Comput. Sustain. Global Develop. (INDIACom)*, Mar. 2022, pp. 506–510.
[38] R. Kavuri, S. Voruganti, S. Mohammed, S. Inapanuri, and B. H. Goud, "Quantum cryptography with an emphasis on the security analysis of qkd protocols," *Evol. Appl. Quantum Comput.*, vol. 2023, pp. 265–288, May 2023.
[39] A. Aji, K. Jain, and P. Krishnan, "A survey of quantum key distribution (QKD) network simulation platforms," in *Proc. 2nd Global Conf. Advancement Technol. (GCAT)*, Oct. 2021, pp. 1–8.
[40] S. R. Hasan, M. Z. Chowdhury, M. Saiam, and Y. M. Jang, "Quantum communication systems: Vision, protocols, applications, and challenges," *IEEE Access*, vol. 11, pp. 15855–15877, 2023.
[41] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.
[42] S. K. Sahu and K. Mazumdar, "State-of-the-art analysis of quantum cryptography: Applications and future prospects," *Frontiers Phys.*, vol. 12, Aug. 2024, Art. no. 1456491.
[43] S. Sonko, K. I. Ibekwe, V. I. Ilojianya, E. A. Etukudoh, and A. Fabuyide, "Quantum cryptography and us digital security: A comprehensive review: Investigating the potential of quantum technologies in creating unbreakable encryption and their future in national security," *Comput. Sci. IT Res. J.*, vol. 5, no. 2, pp. 390–414, Feb. 2024.
[44] N. Aquina, S. Rommel, and I. T. Monroy, "Quantum secure communication using hybrid post-quantum cryptography and quantum key distribution," in *Proc. 24th Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2024, pp. 1–4.
[45] S. Keele, "Guidelines for performing systematic literature reviews in software engineering," School Comput. Sci., Univ. Durham, Durham, U.K., Tech. Rep.EBSE-2007-01, 2007.
[46] L. Chen, M. A. Babar, and H. Zhang, "Towards an evidence-based understanding of electronic data sources," in *Proc. 14th Int. Conf. Eval. Assessment Softw. Eng. (EASE)*, 2010, pp. 1–13.
[47] E. Diamanti, "Addressing practical challenges in quantum cryptography," in *Proc. 45th Eur. Conf. Opt. Commun. (ECOC)*, Sep. 2019, pp. 1–2.
[48] K. Balygin, V. Zaitsev, A. N. Klimov, A. I. Klimov, S. P. Kulik, and S. N. Molotkov, "Practical quantum cryptography," *JETP Lett.*, vol. 105, pp. 606–612, Jun. 2017.
[49] F. Cavaliere, J. Mattsson, and B. Smeets, "The security implications of quantum cryptography and quantum computing," *Netw. Secur.*, vol. 2020, no. 9, pp. 9–15, Sep. 2020.
[50] S. Roy and A. Ghosh, "Securing medical images using quantum key distribution scheme bb84," in *Proc. Int. Conf. Innov. Data Anal.* Cham, Switzerland: Springer, 2022, pp. 585–594.
[51] A. Ahmad, A. A. Khan, M. Waseem, M. Fahmideh, and T. Mikkonen, "Towards process centered architecting for quantum software systems," in *Proc. IEEE Int. Conf. Quantum Softw. (QSW)*, Jul. 2022, pp. 26–31.

[52] A. Nanda, D. Puthal, S. P. Mohanty, and U. Choppali, "A computing perspective of quantum cryptography [Energy and Security]," *IEEE Consum. Electron. Mag.*, vol. 7, no. 6, pp. 57–59, Nov. 2018.

[53] N. S. Agency. (2023). *Quantum Key Distribution (qkd) and Quantum Cryptography (qc)*. Accessed: Jun. 5, 2023. [Online]. Available: https://www.nsa.gov/Cybersecurity/QuantumKey-Distribution-QKD-and-Quantum-Cryptography-QC/

[54] W. Kozlowski and S. Wehner, "Towards large-scale quantum networks," in *Proc. 6th Annu. ACM Int. Conf. Nanosc. Comput. Commun.*, Sep. 2019, pp. 1–7.

[55] F. Grasselli, "Quantum cryptography," in *Quantum Science and Technology*. Cham, Switzerland: Springer, 2021.

[56] M. Mehic, M. Niemiec, S. Rass, J. Ma, M. Peev, A. Aguado, V. Martin, S. Schauer, A. Poppe, and C. Pacher, "Quantum key distribution: A networking perspective," *ACM Comput. Surv. (CSUR)*, vol. 53, no. 5, pp. 1–41, 2020.

[57] C.-Y. Chen, G.-J. Zeng, F.-J. Lin, Y.-H. Chou, and H.-C. Chao, "Quantum cryptography and its applications over the Internet," *IEEE Netw.*, vol. 29, no. 5, pp. 64–69, Sep. 2015.

[58] U. Vazirani and T. Vidick, "Fully device independent quantum key distribution," *Commun. ACM*, vol. 62, no. 4, p. 133, Mar. 2019.

[59] A. P. Bhatt and A. Sharma, "Quantum cryptography for Internet of Things security," *J. Electron. Sci. Technol.*, vol. 17, no. 3, pp. 213–220, 2019.

[60] G. Alagic, T. Gagliardoni, and C. Majenz, "Unforgeable quantum encryption," in *Proc. Annu. Int. Conf. theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 2018, pp. 489–519.

[61] S. Wang, M. Rohde, and A. Ali, "Quantum cryptography and simulation: Tools and techniques," in *Proc. 4th Int. Conf. Cryptogr., Secur. Privacy*, Jan. 2020, pp. 36–41.

[62] S. N. Molotkov, "Trojan horse attacks, decoy state method, and side channels of information leakage in quantum cryptography," *J. Experim. Theor. Phys.*, vol. 130, no. 6, pp. 809–832, Jun. 2020.

[63] S. N. Molotkov, "On eavesdropping in quantum cryptography through side channels of information leakage," *JETP Lett.*, vol. 111, no. 11, pp. 653–661, Jun. 2020.

[64] Z. Hu, Y. Vasiliu, O. Smirnov, V. Sydorenko, and Y. Polishchuk, "Abstract model of eavesdropper and overview on attacks in quantum cryptography systems," in *Proc. 10th IEEE Int. Conf. Intell. Data Acquisition Adv. Comput. Syst., Technol. Appl. (IDAACS)*, vol. 1, Sep. 2019, pp. 399–405.

[65] Y.-G. Yang, Y.-C. Wang, Y.-L. Yang, X.-B. Chen, D. Li, Y.-H. Zhou, and W.-M. Shi, "Participant attack on the deterministic measurement-device-independent quantum secret sharing protocol," *Sci. China Phys., Mech. Astron.*, vol. 64, no. 6, Jun. 2021, Art. no. 260321.

[66] D. Park, G. Kim, D. Heo, S. Kim, H. Kim, and S. Hong, "Single trace side-channel attack on key reconciliation in quantum key distribution system and its efficient countermeasures," *ICT Exp.*, vol. 7, no. 1, pp. 36–40, Mar. 2021.

[67] B. Liu, D. Xiao, H.-Y. Jia, and R.-Z. Liu, "Collusive attacks to," *Quantum Inf. Process.*, vol. 15, pp. 2113–2124, 2016.

[68] Y.-Y. Fei, X.-D. Meng, M. Gao, H. Wang, and Z. Ma, "Quantum man-in-the-middle attack on the calibration process of quantum key distribution," *Sci. Rep.*, vol. 8, no. 1, p. 4283, Mar. 2018.

[69] C. Navas-Merlo and J. C. Garcia-Escartin, "Detector blinding attacks on counterfactual quantum key distribution," *Quantum Inf. Process.*, vol. 20, no. 6, p. 196, Jun. 2021.

[70] M. E. Sabani, I. K. Savvas, D. Poulakis, G. C. Makris, and M. A. Butakova, "The bb84 quantum key distribution protocol and potential risks," in *Proc. Int. Congr. Inf. Commun. Technol.* Cham, Switzerland: Springer, 2023, pp. 429–437.

[71] P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Security of continuous-variable quantum key distribution against canonical attacks," in *Proc. Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2021, pp. 1–6.

[72] J. Gu, X.-Y. Cao, Y. Fu, Z.-W. He, Z.-J. Yin, H.-L. Yin, and Z.-B. Chen, "Experimental measurement-device-independent type quantum key distribution with flawed and correlated sources," *Sci. Bull.*, vol. 67, no. 21, pp. 2167–2175, Nov. 2022.

[73] A. Agarwal, J. Bartusek, D. Khurana, and N. Kumar, "A new framework for quantum oblivious transfer," in *Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn.* Cham, Switzerland: Springer, 2023, pp. 363–394.

[74] R. Srikanth, "Quantum bit commitment and the reality of the quantum state," *Found. Phys.*, vol. 48, no. 1, pp. 92–109, Jan. 2018.

[75] A. Nayak, J. Sikora, and L. Tunçel, "A search for quantum coin-flipping protocols using optimization techniques," *Math. Program.*, vol. 156, nos. 1–2, pp. 581–613, Mar. 2016.

[76] F. Furrer, T. Gehring, C. Schaffner, C. Pacher, R. Schnabel, and S. Wehner, "Continuous-variable protocol for oblivious transfer in the noisy-storage model," *Nature Commun.*, vol. 9, no. 1, p. 1450, Apr. 2018.

[77] M. Junge, A. M. Kubicki, C. Palazuelos, and D. Pérez-García, "Geometry of Banach spaces: A new route towards position based cryptography," *Commun. Math. Phys.*, vol. 394, no. 2, pp. 625–678, Sep. 2022.

[78] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, "Position based cryptography with location privacy: A step for fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 799–806, Jan. 2018.

[79] F. Grasselli and F. Grasselli, "Device-independent quantum cryptography," in *Proc. Quantum Cryptogr., Key Distrib. Conf. Key Agreement*. Cham, Switzerland: Springer, 2021, pp. 105–148.

[80] P. A. Shemin and K. S. Vipinkumar, "E—Payment system using visual and quantum cryptography," *Proc. Technol.*, vol. 24, pp. 1623–1628, Jul. 2016.

[81] T. Hassan and F. Ahmed, "Transaction and identity authentication security model for e-banking: Confluence of quantum cryptography and ai," in *Proc. 1st Int. Conf. Intell. Technol. Appl. (INTAP)*, Bahawalpur, Pakistan. Cham, Switzerland: Springer, 2018, pp. 338–347.

[82] U. P. Madje and M. B. Pande, "Use of quantum cryptography environment for authentication in online banking transactions security," in *Proc. IEEE 2nd Int. Conf. Technol., Eng., Manage. Societal Impact Using Marketing, Entrepreneurship Talent (TEMSMET)*, Dec. 2021, pp. 1–8.

[83] S. K. Routray, M. K. Jha, L. Sharma, R. Nyamangoudar, A. Javali, and S. Sarkar, "Quantum cryptography for IoT: APerspective," in *Proc. Int. Conf. IoT Appl. (ICIOT)*, May 2017, pp. 1–4.

[84] H. Amellal, A. Meslouhi, and A. E. Allati, "Secure big data using QKD protocols," *Proc. Comput. Sci.*, vol. 148, pp. 21–29, Jul. 2019.

[85] J. Han, Y. Liu, X. Sun, and L. Song, "Enhancing data and privacy security in mobile cloud computing through quantum cryptography," in *Proc. 7th IEEE Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Aug. 2016, pp. 398–401.

[86] M. Thangapandiyan, P. M. R. Anand, and K. S. Sankaran, "Quantum key distribution and cryptography mechanisms for cloud data security," in *Proc. Int. Conf. Commun. Signal Process. (ICCSP)*, Apr. 2018, pp. 1031–1035.

[87] R. Aluvalu, K. K. Chennam, V. U. Maheswari, and M. Jabbar, "A novel and secure approach for quantum key distribution in a cloud computing environment," in *Intelligent Computing and Networking: Proceedings of IC-ICN 2020*. Cham, Switzerland: Springer, 2020, pp. 271–283.

[88] M. S. Rahman and M. Hossam-E-Haider, "Quantum IoT: A quantum approach in IoT security maintenance," in *Proc. Int. Conf. Robot., Elect. Signal Process. Techn. (ICREST)*, Jan. 2019, pp. 269–272.

[89] K. Sundar, S. Sasikumar, C. Jayakumar, D. Nagarajan, and S. Karthick, "Quantum cryptography based cloud security model (QC-CSM) for ensuring cloud data security in storage and accessing," *Multimedia Tools Appl.*, vol. 82, no. 27, pp. 42817–42832, Nov. 2023.

[90] M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, and N. Kumar, "Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications," *J. Inf. Secur. Appl.*, vol. 56, Feb. 2021, Art. no. 102673.

[91] A. M. Perumal and E. R. S. Nadar, "Architectural framework and simulation of quantum key optimization techniques in healthcare networks for data security," *J. Ambient Intell. Humanized Comput.*, vol. 12, pp. 7173–7180, Oct. 2021.

[92] G. Sharma and S. Kalra, "Identity based secure authentication scheme based on quantum key distribution for cloud computing," *Peer-Peer Netw. Appl.*, vol. 11, pp. 220–234, May 2018.

[93] J. Pinnell, I. Nape, M. de Oliveira, N. TabeBordbar, and A. Forbes, "Experimental demonstration of 11-dimensional 10-party quantum secret sharing," *Laser Photon. Rev.*, vol. 14, no. 9, 2020, Art. no. 2000012.

[94] G. Murali and R. S. Prasad, "Secured cloud authentication using quantum cryptography," in *Proc. Int. Conf. Energy, Commun., Data Anal. Soft Comput. (ICECDS)*, Aug. 2017, pp. 3753–3756.

[95] S. Gupta, A. Gupta, I. Y. Pandya, A. Bhatt, and K. Mehta, "End to end secure e-voting using blockchain & quantum key distribution," *Mater. Today, Proc.*, vol. 80, pp. 3363–3370, Jul. 2023.

[96] M. Mehic, O. Maurhart, S. Rass, and M. Voznak, "Implementation of quantum key distribution network simulation module in the network simulator NS-3," *Quantum Inf. Process.*, vol. 16, no. 10, pp. 1–23, Oct. 2017.

[97] R. Satoh, M. Hajdušek, N. Benchasattabuse, S. Nagayama, K. Teramoto, T. Matsuo, S. A. Metwalli, P. Pathumsoot, T. Satoh, S. Suzuki, and R. V. Meter, "QuISP: A quantum Internet simulation package," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Sep. 2022, pp. 353–364.
[98] S. Alhazmi, P. Kandel, J. Sabovik, N. Matondo-Mvula, and K. Elleithy, "Mitigating man-in-the-middle attack using quantum key distribution," in *Proc. IEEE Long Island Syst., Appl. Technol. Conf. (LISAT)*, May 2023, pp. 1–6.
[99] S. Diadamo, J. Nötzel, B. Zanger, and M. M. Bese, "QuNetSim: A software framework for quantum networks," *IEEE Trans. Quantum Eng.*, vol. 2, pp. 1–12, 2021.
[100] J. Yin et al., "Entanglement-based secure quantum cryptography over 1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501–505, Jun. 2020.
[101] I. Burak Adiyaman and I. Sogukpinar, "Simulation of BB84 quantum key exchange protocol and attack analysis," in *Proc. 5th Int. Conf. Comput. Sci. Eng. (UBMK)*, Sep. 2020, pp. 203–207.
[102] N. Gopinath and S. P. Shyry, "Side channel attack free quantum key distribution using entangled fuzzy logic," *Brazilian J. Phys.*, vol. 53, no. 2, p. 35, Apr. 2023.
[103] M. Bozzio, A. Orieux, L. T. Vidarte, I. Zaquine, I. Kerenidis, and E. Diamanti, "Experimental investigation of practical unforgeable quantum money," *Npj Quantum Inf.*, vol. 4, no. 1, p. 5, Jan. 2018.
[104] P. Xue, K. Wang, and X. Wang, "Efficient multiuser quantum cryptography network based on entanglement," *Sci. Rep.*, vol. 7, no. 1, p. 45928, Apr. 2017.
[105] C.-Y. Zhang and Z.-J. Zheng, "Entanglement-based quantum key distribution with untrusted third party," *Quantum Inf. Process.*, vol. 20, no. 4, pp. 1–20, Apr. 2021.
[106] S. Wengerowsky, S. K. Joshi, F. Steinlechner, H. Hübel, and R. Ursin, "An entanglement-based wavelength-multiplexed quantum communication network," *Nature*, vol. 564, no. 7735, pp. 225–228, Dec. 2018.
[107] S.-K. Liao et al., "Satellite-to-ground quantum key distribution," *Nature*, vol. 549, no. 7670, pp. 43–47, Aug. 2017.
[108] H.-Y. Su, "Simple analysis of security of the BB84 quantum key distribution protocol," *Quantum Inf. Process.*, vol. 19, no. 6, p. 169, Jun. 2020.
[109] J. F. Dynes, A. Wonfor, W. W.-S. Tam, A. W. Sharpe, R. Takahashi, M. Lucamarini, A. Plews, Z. L. Yuan, A. R. Dixon, J. Cho, Y. Tanizawa, J.-P. Elbers, H. Greißer, I. H. White, R. V. Penty, and A. J. Shields, "Cambridge quantum network," *Npj Quantum Inf.*, vol. 5, no. 1, p. 101, Nov. 2019.
[110] T. Choi, S. Yoon, T. Y. Kim, and H. Kim, "Design and implementation of quantum key distribution network control and management," in *Proc. Int. Conf. Inf. Commun. Technol. Converg. (ICTC)*, Oct. 2021, pp. 724–727.
[111] Y. Tanizawa, R. Takahashi, and A. R. Dixon, "A routing method designed for a quantum key distribution network," in *Proc. 8th Int. Conf. Ubiquitous Future Netw. (ICUFN)*, Jul. 2016, pp. 208–214.
[112] M. Mehic, P. Fazio, S. Rass, O. Maurhart, M. Peev, A. Poppe, J. Rozhon, M. Niemiec, and M. Voznak, "A novel approach to quality-of-service provisioning in trusted relay quantum key distribution networks," *IEEE/ACM Trans. Netw.*, vol. 28, no. 1, pp. 168–181, Feb. 2020.
[113] F. Hahn, A. Pappa, and J. Eisert, "Quantum network routing and local complementation," *npj Quantum Inf.*, vol. 5, no. 1, p. 76, Sep. 2019.
[114] O. Amer, W. O. Krawec, and B. Wang, "Efficient routing for quantum key distribution networks," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Oct. 2020, pp. 137–147.
[115] Z. Tang, Y. Qin, Z. Jiang, W. O. Krawec, and P. Zhang, "Quantum-secure networked microgrids," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2020, pp. 1–5.
[116] Z. Tang, P. Zhang, W. O. Krawec, and Z. Jiang, "Programmable quantum networked microgrids," *IEEE Trans. Quantum Eng.*, vol. 1, pp. 1–13, 2020.
[117] C. Cai, Y. Sun, J. Niu, and Y. Ji, "A quantum access network suitable for internetworking optical network units," *IEEE Access*, vol. 7, pp. 92091–92099, 2019.
[118] Y. Cao, Y. Zhao, J. Wang, X. Yu, Z. Ma, and J. Zhang, "KaaS: Key as a service over quantum key distribution integrated optical networks," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 152–159, May 2019.
[119] P. Sharma, V. Bhatia, and S. Prakash, "Efficient ordering policy for secret key assignment in quantum key distribution-secured optical networks," *Opt. Fiber Technol.*, vol. 68, Jan. 2022, Art. no. 102755.
[120] R. Kaewpuang, M. Xu, D. Niyato, H. Yu, and Z. Xiong, "Resource allocation in quantum key distribution (QKD) for space-air-ground integrated networks," in *Proc. IEEE 27th Int. Workshop Comput. Aided Model. Design Commun. Links Netw. (CAMAD)*, Nov. 2022, pp. 71–76.
[121] Y.-A. Chen et al., "An integrated space-to-ground quantum communication network over 4,600 kilometres," *Nature*, vol. 589, no. 7841, pp. 214–219, Jan. 2021.
[122] J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, Z.-Y. Han, S.-Z. Ma, X.-L. Hu, Y.-H. Li, H. Liu, F. Zhou, H.-F. Jiang, T.-Y. Chen, H. Li, L.-X. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," *Nature Photon.*, vol. 15, no. 8, pp. 570–575, Aug. 2021.
[123] Y. Cao, Y. Zhao, J. Li, R. Lin, J. Zhang, and J. Chen, "Hybrid trusted/untrusted relay-based quantum key distribution over optical backbone networks," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 9, pp. 2701–2718, Sep. 2021.
[124] S. K. Sehgal and R. Gupta, "SOA based BB84 protocol for enhancing quantum key distribution in cloud environment," *Wireless Pers. Commun.*, vol. 130, no. 3, pp. 1759–1793, Jun. 2023.
[125] V. Monita, R. Munadi, and I. D. Irawati, "A quantum key distribution network routing performance based on software-defined network," in *Proc. IEEE 13th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Mar. 2023, pp. 1121–1125.
[126] Q. Zhang, O. Ayoub, A. Gatto, J. Wu, F. Musumeci, and M. Tornatore, "Routing, channel, key-rate and time-slot assignment for QKD in optical networks," *IEEE Trans. Netw. Service Manage.*, vol. 21, no. 1, pp. 148–160, Jan. 2023.
[127] M. S. Akhtar, G. Krishnakumar, V. Vishnu, and A. Sinha, "Fast and secure routing algorithms for quantum key distribution networks," *IEEE/ACM Trans. Netw.*, vol. 31, no. 5, pp. 2281–2296, Oct. 2023.
[128] Z.-D. Li, R. Zhang, X.-F. Yin, L.-Z. Liu, Y. Hu, Y.-Q. Fang, Y.-Y. Fei, X. Jiang, J. Zhang, L. Li, N.-L. Liu, F. Xu, Y.-A. Chen, and J.-W. Pan, "Experimental quantum repeater without quantum memory," *Nature Photon.*, vol. 13, no. 9, pp. 644–648, Sep. 2019.
[129] X. Yu, Y. Liu, X. Zou, Y. Cao, Y. Zhao, A. Nag, and J. Zhang, "Secret-key provisioning with collaborative routing in partially-trusted-relay-based quantum-key-distribution-secured optical networks," *J. Lightw. Technol.*, vol. 40, no. 12, pp. 3530–3545, Jun. 15, 2022.
[130] I. Monga, E. Saglamyurek, E. Kissel, H. Haffner, and W. Wu, "QUANT-NET: A testbed for quantum networking research over deployed fiber," in *Proc. 1st Workshop Quantum Netw. Distrib. Quantum Comput.*, Sep. 2023, pp. 31–37.
[131] N. Delcour, L. Duncan, S. Frahm, P. Lancaster, and L. Vann, "Estimation of technology convergence by 2035," Mad Scientist Fellows Strategic Res. Project, U.S. Army War College, Carlisle, PA, USA, Tech. Rep., 2035.
[132] M. Fore, "Quantum security trials with toshiba have begun on 124-mile quantum network; open soon to industry and academics for testing," *UWIRE Text*, Jun. 2022.
[133] L. D. Cooper, "Washington metropolitan quantum network research consortium, DC-Qnet overview, developing a quantum network infrastructure," in *Proc. Quantum World Congress*, 2022.
[134] L. O. Mailloux, D. D. Hodson, M. R. Grimaila, R. D. Engle, C. V. Mclaughlin, and G. B. Baumgartner, "Using modeling and simulation to study photon number splitting attacks," *IEEE Access*, vol. 4, pp. 2188–2197, 2016.
[135] J. Chung, G. Kanter, N. Lauk, R. Valivarthi, W. Wu, R. R. Ceballos, C. Peña, N. Sinclair, J. Thomas, S. Xie, R. Kettimuthu, P. Kumar, P. Spentzouris, and M. Spiropulu, "Illinois express quantum network (IEQNet): Metropolitan-scale experimental quantum networking over deployed optical fiber," *Proc. SPIE*, vol. 11726, May 2021, Art. no. 1172602.
[136] C. Elliott, "The darpa quantum network," in *Quantum Communications and Cryptography*. Boca Raton, FL, USA: CRC Press, 2018, pp. 91–110.
[137] D. Earl, K. Karunaratne, J. Schaake, R. Strum, P. Swingle, and R. Wilson, "Architecture of a first-generation commercial quantum network," 2022, *arXiv:2211.14871*.
[138] S. M. Clark, D. Lobser, M. C. Revelle, C. G. Yale, D. Bossert, A. D. Burch, M. N. Chow, C. W. Hogle, M. Ivory, J. Pehr, B. Salzbrenner, D. Stick, W. Sweatt, J. M. Wilson, E. Winrow, and P. Maunz, "Engineering the quantum scientific computing open user testbed," *IEEE Trans. Quantum Eng.*, vol. 2, pp. 1–32, 2021.

[139] D. Subhi and L. Bacsardi, "Using quantum nodes connected via the quantum cloud to perform IoT quantum network," *Condens. Matter*, vol. 8, no. 1, p. 24, Feb. 2023.

[140] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpedek, M. Pompili, A. Stolk, P. Pawelczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, and S. Wehner, "A link layer protocol for quantum networks," *Proc. ACM Int. Group Data Commun. (SIGCOMM)*, vol. 2019, pp. 159–173, Jul. 2019.

[141] J. Miguel-Ramiro, A. Pirker, and W. Dür, "Optimized quantum networks," *Quantum*, vol. 7, p. 919, Feb. 2023.

[142] D. Bacco, J. F. F. Bulmer, M. Erhard, M. Huber, and S. Paesani, "Proposal for practical multidimensional quantum networks," *Phys. Rev. A*, vol. 104, no. 5, Nov. 2021, Art. no. 052618.

[143] M. Caleffi, "Optimal routing for quantum networks," *IEEE Access*, vol. 5, pp. 22299–22312, 2017.

[144] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen, Y.-G. Zhu, P. V. Morozov, A. V. Divochiy, Z. Zhou, G.-C. Guo, and Z.-F. Han, "Twin-field quantum key distribution over 830-km fibre," *Nature Photon.*, vol. 16, no. 2, pp. 154–161, Feb. 2022.

[145] D. Dequal, G. Vallone, D. Bacco, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental single-photon exchange along a space link of 7000 km," *Phys. Rev. A*, vol. 93, no. 1, Jan. 2016, Art. no. 010301.

[146] R. Kaltenbaek et al., "Quantum technologies in space," *Exp. Astron.*, vol. 51, no. 3, pp. 1677–1694, 2021.

[147] F. Vedovato, C. Agnesi, M. Schiavon, D. Dequal, L. Calderaro, M. Tomasin, D. G. Marangon, A. Stanco, V. Luceri, and G. Bianco, "Extending wheeler's delayed-choice experiment to space," *Sci. Adv.*, vol. 3, no. 10, 2017, Art. no. 1701180.

[148] S.-K. Liao et al., "Long-distance free-space quantum key distribution in daylight towards inter-satellite communication," *Nature Photon.*, vol. 11, no. 8, pp. 509–513, Aug. 2017.

[149] L. Calderaro, C. Agnesi, D. Dequal, F. Vedovato, M. Schiavon, A. Santamato, V. Luceri, G. Bianco, G. Vallone, and P. Villoresi, "Towards quantum communication from global navigation satellite system," *Quantum Sci. Technol.*, vol. 4, no. 1, Dec. 2018, Art. no. 015012.

[150] M. Avesani, L. Calderaro, M. Schiavon, A. Stanco, C. Agnesi, A. Santamato, M. Zahidy, A. Scriminich, G. Foletto, G. Contestabile, M. Chiesa, D. Rotta, M. Artiglia, A. Montanaro, M. Romagnoli, V. Sorianello, F. Vedovato, G. Vallone, and P. Villoresi, "Full daylight quantum-key-distribution at 1550 nm enabled by integrated silicon photonics," *npj Quantum Inf.*, vol. 7, no. 1, p. 93, Jun. 2021.

[151] M. Avesani, C. Agnesi, A. Stanco, G. Vallone, and P. Villoresi, "Stable, low-error, and calibration-free polarization encoder for free-space quantum communication," *Opt. Lett.*, vol. 45, no. 17, p. 4706, 2020.

[152] A. Vetto, "Space systems for optical communications," Univ. Padova, Veneto, Italy, Tech. Rep., 2023.

[153] D. Ribezzo et al., "Deploying an inter-European quantum network," *Adv. Quantum Technol.*, vol. 6, no. 2, Feb. 2023, Art. no. 2200061.

[154] M. C. Sarihan, X. Cheng, K.-C. Chang, and C. W. Wong, "Wavelength-multiplexed multi-user quantum network based on high-dimensional time-bin encoding," in *Proc. CLEO*, 2023, pp. 1–23.

[155] X. Cheng, M. C. Sarihan, K.-C. Chang, C. Chen, F. N. C. Wong, and C. W. Wong, "Secure high dimensional quantum key distribution based on wavelength-multiplexed time-bin encoding," in *Proc. Conf. Lasers Electro-Opt. (CLEO)*, May 2021, pp. 1–2.

[156] K. Sulimany, R. Dudkiewicz, S. Korenblit, H. S. Eisenberg, Y. Bromberg, and M. Ben-Or, "Scrambled time-bin encoding for efficient high-dimensional quantum key distribution," in *Proc. Conf. Lasers Electro-Opt. (CLEO)*, May 2022, pp. 1–2.

[157] N. T. Islam, C. C. W. Lim, C. Cahall, B. Qi, J. Kim, and D. J. Gauthier, "Scalable high-rate, high-dimensional time-bin encoding quantum key distribution," *Quantum Sci. Technol.*, vol. 4, no. 3, Jul. 2019, Art. no. 035008.

[158] I. Vagniluca, B. D. Lio, D. Rusca, D. Cozzolino, Y. Ding, H. Zbinden, A. Zavatta, L. K. Oxenløwe, and D.Bacco, "Efficient time-bin encoding for practical high-dimensional quantum key distribution," *Phys. Rev. Appl.*, vol. 14, no. 1, Jul. 2020, Art. no. 014051.

[159] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, "Provably secure and practical quantum key distribution over 307 km of optical fibre," *Nature Photon.*, vol. 9, no. 3, pp. 163–168, Mar. 2015.

[160] A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, M. Caloz, M. Perrenoud, G. Gras, F. Bussières, M.-J. Li, D. Nolan, A. Martin, and H. Zbinden, "Secure quantum key distribution over 421 km of optical fiber," *Phys. Rev. Lett.*, vol. 121, no. 19, Nov. 2018, Art. no. 190502.

[161] M. Takeoka, M. Fujiwara, and M. Sasaki, "R&d trends and future prospects of quantum cryptography," *New Breeze Winter*, 2019.

[162] M. Travagnin and A. Lewis, "Quantum key distribution in-field implementations," Publications Office Eur. Union, Luxembourg, U.K., Tech. Rep. EUR 29865 EN, 2019.

[163] C.-Y. Lu, C.-Z. Peng, and J.-W. Pan, "Quantum communication at 7,600 km and beyond," *Commun. ACM*, vol. 61, no. 11, pp. 42–43, 2018.

[164] J.-G. Ren et al., "Ground-to-satellite quantum teleportation," *Nature*, vol. 549, pp. 70–73, Sep. 2017.

[165] J. Yin et al., "Satellite-based entanglement distribution over 1200 kilometers," *Science*, vol. 356, no. 6343, pp. 1140–1144, Jun. 2017.

[166] H. Hübel, F. Kutschera, C. Pacher, M. Achleitner, W. Strasser, F. Vedovato, E. Rossi, F. Picciariello, G. Vallone, P. Villoresi, L. Calderaro, V. Martín, J. P. Brito, L. Ortíz, D. Lopez, A. Pastor-Perales, M. Geitz, R.-P. Braun, and P. Rydlichowski, "Deployed QKD networks in Europe," in *Proc. Opt. Fiber Commun. Conf. Exhib. (OFC)*, Mar. 2023, pp. 1–3.

[167] A. Ahmad, A. B. Altamimi, and J. Aqib, "A reference architecture for quantum computing as a service," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 36, no. 6, Jul. 2024, Art. no. 102094.

[168] I. Giroti and M. Malhotra, "Quantum cryptography: A pathway to secure communication," in *Proc. 6th Int. Conf. Comput. Syst. Inf. Technol. Sustain. Solutions (CSITSS)*, Dec. 2022, pp. 1–6.

[169] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, and J. Dynes, "The secoqc quantum key distribution network in Vienna," *New J. Phys.*, vol. 11, no. 7, 2009, Art. no. 075001.

[170] M. Sasaki et al., "Field test of quantum key distribution in the Tokyo QKD network," *Opt. Exp.*, vol. 19, no. 11, pp. 10387–10409, 2011.

[171] D. Stucki et al., "Long-term performance of the SwissQuantum quantum key distribution network in a field environment," *New J. Phys.*, vol. 13, no. 12, Dec. 2011, Art. no. 123001.

[172] S. Wang et al., "Field and long-term demonstration of a wide area quantum key distribution network," *Opt. Exp.*, vol. 22, no. 18, pp. 21739–21756, 2014.

[173] QuTech. (Aug. 5, 2022). *Qutech, Eurofiber and Juniper Networks Partner to Deploy a Quantum Testbed in The Netherlands*. Accessed: Aug. 27, 2024. [Online]. Available: https://qutech.nl/2022/07/05/qutech-eurofiber-juniper-deploy-quantum-testbed/

[174] Ministry of Defence. (Dec. 9, 2020). *Quantum Communication Between Two Drdo Laboratories*. Accessed: Aug. 17, 2023. [Online]. Available: https://pib.gov.in/PressReleasePage.aspx?PRID=1679349

[175] KEEQuant. (2023). *European Quantum Security*. Accessed: Aug. 17, 2023. [Online]. Available: https://www.keequant.com/

[176] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K.Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal, "Experimental quantum key distribution certified by Bell's theorem," *Nature*, vol. 607, no. 7920, pp. 682–686, Jul. 2022.

[177] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, "Current status of the DARPA quantum network," *Proc. SPIE*, vol. 581, pp. 138–149, May 2005.

[178] B. Zhou, B. Lee, A. Karim, G. Mendonca, H. Sun, H. Kim, O. Huang, A. Wu, S. Saenz, A. Baddela, A. Khandelwal, V. Mukund, V. Zhu, and E. Khan, "Policy proposals for the united kingdom's national quantum strategy," *SSRN*, 2023.

[179] L. Global Quantum Intelligence. (Mar. 19, 2024). *Quantumcomputingreport*. Accessed: Aug. 27, 2024. [Online]. Available: https://quantumcomputingreport.com/where-are-the-worldwide-quantum-networking-testbeds/

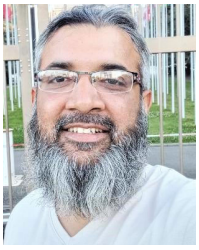
[180] L. Global Quantum Intelligence. (2023). *Quantum Safe '23*. Accessed: Aug. 27, 2024. [Online]. Available: https://www.global-qi.com/product-page/outlook-report-quantum-safe-23

[181] Informatech. (Feb. 21, 2023). *13 Companies Offering Quantum-as-a-service*. Accessed: Aug. 27, 2024. [Online]. Available: https://www.iotworldtoday.com/industry/13-companies-offering-quantum-as-a-service/

[182] I. T. Union. (Oct. 2019). *Overview on Networks Supporting Quantum Key Distribution.* Accessed: Aug. 12, 2023. [Online]. Available: http://handle.itu.int/11.1002/1000/11830-en

[183] A. Sebastián-Lombraña, U. M. Córdova, J. Pedro Brito, V. Martín, and L. Ortiz, "A model-driven satellite quantum communication simulator," in *Proc. 23rd Int. Conf. Transparent Opt. Netw. (ICTON)*, Jul. 2023, pp. 1–4.
[184] E. S. Agency. *Eagle-1*. Accessed: Aug. 17, 2024. [Online]. Available: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Eagle-1
[185] M. I. García Cid, L. Ortiz Martín, and V. Martín Ayuso, "Madrid quantum network: A first step to quantum Internet," in *Proc. 16th Int. Conf. Availability, Rel. Secur.*, Aug. 2021, pp. 1–7.
[186] AI LinkedIn community. *What Are the Main Challenges of Implementing Qkd Network in a Large Scale?*. Accessed: Aug. 17, 2023. [Online]. Available: https://www.linkedin.com/advice/1/what-main-challenges-implementing-qkd-network#:~: text=One%20of%20the%20major%20challenges,ratio%20and%20the%20key%20rate
[187] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, and W.-Y. Liu, "Satellite-relayed intercontinental quantum network," *Phys. Rev. Lett.*, vol. 120, no. 3, 2018, Art. no. 030501.
[188] P. Ball, "Intercontinental, quantum-encrypted messaging and video," *Physics*, vol. 11, p. 7, Jan. 2018.
[189] (Mar. 2020). *Verizon Achieves Milestone in Future-Proofing Data From Hackers*. Accessed: Aug. 12, 2023. [Online]. Available: https://www.verizon.com/about/news/verizon-achieves-milestone-future-proofingdata-hackers
[190] B. G. Newsroom. (Oct. 2020). *Bt and Toshiba Install Uk's First Quantum-secure Industrial Network Between Key Uk Smart Production Facilities*. Accessed: Aug. 12, 2023. [Online]. Available: https://newsroom.bt.com/bt-and-toshiba-install-uks-first-quantum-secure-industrial-network-between-key-uk-smart-production-facilities
[191] L. GB. (Apr. 2022). *Bt and Toshiba Launch First Commercial Trial of Quantum Secured Communication Services - Ey Becomes First Commercial Customer.* Accessed: Aug. 12, 2023. [Online]. Available: https://www.ey.com/en_uk/news/2022/04/bt-and-toshiba-launch-first-commercial-trial-of-quantum-secured-communication-services
[192] C.-W. Tsai, C.-W. Yang, J. Lin, Y.-C. Chang, and R.-S. Chang, "Quantum key distribution networks: Challenges and future research issues in security," *Appl. Sci.*, vol. 11, no. 9, p. 3767, Apr. 2021.
[193] G. M. Mangipudi, S. Eswaran, and P. B. Honnavalli, "Quantum cryptography and quantum key distribution protocols: A survey on the concepts, protocols, current trends and open challenges," *Protocols, Current Trends Open Challenges*, p. 16, Apr. 2022.
[194] SDT Inc. (May 31, 2022). *Quantum Cryptography 101: 9 Applications*. Accessed: Aug. 12, 2023. [Online]. Available: https://sdtinc.medium.com/quantum-cryptography-101-9-current-applications-3d66da4479ce
[195] Fortune Business Insights. (Aug. 2023). *Fortune Business Insights Quantum Cryptography Market Research Report.* Accessed: Aug. 12, 2023. [Online]. Available: https://www.fortunebusinessinsights.com/industry-reports/quantum-cryptography-market-100211
[196] C. Wohlin, P. Runeson, M. Höst, M. C. Ohlsson, B. Regnell, and A. Wesslén, *Experimentation in Software Engineering*, vol. 236. Cham, Switzerland: Springer, 2012.
[197] X. Zhou, Y. Jin, H. Zhang, S. Li, and X. Huang, "A map of threats to validity of systematic literature reviews in software engineering," in *Proc. 23rd Asia–Pacific Softw. Eng. Conf. (APSEC)*, Dec. 2016, pp. 153–160.
[198] S. Jalali and C. Wohlin, "Systematic literature studies: Database searches vs. Backward snowballing," in *Proc. ACM-IEEE Int. Symp. Empirical Softw. Eng. Meas.*, Sep. 2012, pp. 29–38.
[199] V. Braun and V. Clarke, "Using thematic analysis in psychology," *Qualitative Res. Psychol.*, vol. 3, no. 2, pp. 77–101, Jan. 2006.

DURR-E-SHAHWAR received the M.S. degree in information security from the Foundation University School of Science and Technology, Pakistan, in 2023. She is currently a Lecturer with the Department of Software Engineering, Foundation University School of Science and Technology. Her current research interests include cryptography and information security.



MUHAMMAD IMRAN received the M.I.T. degree in information technology from the University of the Punjab, Pakistan, in 2007, the M.S.I.T. degree in information technology from the National University of Science and Technology, Pakistan, in 2011, and the Ph.D. degree in electronic engineering from Dublin City University, Ireland, in 2017. Since July 2008, he has been a Senior Scientist with the National Centre for Physics, Pakistan. His research interests include cloud computing, big data, software engineering, SDN, and optical networks.

AHMED B. ALTAMIMI received the Ph.D. degree in electrical and computer engineering from the University of Victoria, Victoria, BC, Canada, in 2014. He is currently a Professor with the University of Ha'il, Ha'il, Saudi Arabia. His research interests include routing and mobility modeling in wireless networks, and security and privacy threats in Internet of things (IoT) environment.

WILAYAT KHAN received the M.S. degree in IT from Kungliga Tekniska Hogskolan (KTH), Sweden, in 2009, and the Ph.D. degree from the University of Venice, Italy, in 2015. He worked as an Exchange Researcher at KU Leuven, Belgium, and a Research Fellow at Nanyang Technological University, Singapore. He is currently an Assistant Professor with the Department of Computer Engineering, University of Ha'il, Saudi Arabia. Until March 2024, he worked as an Associate Professor with COMSATS University Islamabad, Wah Campus, Pakistan. He is the author of the hardware description language VeriFormal, Chrome extensions CookiExt and SpoofCatch, and a formal tool CoCEC. He has published a number of research papers in reputed journals and conference proceedings. His research interests include theorem proving, information security, and programming languages design.

SHARIQ HUSSAIN received the master's degree in computer science from PMAS-Arid Agriculture University, Rawalpindi, Pakistan, in 2007, and the Ph.D. degree in applied computer technology from the University of Science and Technology Beijing, China, in 2014. Since 2014, he has been with the Department of Software Engineering, Foundation University Rawalpindi Campus, where he is currently an Associate Professor. His main research interests include web services, QoS in web services, web service testing, the IoT, and e-learning. He served as the Publicity Chair for the IEEE International Conference on Internet of People, in 2015. He is an Editorial Board Member of *Journal of Next Generation Information Technology*, AICIT, South Korea.

MOHAMMAD ALSAFFAR is currently an Associate Professor with the Department of Information and Computer Science, University of Ha'il, Ha'il, Saudi Arabia. His research interests include user experience, human–computer interaction, the IoT, data science, and cyber security.