IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526

International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering

Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026

DOI: 10.17148/IJIREEICE.2026.14517

Hardware-Oriented Quantum Communication Systems for Practical Quantum Key Distribution: Architectures, Challenges, and Implementations

Chirag Thakur[1], Raj Kumar Saini[2], Amita Verma[3], Ravi Kant[4], Simon Nyithpuou Chiman[5], Chirag Bharmaik[6], Senate Judith Makobane[7], Nitesh Kumar Vashisht[8]

Shoolini University, solan (H.P), India[1-8]

Abstract: While classical encryption algorithms like RSA and ECC are based on mathematical complexity and are susceptible to attacks by quantum computers in the future, Quantum Key Distribution offers an information-theoretically secure protocol based on the laws of quantum physics. From its conception to today, Quantum Key Distribution technology has developed from a mere theory to practical implementations of quantum communication systems that implement Quantum Key Distribution through quantum states of photons.

This paper provides an overview of the existing Quantum Key Distribution technology, paying particular attention to the hardware aspects of these systems, including their building blocks, like photon sources, modulators, quantum channels, and single-photon detectors, along with implementation issues, including loss, noise, scalability, and overall complexity. Emphasis is paid to recent developments in integrated photonics and photonic integrated circuits.

In addition to conventional Quantum Key Distribution systems, this paper covers advanced Quantum Key Distribution protocols, such as Continuous-Variable Quantum Key Distribution, Measurement-Device-Independent Quantum Key Distribution and Twin-Field Quantum Key Distribution, as well as the related security threats, including side-channel and detector-related attacks. Moreover, this paper looks at how Quantum Key Distribution is evolving to quantum networks and how it can be integrated with post-quantum cryptography.

Finally, this paper addresses some of the emerging topics, including quantum internet and intelligent optimization of Quantum Key Distribution systems.

Keywords: Quantum Key Distribution, Quantum Cryptography, Measurement-Device-Independent Quantum Key Distribution, Twin-Field Quantum Key Distribution.

1.INTRODUCTION

Fast progress in the field of quantum computers is threatening to undermine conventional approaches to public key cryptography, like RSA and Elliptic Curve Cryptography, which rely on certain problems being difficult to solve. With the invention of Shor's algorithm, it has become clear that such algorithms may be cracked with the aid of quantum computers, thus raising serious questions about the safety of existing global encryption systems **[1]**. Thus, there is an acute demand for cryptography schemes providing information-theoretical security.

Among the most efficient ways of ensuring the security of communication lies quantum key distribution (QKD). Unlike other cryptography approaches, (QKD) utilizes the principles of quantum physics like no cloning theorem, entanglement, and superposition, to assure the security of QKD **[1][4][19][21]**. Using the revolutionary principle of encoding information into the quantum state of photons, the BB84 protocol enables the two parties to create their shared secret keys by which they can detect any attempt at eavesdropping **[2]**. Quantum cryptography has evolved from being just theoretical to employing the use of entangled state such as CV-QKD and E91protocol **[3].**

While initially, many resources were allocated to the development of such protocol, the current focus is on ensuring their practical feasibility. The list of hardware elements includes single photon sources, state encoders using modulators, quantum channels, single photon detectors, synchronization devices, and electronics used for classical postprocessing operations **[6][7]**. Nevertheless, errors present in actual physical devices introduce vulnerabilities that can be targeted by various forms of quantum or side channel attacks, necessitating improved hardware design and security analysis **[8][12]**. Among the key enabling technologies that can solve these problems is the use of integrated quantum photonics technology. Using photonic integrated circuits, compact and robust quantum key distribution transmitters and receivers

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026
DOI: 10.17148/IJIREEICE.2026.14517

can be manufactured on a massive scale, reducing their size and costs immensely **[3][16]**. Scalable quantum-secured communication networks are enabled by using quantum communication systems on chips, along with greater phase stability, higher complexity of circuits, and greater compatibility with present telecom systems.

In addition to point-to-point connections, secure relay nodes, key management strategies, compatibility with existing communication systems, and incorporation within future wireless technologies such as 6G, some of the emerging technological challenges introduced by the development of QKD to a networked framework include **[9][15]**. Despite numerous reviews having been conducted on the protocols, proofs of security, and network architectures associated with QKD, comparatively fewer investigations focus on an in-depth hardware perspective, which incorporates photonic integration, system architectures, potential weaknesses in devices, and practical implementation issues.

Quantum communications systems from hardware perspective that can enable real-word QKD applications will be discussed in detail in this review paper. The architecture of the system, photonic devices that can support such an architecture, the difficulties involved in implementing such systems, and the experimental demonstrations made so far will be systematically considered. In this context, the intention is to consolidate the knowledge regarding QKD hardware system, their limitations, and the way forward toward building a practical quantum communication network **[17][18]**.

Whereas many papers have explored protocols and security proofs in QKD, there has been relatively little study done on an integrated hardware-based approach to linking the design of the physical devices themselves with the overall performance and security of the QKD system. Much of the literature considers these aspects separately from each other, which creates a narrow approach to the problem. The purpose of this review is to address this gap by examining QKD systems from a hardware-based perspective.

2. METHODOLOGY

A systematic approach will be adopted in assessing the evolution of Quantum Key Distribution (QKD) hardware implementations. With this view in mind, therefore, the main objective here is to evaluate the trends in technologies, implementation issues, and potential gaps in QKD hardware implementations.

For this reason, relevant literature has been collected from reliable scientific journals, including IEEE Xplore, ScienceDirect, SpringerLink, and arXiv. The keyword search process for retrieving articles included such keywords as "Quantum Key Distribution," "QKD Hardware," "Integrated Photonics," and "Quantum Communication Systems."

Some of the literature that is subject to analysis include scholarly papers dealing with QKD protocols, QKD hardware implementation, security vulnerabilities in QKD technology, and QKD network. Additionally, attention has been paid to more recent articles on this subject.

After collecting papers and categorizing them into various themes like protocols, QKD hardware, integrated photonics, security challenges, and QKD networks, this paper analyzes each of these themes separately.

3. FUNDAMENTALS OF QUANTUM KEY DISTRIBUTION

Quantum Key Distribution is founded on basic physical laws of quantum mechanics, and it is free from any assumption relating to computation. Quantum Key Distribution's security is based on physical properties like the no-cloning theorem, which does not allow for copying of unknown quantum states, as well as the observer effect, which is an indication of eavesdropping **[1][4][19][21]**.

BB84, proposed by Bennett and Brassard, is the most extensively researched QKD protocol, as shown in **Fig.1**. It uses non-orthogonal quantum states for information coding, enabling authorized users to identify any possible attack by the rise in error **[1][19][21]**. The entanglement-based E91 QKD protocol enhances security by making use of the non-locality property of quantum-entangled states **[4][20][21]**.

Several modern QKD protocols have emerged in recently. CV-QKD exploits light quadratures and allows interoperability with conventional optical communication channels **[9][10]**. These developments illustrate how QKD has evolved from theoretical models into functional and secure communication protocols. The efficiency of QKD communication protocols is usually assessed based on the Quantum Bit Error Rate (QBER), defined as the ratio of the number of erroneous bits to the total number of bits transmitted:

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026
DOI: 10.17148/IJIREEICE.2026.14517

QBER = (Number of erroneous bits) / (Total transmitted bits)

The greater the QBER, the more noise there will be, the poorer the quality of the system, and even the possibility of eavesdropping may arise. Key generation is feasible only if the QBER is kept below a specific value.

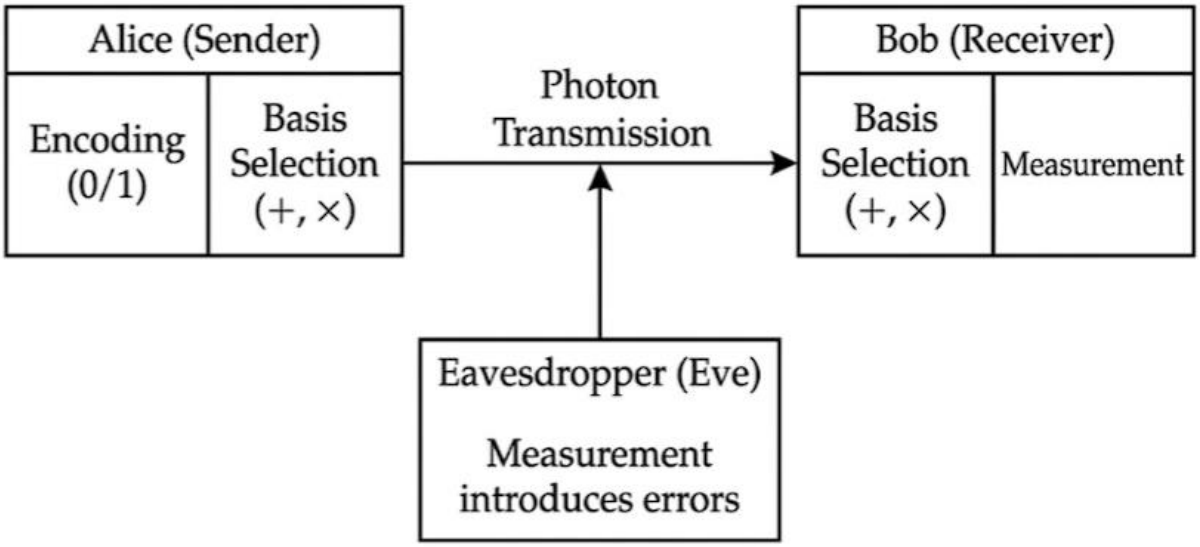

Fig. 1.- BB84 protocol showing encoding, transmission, and eavesdropping detection.

Table I: Comparison of Major QKD Protocols

Protocol	Type	Key Feature	Advantage	Limitation	References
BB84	Discrete Variable	Polarization encoding	Simple, widely used	Device vulnerabilities	[1][7]
E91	Entanglement-based	Bell inequality	Strong security	Complex implementation	[2][4]
CV-QKD	Continuous Variable	Amplitude & phase	Telecom compatible	Noise sensitive	[3][9]
MDI-QKD	Measurement-independent	Removes detector trust	High security	Complex system	[10][11]
DI-QKD	Device-independent	No device trust	Maximum security	Very hard to implement	[10][11]

4. HARDWARE ARCHITECTURE OF QKD SYSTEMS

Theoretically, when talking about QKD, it seems to have everything going for it. Photons are made, sent, and received, and then presto the key is made. But in actuality, the QKD process is very complicated, with classical parts working together in perfect harmony. Even slight errors in parts working together in perfect harmony. Even slight errors in the parts can result in problems. In the macro world, QKD involves the following components **[5][7]**, as illustrated in **Fig.2.**

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026
DOI: 10.17148/IJIREEICE.2026.14517

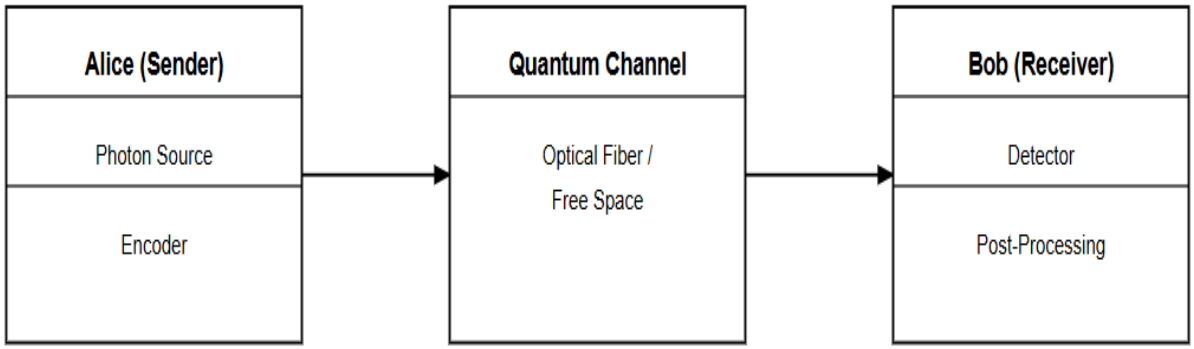

Fig. 2 - Basic QKD system showing Alice, quantum channel, and Bob.

4.1 Photon Sources

All starts with the emission of photons carrying quantum information. In an ideal situation, QKD involves single photon generators that emit photons one at a time. This is because emitting more than one photon per pulse poses risks for systems susceptible to photon number splitting attacks.

But perfect sources for single photons are still a challenge for practical implementation. Therefore, in actual quantum key distribution applications, sources of weak coherent states (WCS), obtained using attenuated lasers, are used instead. Weak coherent states represent an approximate realization of single photons since their average photon number is very small.

That said, this is a trade-off. WCPs are simpler to implement, but they are not perfectly secure. More advanced methods, like quantum dot emitters and spontaneous parametric down-conversion (SPDC) sources, can generate more controlled single photons and even entangled photon pairs. These sources have better security guarantees but are often more complex and less mature for large-scale deployment **[2][22][23][24]**.

4.2 Modulators and Encoding

Having been emitted, these photons have to be first encoded with some information, which is done using electro-optical modulators, manipulating the quantum state of photons depending on the particular QKD protocol being used. Encoding can involve the use of any of the physical characteristics of light, such as polarization, phase, or amplitude of a light wave, depending on the particular type of QKD employed. Thus, in polarization QKD systems, polarization of light is manipulated in order to encode some information into a photon stream, while phase QKD utilizes a phase difference between two optical paths to encode data.

This phase demands very high accuracy and stability since even tiny changes arising from temperature fluctuations, mechanical vibration, and electronics noises can create errors. The errors may be mistaken for a tapping attack, but even worse, the errors may mask any real attack on security. Another problem arising from the increased need for more frequent key generation is the creation of modulators that perform at high speeds with negligible distortion. **[2][10][26][27][28]**.

4.3 Quantum Channels

After the encoding step, the photons are sent along the quantum channel connecting the sender and receiver, Alice and Bob. In a QKD setup, the quantum communication is usually performed using either fiber-optical channels or free space channels. The use of fiber-optic QKD is common since such a system allows for seamless integration into current telecom infrastructure; nevertheless, optical fiber suffers from the effects of attenuation, leading to absorption and scattering of photons in longer transmissions. This reduces the distance over which reliable quantum communication can be achieved, usually within 200 kilometers without quantum repeaters. **[6][28]**.

Free-space quantum key distribution is another technique that permits the transfer of photons over air or space-based connections, rendering it applicable to global communications. While this offers one distinct benefit, it is important to understand that free-space communication is very susceptible to external interference from environmental variables. **[6][29][30]**.

In both cases, quantum channels will always be vulnerable since any loss or noise will impact the speed of generation, the level of errors and in general the performance of the system. Thus, the onset of long-distance, effective, and stable quantum channels is still a challenging task. **[6][28][30]**.

4.4 Detectors

In a quantum key distribution setup, photon detection is done at the receiver side very accurately, hence making single photon detectors one of the essential parts. From all types of photon detectors that can be employed, avalanche photodiodes (APDs) remain one of the most preferred ones because they are quite economical, small, and simple to

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026
DOI: 10.17148/IJIREEICE.2026.14517

implement. However, they have some limitations concerning their efficiency and noise levels. On the other hand, superconducting nanowire single-photon detectors (SNSPDs) are highly superior compared to APDs, but the problem is that SNSPDs need to work in cryogenic temperatures.

Detector performance affects crucial factors, such as quantum bit error rate, key generation rate, and communication range, of QKD systems. Additionally, detectors constitute an important threat point in QKD systems due to the existence of some quantum hacking approaches, including blinding attacks, that take advantage of detectors' characteristics. Therefore, research work on detectors aims at designing detectors with high efficiency and high resistance against security threats. **[7][31][32][33]**.

4.5 Post-processing

QKD systems depend on classical post-processing to convert unprocessed measurement data into a secure cryptographic key following the quantum transmission phase. Alice and Bob use the classical channel to communicate and correct their data. In this step, Alice and Bob communicate to reconcile and distill their data. There are several important steps in this process, including sifting, error correction, and privacy amplification.

In the sifting stage, measurement results that correspond to incompatible encoding and measurement bases are discarded so that only correlated data remains. Then error correction is performed to remove discrepancies between Alice's and Bob's keys by using classical algorithms to make them consistent. Finally, the privacy amplification step is performed, which removes any partial information obtained by an eavesdropper and results in a shorter but very secure final key.

Post-processing, although executed through classical communication, is an essential part of the overall security of QKD systems. If this step is wrong or inefficient, security can be compromised even if the quantum channel is perfect. These post-processing steps are mathematically rigorous and are required to achieve information-theoretic security in practical QKD implementations **[10][34][35][36]**.

Table II: Comparison of QKD Hardware Components

Component	Options	Advantage	Challenge	References
Photon Source	WCP, SPDC, Quantum dots	Practical implementation, scalable	Multi-photon emissions, imperfect single-photon sources	[2][5]
Modulators	Phase, Polarization	Flexible encoding schemes high-speed operation	High sensitivity to noise, Stability issues	[2][10]
Channel	Fiber, Free-space	Existing infrastructure, Long-distance potential	Loss, noise, environmental disturbance	[6][28]
Detectors	APD, SNSPD	High detection efficiency (SNSPD), practical (APD)	Cost, Cryogenic cooling requirements	[7][31][32]
Post-Processing	Error correction, Privacy amplification	Secure key generation	Computational Overhead, Latency	[10][34]

5. INTEGRATED PHOTONICS FOR QKD

The use of integrated photonics technology has evolved from being a topic worth investigating to becoming essential in scaling QKD systems to a stage where their implementation would go beyond lab tests. In conventional optical setups comprising several components such as lenses, beam splitters, and fiber couplings, their performance is often high within confined laboratory settings; however, they prove to be bulky, alignment-sensitive, and challenging to duplicate on a large scale.

Photonic Integrated Circuits (PICs) allow the integration of multiple optical elements such as modulators, interferometers, and waveguides on a compact platform. The PIC-based QKD system is shown in **Fig. 3.**

In contrast to the assembly of components, the entire circuit could be fabricated by semiconductor techniques in one process. The size will be minimized; also, the relative positioning of the components will be stable because of the fact

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026
DOI: 10.17148/IJIREEICE.2026.14517

that they have been assembled at once. This is particularly important for QKD circuits, where the phase stabilization is crucial. **[2][14][37]**.

Taking this concept forward, chip-based QKD has started to show some practical benefits. The processes involved in setting up a QKD system such as preparing quantum states, encoding, and even the detection process could all be done on a chip. Chip-based QKD systems are energy-efficient and less susceptible to external disturbances such as vibrations and variations in temperature. Silicon photonic devices have been popular recently due to their compatibility with current CMOS technology. Such compatibility makes mass production possible, an important step towards the mainstreaming of QKD. **[3][14][37][38]**.

However, integration is not the silver bullet for all problems; some actually come to light as others disappear. Optical losses in the chip can result in a lower quality of the signal, which is especially problematic in the case of single photons. Another problem is that of thermal sensitivity, since temperature differences will impact the stability of phases in an integrated circuit. Last but not least, it is extremely difficult to integrate efficient single-photon detectors into integrated devices.

Even with these limitations, integrated photonics is widely seen as a key step toward practical QKD deployment. It offers a pathway toward compact, scalable, and potentially cost-effective quantum communication systems. The technology is still evolving, and there are trade-offs to navigate, but it is difficult to imagine large-scale quantum-secured networks without some form of photonic integration at their core **[14][27][39]**.

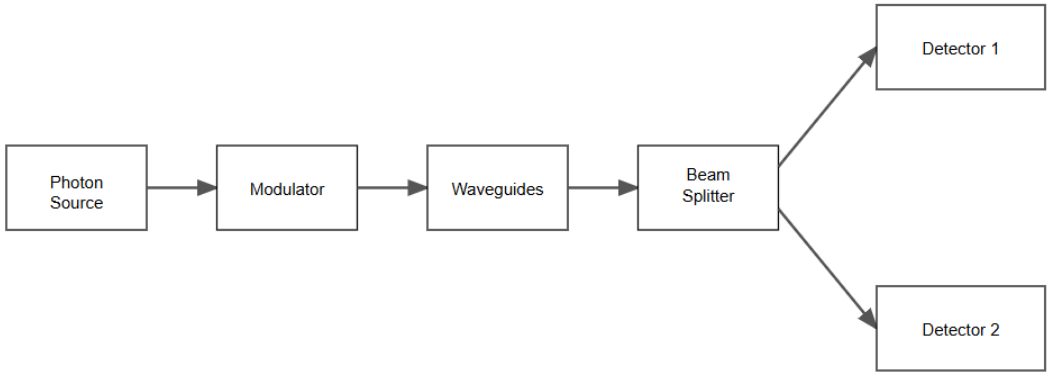

Fig.3- Integrated photonic QKD system.

6. SECURITY CHALLENGES AND QUANTUM HACKING

Quantum Key Distribution has been termed as “unconditional security,” but such notions only hold in an ideal setting when the equipment is perfect and nothing unexpected happens. This cannot happen in the real world, and there can always be hardware failures, misalignment of parts, and unexpected behavior of equipment.
However, within the last 10 years or so, it was proven that you do not need to violate quantum mechanics to hack into such systems. One can target the physical devices. This is known as quantum hacking, which involves identifying and exploiting small irregularities in hardware as opposed to looking for loopholes in the theoretical framework **[7][10][40][41]**.

6.1 Detector Blinding Attacks

Another famous example of such a flaw is the blinding of the detector. In usual setups of QKD system, the detectors operate on single photons. But under some conditions, the attacker might illuminate the detector with intense light, forcing it to operate in the classical regime.

The detector would then cease to function as a real quantum apparatus and, rather, could be easily controlled by the attacker in a predetermined fashion based on the properties of the input signals. Thus, using a carefully crafted combination of signals, an attacker could manipulate the detection results without causing any apparent mistakes in the process.

This is especially alarming because, from the viewpoint of Alice and Bob, things can seem perfectly normal until certain precautions have been taken **[40][41]**.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026
DOI: 10.17148/IJIREEICE.2026.14517

6.2 Photon-Number Splitting (PNS) Attacks

Another crucial weakness is the utilization of low-intensity coherent pulses rather than perfect sources of single photons. Because of the occasional multiplicity of photons in these pulses, a possible attack is the photon number splitting (PNS). In this case, the attacker only extracts one photon from a multiphoton packet while letting the rest proceed towards the receiver. The basic principle is that the attacker can store the intercepted photon and read it once the basic information has been declared in public. In this manner, he would have enough time to extract information from the key without causing any disturbance to the system at all.

The example underscores a crucial yet delicate issue: practical compromise in terms of feasibility, such as employing weak laser pulses, may actually give rise to brand new threats **[24][42].**

6.3 Side-Channel Attacks

Side-channel attacks constitute a wide range of security threats faced by QKD systems because such attacks rely on unintentional data leakage from hardware implementations, rather than on attacking the quantum channel itself. These leaks can come from time-related fluctuations in signal processing, power consumption variations, electromagnetic interference, and nonidealities in the modulation signals. While each factor may seem negligible in isolation, they can be analyzed using sophisticated methods that will allow an attacker to gather information about the secret key.

One of the critical issues concerning side-channel attacks lies in their roots, which are in the inherent deficiencies of real-world implementations and not in any weaknesses within the quantum protocols themselves. As such, even theoretically safe QKD protocols may be rendered unsafe under certain conditions due to the way they have been implements **[27][41][42].**

6.4 Bridging the Gap: Advanced Protocols

Several sophisticated schemes for QKD have been suggested to deal with these security loopholes. This category includes schemes such as Measurement Device Independent Quantum Key Distribution (MDI-QKD). In MDI-QKD, the basic premise of making the measurement device secure is dropped completely, and neither Bob nor any other party makes the actual measurements, but instead, Alice and Bob make their states available to the node. **[7][10][21]**.

The second method is called Device-Independent QKD (DI-QKD). This method seeks to secure communications without making any assumptions about how the underlying devices operate. Rather, DI-QKD secures information using quantum entanglement that is proven by Bell inequalities. Theoretically, DI-QKD can be implemented even when using totally untrusted devices.

In spite of all that, these methods have their shortcomings too. For example, they are more difficult to apply and require more stringent condition for experiments.

7. QKD NETWORK ARCHITECTURES

The initial QKD configuration was quite elementary: a source connected to a detector with a quantum channel. It is ideal for proving the technology, but the approach falls short of requirements if one needs to construct a real-life communication network. Communications are not so straightforward; they are complicated, involving many users scattered across huge territories and incorporating complex routing systems. Scaling QKD for such scenarios requires not only mastering quantum communications but also poses architectural challenges as well.

Numerous approaches have been formulated in an attempt to solve this challenge. Several types of networks have been developed (you can see some examples in **Fig. 4**), all offering their perspectives on the balance between practicality, security, and scalability **[6][8][43][44].**

7.1 Point-to-Point Systems

The simplest form of networking is the point-to-point configuration, where the communication is done between two parties through the quantum communication channel. From the architectural point of view, this is the easiest form of configuration, which means fewer hardware components and easier security testing.

Nevertheless, this easiness is associated with a significant cost. Every user would require its own connection, which would be very hard to achieve, as the number of network participants increases. Imagine the situation where in order to have a reliable communication channel, every pair of devices would be connected by a wire.

7.2 Trusted-Node Networks

In order to address the problem of distance and scalability, the architecture of trusted nodes employs additional nodes used to relay keys from one user to another. This does not mean establishing a direct link; on the contrary, the key travels via a series of nodes, where QKD takes place between adjacent nodes.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026
DOI: 10.17148/IJIREEICE.2026.14517

Indeed, such an approach has already found application in numerous testbed experiments. As a result, the distance over which QKD can take place is extended, but not at the expense of extremely long direct links.
All this being said, it should be admitted that the term "trusted" bears too much meaning in the context of the current architecture. Indeed, every intermediate node needs to be secure, as it gets access to the key at some point during its transmission. Hence, compromising just one node may affect the security of the whole path **[8][43].**

7.3 Satellite-Based QKD

Satellite-based QKD has been tried by means of links between satellites and the ground, thus enabling key distribution up to several thousand kilometers **[17]**. Satellite-based QKD has been tried by means of links between satellites and the ground, thus enabling key distribution up to several thousand kilometers.

Its feasibility has been demonstrated, and its power resides in connecting the whole world with fewer intermediate nodes. However, the disadvantages are equally obvious, including precise positioning, atmospheric disturbance, time-limited communication windows, and high costs involved.
Still, satellite QKD is often regarded as an essential step toward a worldwide quantum communication network.**[17][29][44]**.

7.4 Hybrid Networks (Quantum + Classical + 6G)

From the point of view of implementation, it is highly unlikely that the use of QKD will completely replace traditional communication protocols. Instead, QKD will become a part of existing communication systems and networks. This has resulted in the creation of hybrid networks in which quantum channels are employed to transmit keys while classical channels are used for the transmission of information.

There is growing interest in combining QKD into emerging communication infrastructures, including upcoming 6G technologies. While the implementation of QKD technologies offers numerous advantages, several challenges stand in the way of their successful deployment. They include efficient bandwidth usage, synchronization of quantum and classical channels, and end-to-end security across multiple layers of the communication network **[44][13]**.

7.5 Key Management in QKD Networks

In an expanding QKD network, key management proves to be among the most important of challenges faced by such systems. This not only involves key generation but also encompasses key storage, distribution, and routing throughout the network. Key management is vital in guaranteeing end-to-end security.

Challenges that must be addressed include security of key storage, effective routing among network nodes, key refreshing and management, and the seamless integration of quantum cryptography with traditional cryptography systems. Regardless of how well the quantum communication level functions, poor key management will render the entire system vulnerable to attacks. Consequently, QKD networks have to be designed with an equal amount of focus on quantum communication levels and system-wide key management methods **[8][13][43]**.

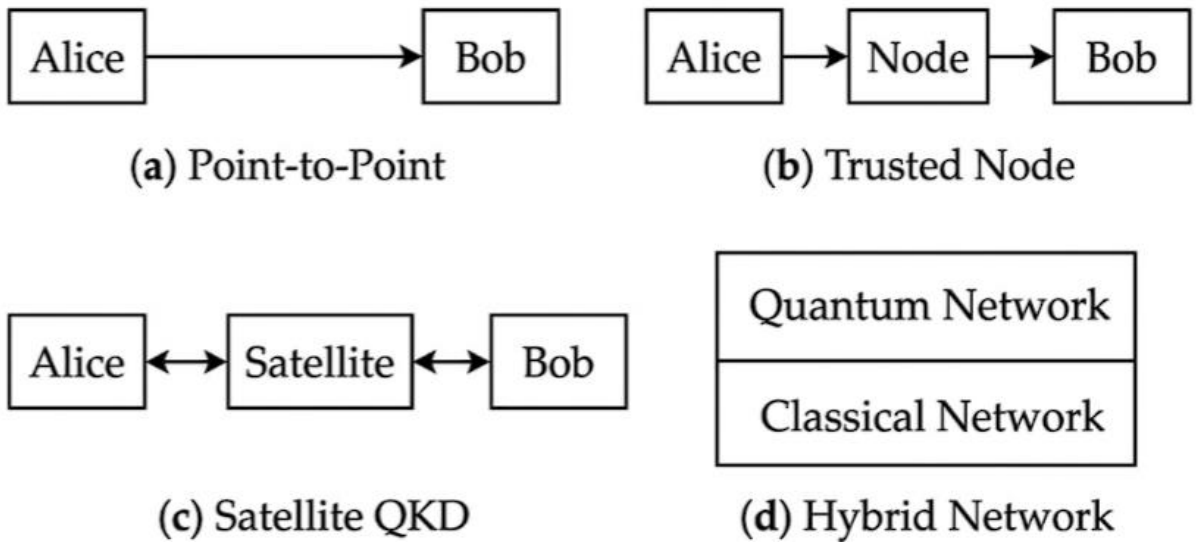

Fig. 4. - QKD network architectures.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026
DOI: 10.17148/IJIREEICE.2026.14517

Table III: Comparison of QKD Network Architectures

Architecture	Description	Advantage	Limitation	Use Case	References
Point-to-Point	Direct link	Simple	Not scalable	Small systems	[6]
Trusted Node	Relay nodes	Long distance	Required trust	City networks	[8]
Satellite QKD	Space-based	Global coverage	Expensive	Global security	[12][14]
Hybrid	Quantum + classical	Flexible	Complex	Future networks	[14]

8. IMPLEMENTATION CHALLENGES

One of the most essential constraints in QKD communication is the distance between two users. Since photons will encounter attenuation because of absorption and scattering while propagating in an optical fiber there will be considerable signal loss. In contrast to classical signals, quantum communication signals cannot be amplified using repeaters because amplification causes disturbance in the quantum state. Thus, quantum key distribution in fiber optics can reach only a few hundreds of kilometers **[6][16][45]**. At distances outside of this range, the rate at which the keys can be generated falls sharply, thereby making secure communications very difficult. It is possible to perform QKD over optical fiber lengths of hundreds of kilometers **[18][28]**. Even though there have been several solutions proposed, such as quantum repeaters and communication via satellites, such methods are currently still in their developmental stages and have not yet been implemented in practice.

8.1 Photon Loss and Noise

Even in cases where the distance between transmitter and receiver is relatively short, QKD faces challenges related to photon losses and noises. This is due to such factors as the imperfection of optical fibers, the misalignment of free space channels, or the low efficiency of photon detection. Moreover, environmental noise sources such as thermal noise and electronic interference adversely affect the process by introducing errors. All of these problems lead to deterioration of important performance parameters, including quantum bit error rate, key generation rate, and overall reliability. The higher the error rate, the more bits must be removed from the post-processed stream; as a result, the effective secret key length decreases significantly. In some cases, excessive errors cause detection of an insecure channel and stop further key generation **[7][28][45]**.

8.2 Cost and Complexity

Another key challenge with the implementation of QKD technology is its cost and complexity. Components used in QKD are more sophisticated compared to their equivalents in traditional communication systems, meaning they have not evolved to the point of efficiency and cost effectiveness witnessed in traditional communication systems. This is because detectors used in QKD, like superconducting nanowire single photon detectors, need cryogenic cooling, and other optical components require precise alignment. This results in higher costs involved in implementing and maintaining the technology. Unlike cryptography methods that are implemented using software alone, the cost of implementing QKD remains relatively high. **[5][31]**.

8.3 Synchronization Issues

Synchronicity is crucial for QKD systems to operate. It is important that both Alice and Bob remain highly synchronized with each other in order to be able to interpret the photon timings and the results obtained from measurements. In fast QKD systems, there will be an increased error probability if there are any errors made in synchronicity. The reason is that this leads to incorrect interpretation of the value of the bits. As the distance between them increases, synchronization becomes increasingly harder. **[10][25]**.

9. FUTURE RESEARCH DIRECTIONS

Quantum Key Distribution (QKD) has evolved from being a theoretical idea to becoming an implemented technology in miniature setups; however, it still exists at the junction of concept and actual application. Although the core ideas have been well understood and proven through experiments, the main issue at hand is how to scale up the process such that it

DOI: 10.17148/IJIREEICE.2026.14517

becomes feasible, economical, and scalable to be used extensively. This is currently what most research in QKD aims to achieve.

9.1 Quantum Repeaters

Distance is one of the key limitations that pose problems in QKD. The maximum distance possible depends on the extent of photon loss experienced during the process of transmission via the optical channel. Quantum repeaters have been proposed as the means for overcoming this limitation. As opposed to classical repeaters, which involve signal amplification, quantum repeaters depend on entanglement generation, storage using quantum memory, and entanglement swapping within intermediate stations. This mechanism would facilitate the extension of quantum information over large distances without the need for direct amplification of the quantum state. Nonetheless, the deployment of quantum repeaters continues to be a difficult task due to the necessity for reliable quantum memory, low noise, and synchronization. Despite several experimental advancements, practical quantum repeater systems do not exist yet **[6][45]**.

9.2 Quantum Internet

The concept of quantum repeaters is also intimately connected with that of a quantum internet, a far-reaching idea of creating an interconnected network of quantum machines able to distribute quantum entanglement among themselves and perform quantum operations. Within this framework, quantum key distribution will find its primary application in the field of secure communication. However, quantum communication will offer much more besides that, from distributed computing to sensing and novel forms of communication altogether, unattainable by means of classical systems. At present, quantum internet is only at the theoretical stage and still lacks practical implementations. **[30][44]**.

9.3 Artificial Intelligence in QKD

The role of artificial intelligence (AI) in improving QKD system capabilities is becoming increasingly clear, especially in difficult operating environments where noise levels are high. The use of machine learning can help optimize the parameters of the system, enable adaptive key management, minimize the impact of noise, and also detect any form of security breach in real time. For example, AI can assist in optimizing the parameters of the channel according to the current state, make the error-correction process more efficient, and even help spot suspicious behavior indicating an attack. Even though this research area is very new, there is great potential here **[11]**.

9.4 Twin-Field Quantum Key Distribution (TF-QKD)

Twin-Field Quantum Key Distribution (TF-QKD) represents a notable breakthrough in dealing with the inherent limits on the rate-distance trade-off of standard QKD schemes. In standard QKD schemes, the main challenge is related to the secret-key capacity in the absence of quantum repeaters; because of the exponentially increasing loss of photons with distance, this poses a limit for the scheme's performance in practice. By exploiting single-photon interference at an intermediate measurement station, TF-QKD solves this problem. **[6][16][46]**.

In TF-QKD, each of the two parties separately transmits phase-randomized weak coherent pulses to an intermediate site, where interferometry is done. The key advantage of TF-QKD is that it offers better scalability of the key rate with respect to distance, as compared to regular point-to-point QKD schemes. Recent experiments have demonstrated that TF-QKD can enable communication at much larger distances than possible with existing methods **[46][18]**.
While there are some issues associated with TF-QKD, such as phase locking for a distance and synchronization issues, it is nonetheless a very significant advancement in the world of QKD systems **[6][16][45][46]**.

9.5 Post-Quantum Cryptography (PQC) vs. QKD

One of the prominent trends in recent secure communication technology is that of comparing Quantum Key Distribution (QKD) with post-quantum cryptography (PQC). PQC is required because of the risk posed by large-scale quantum computers, as they can break down classic cryptographic schemes like RSA and ECC through algorithms like Shor's **[1][47]**.

The goal of PQC is to create cryptographic system that will still be safe in the face of quantum attacks. The problems used to design such system are problems for which there are no efficient quantum solutions at present, such as those related to lattices, hash functions, and codes. An important characteristic of PQC is that it can be easily integrated into existing communications systems since it is purely software based **[6][47]**. However, this brings out an important trade-off since QKD is more secure theoretically, but PQC is more practical and scalable.

On the other hand, QKD uses quantum theory to ensure information-theoretical security, meaning that the security of QKD is not dependent on any assumptions about computation. Nonetheless, QKD requires special hardware such as photon source, detectors, and quantum channels **[6][13]**.

IJIREEICE ISSN (O) 2321-2004, ISSN (P) 2321-5526
International Journal of Innovative Research in Electrical, Electronics, Instrumentation and Control Engineering
Impact Factor 8.414 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 14, Issue 5, May 2026
DOI: 10.17148/IJIREEICE.2026.14517

This leads to the fact that QKD and PQC provide complementing benefits instead of being competing approaches. QKD guarantees provable security in the key distribution process, whereas PQC ensures scalability and economy of implementation with the help of classical devices. This is why hybrid approaches utilizing both QKD and PQC have become a popular choice recently **[13][44][47]**.

9.6 Scalable Chip-Based Systems

A third important line of investigation is that of enhancing scalability via integrated photonics. Chip-based QKD protocols present an opportunity for realizing small-sized, robust, and affordable QKD systems by integrating various optical components on a photonic chip. Efforts are currently being made towards developing greater degrees of integration, reducing optical loss, enhancing compatibility with telecommunications networks, and enabling large-scale production via semiconductor processing methods. If successful, QKD would move beyond its niche application and become a mainstream communication protocol, possibly incorporated into consumer electronics. Nevertheless, many hurdles need to be overcome, especially the issue of incorporating highly sensitive single-photon detectors along with ensuring system stability **[14][15][37]**.

10. CONCLUSION

Quantum Key Distribution is certainly a significant evolution in our approach to security. While other forms of cryptography rely on unproven mathematical premises, quantum cryptography relies on physical laws. The concept itself is intriguing, but as we have discussed throughout this review, the actual implementation of QKD is not an easy task.
Throughout this essay, it was seen that QKD system were not just constrained to the protocol but had the physical component contributed to its vulnerability. The source, modulator, detector, and post-processing unit all have their weaknesses and compromise to make. It may be theoretically sound, but the practicality lies in the imperfection within the equipment used.

The importance of integrated photonics comes into focus in this context. The transition from heavy optical systems to semiconductor-based solutions provides a tangible solution towards scalability and stability. However, it poses its own unique challenges, such as loss due to photons and thermal effects. In much the same way, the concept of quantum hacking brings into sharp relief one essential aspect of quantum cryptography. The strength of QKD relies upon the integrity of all physical components.

When it comes to expanding QKD technology from point-to-point system to networked environment, even more complications arise. There are trusted-node system, satellite connectivity, and a blend of quantum/classical networks that can be used as solutions; however, these methods have different implications, especially in terms of security, pricing, and scalability.

The future of QKD, however, appears to depend greatly on the ability of several technologies to come together. Quantum repeaters, photonic integration, artificial intelligence, and networking play their roles. One technology alone will not be enough, but consistent developments in these fields will slowly lead to practical quantum communication.

All in all, quantum cryptography is no longer just a topic for theoretical discussions. Although there are many difficulties in making it widely available, things are beginning to become much clearer. In other words, it seems only natural to assume that quantum key distribution will have an important place in the future of secure communication.

After all, the successful commercialization of QKD technology will be contingent not only upon advances in quantum physics but also on improvements in hardware technology and network design.

Acknowledgements
A generative Artificial Intelligence (AI) tools is used for grammar improvement only.

Disclosure statement
No potential conflict of interest was reported by the author(s).

Data availability statement
Data will be made available on request.

DOI: 10.17148/IJIREEICE.2026.14517

REFERENCES

[1] Shor, P. W. (1994, November). Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science* (pp. 124-134).

[2] Bennett, C. H., & Brassard, G. (2014). Quantum cryptography: Public key distribution and coin tossing. *Theoretical computer science*, *560*, 7-11.

[3] Ekert, A. K. (1991). Quantum cryptography based on Bell's theorem. *Physical review letters*, *67*(6), 661.

[4] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of modern physics*, *74*(1), 145.

[5] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of modern physics*, *81*(3), 1301-1350.

[6] 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. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. 12, 1012-1236 (2020)

[7] Lo, H. K., Curty, M., & Qi, B. (2012). Measurement-device-independent quantum key distribution. *Physical review letters*, *108*(13), 130503.

[8] Braunstein, S. L., & Van Loock, P. (2005). Quantum information with continuous variables. *Reviews of modern physics*, *77*(2), 513-577.

[9] Sun, S., & Huang, A. (2022). A review of security evaluation of practical quantum key distribution system. *Entropy*, *24*(2), 260.systems,"

[10] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, "Continuous-variable quantum key distribution: Past, present, and future," Appl. Phys. Rev., vol. 11, no. 1, 2024.

[11] Rusca, D., & Gisin, N. (2024). Quantum cryptography: an overview of quantum key distribution. *arXiv preprint arXiv:2411.04044*.

[12] Pljonkin, A., & Singh, P. K. (2018, December). The review of the commercial quantum key distribution system. In *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)* (pp. 795-799). IEEE.

[13] Dervisevic, E., Tankovic, A., Fazel, E., Kompella, R., Fazio, P., Voznak, M., & Mehic, M. (2025). Quantum key distribution networks-key management: A survey. *ACM Computing Surveys*, *57*(10), 1-36.

[14] Luo, W., Cao, L., Shi, Y., Wan, L., Zhang, H., Li, S., ... & Liu, A. Q. (2023). Recent progress in quantum photonic chips for quantum communication and internet. *Light: Science & Applications*, *12*(1), 175.

[15] Liu, Q., Huang, Y., Du, Y., Zhao, Z., Geng, M., Zhang, Z., & Wei, K. (2022). Advances in chip-based quantum key distribution. *Entropy*, *24*(10), 1334.

[16] Pirandola, S., Laurenza, R., Ottaviani, C., & Banchi, L. (2017). Fundamental limits of repeaterless quantum communications. *Nature communications*, *8*(1), 15043.

[17] Wang, J. Y., Yang, B., Liao, S. K., Zhang, L., Shen, Q., Hu, X. F., ... & Pan, J. W. (2013). Direct and full-scale experimental verifications towards ground–satellite quantum key distribution. *Nature Photonics*, *7*(5), 387-393.

[18] Korzh, B., Lim, C. C. W., Houlmann, R., Gisin, N., Li, M. J., Nolan, D., ... & Zbinden, H. (2015). Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, *9*(3), 163-168.

[19] Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge university press.

[20] Bouwmeester, D., & Zeilinger, A. (2000). The physics of quantum information: basic concepts. In *The physics of quantum information: quantum cryptography, quantum teleportation, quantum computation* (pp. 1-14). Berlin, Heidelberg: Springer Berlin Heidelberg.

[21] Lo, H. K., & Chau, H. F. (1999). Security of quantum key distribution. *Science*, *283*(arXiv: quant-ph/9803006), 2050-2056.

[22] Michler, P. (Ed.). (2003). *Single quantum dots: Fundamentals, applications and new concepts* (Vol. 90). Springer Science & Business Media.

[23] Santori, C., Fattal, D., Vučković, J., Solomon, G. S., & Yamamoto, Y. (2002). Indistinguishable photons from a single-photon device. *nature*, *419*(6907), 594-597.

[24] Ma, X., Qi, B., Zhao, Y., & Lo, H. K. (2005). Practical decoy state for quantum key distribution. *Physical Review A—Atomic, Molecular, and Optical Physics*, *72*(1), 012326.

[25] Kumar, R., Barrios, E., MacRae, A., Cairns, E., Huntington, E. H., & Lvovsky, A. I. (2012). Versatile wideband balanced detector for quantum optical homodyne tomography. *Optics Communications*, *285*(24), 5259-5267.

[26] Lucamarini, M., Patel, K. A., Dynes, J. F., Fröhlich, B., Sharpe, A. W., Dixon, A. R., ... & Shields, A. J. (2013). Efficient decoy-state quantum key distribution with quantified security. *Optics express*, *21*(21), 24550-24565.

[27] Jain, N., Anisimova, E., Khan, I., Makarov, V., Marquardt, C., & Leuchs, G. (2014). Trojan-horse attacks threaten the security of practical quantum cryptography. *New Journal of Physics*, *16*(12), 123030.

DOI: 10.17148/IJIREEICE.2026.14517

[28] Gisin, N., & Thew, R. (2007). Quantum communication. *Nature photonics*, *1*(3), 165-171.
[29] Ursin, R., Tiefenbacher, F., Schmitt-Manderbach, T., Weier, H., Scheidl, T., Lindenthal, M., ... & Zeilinger, A. (2007). Entanglement-based quantum communication over 144 km. *Nature physics*, *3*(7), 481-486.
[30] Kimble, H. J. (2008). The quantum internet. *Nature*, *453*(7198), 1023-1030.
[31] Marsili, F., Verma, V. B., Stern, J. A., Harrington, S., Lita, A. E., Gerrits, T., ... & Nam, S. W. (2013). Detecting single infrared photons with 93% system efficiency. *Nature Photonics*, *7*(3), 210-214.
[32] Lita, A. E., Miller, A. J., & Nam, S. W. (2008). Counting near-infrared single-photons with 95% efficiency. *Optics express*, *16*(5), 3032-3040.
[33] Rosenberg, D., Harrington, J. W., Rice, P. R., Hiskett, P. A., Peterson, C. G., Hughes, R. J., ... & Nordholt, J. E. (2007). Long-distance decoy-state quantum key distribution in optical fiber. *Physical review letters*, *98*(1), 010503.
[34] Brassard, G., & Salvail, L. (1993, May). Secret-key reconciliation by public discussion. In *Workshop on the Theory and Application of of Cryptographic Techniques* (pp. 410-423). Berlin, Heidelberg: Springer Berlin Heidelberg.
[35] Bennett, C. H., Brassard, G., Crépeau, C., & Maurer, U. M. (1995). Generalized privacy amplification. *IEEE Transactions on Information theory*, *41*(6), 1915-1923.
[36] Tomamichel, M., Lim, C. C. W., Gisin, N., & Renner, R. (2012). Tight finite-key analysis for quantum cryptography. *Nature communications*, *3*(1), 634.
[37] Wang, J., Sciarrino, F., Laing, A., & Thompson, M. G. (2020). Integrated photonic quantum technologies. *Nature photonics*, *14*(5), 273-284.
[38] Bonneau, D., Engin, E., Ohira, K., Suzuki, N., Yoshida, H., Iizuka, N., ... & Thompson, M. G. (2012). Quantum interference and manipulation of entanglement in silicon wire waveguide quantum circuits. *New Journal of Physics*, *14*(4), 045003.
[39] Xiong, C., Zhang, X., Liu, Z., Collins, M. J., Mahendra, A., Helt, L. G., ... & Eggleton, B. J. (2016). Active temporal multiplexing of indistinguishable heralded single photons. *Nature communications*, *7*(1), 10853.
[40] Makarov, V. (2009). Controlling passively quenched single photon detectors by bright light. *New Journal of Physics*, *11*(6), 065003.
[41] Lydersen, L., Wiechers, C., Wittmann, C., Elser, D., Skaar, J., & Makarov, V. (2010). Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature photonics*, *4*(10), 686-689.
[42] Gerhardt, I., Liu, Q., Lamas-Linares, A., Skaar, J., Kurtsiefer, C., & Makarov, V. (2011). Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature communications*, *2*(1), 349.
[43] Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., ... & Zeilinger, A. (2009). The SECOQC quantum key distribution network in Vienna. *New journal of physics*, *11*(7), 075001.
[44] Wehner, S., Elkouss, D., & Hanson, R. (2018). Quantum internet: A vision for the road ahead. *Science*, *362*(6412), eaam9288.
[45] Sangouard, N., Simon, C., De Riedmatten, H., & Gisin, N. (2011). Quantum repeaters based on atomic ensembles and linear optics. *Reviews of Modern Physics*, *83*(1), 33-80.
[46] Lucamarini, M., Yuan, Z. L., Dynes, J. F., & Shields, A. J. (2018). Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, *557*(7705), 400-403.
[47] Bernstein, D. J. (2025). Post-quantum cryptography. In *Encyclopedia of Cryptography, Security and Privacy* (pp. 1846-1847). Cham: Springer Nature Switzerland.