Multimedia Tools and Applications
https://doi.org/10.1007/s11042-024-20535-x

A brief review on Quantum Key Distribution Protocols

Mandeep Kumar[1] · **Bhaskar Mondal**[1]

Received: 2 August 2023 / Revised: 6 September 2024 / Accepted: 17 December 2024

Abstract
Development in Quantum computing paves the path to Quantum key distribution (QKD) by using the principles of quantum physics. QKD enables two remote parties to produce and share secure keys while removing all computing constraints on an adversary. The basic physics laws are used to identify any outside parties eavesdropping on the key exchange. In recent years many revolutionary developments in the field of QKD have been developed to overcome security and networking constraints. This survey provides an overview of the QKD protocol's evolution and quantum network architecture. The paper also demonstrates QKD deployment techniques and elements of the QKD network. It also highlights ongoing design challenges by considering security and error estimation and correction, in contrast to studies concentrating on optical channels and equipment. Finally, this paper examines the possible directions for future research and offers design principles to guide the development of QKD and its related area.

Keywords QKD · Quantum network · Quantum security · Future direction

1 Introduction

Quantum physics offers a quicker and more effective information processing, analysing, and communication method using quantum computers in polynomial time. Quantum information communication requires a new network called a quantum network (QN) [1], that uses quantum physics information and a key exchange mechanism called QKD [2]. As things progress, there is a lot of concern about security in classical communication using classical cryptography. The safety of every cryptographic technique is determined by the robustness of the key used for cryptography operations. The recent development in quantum computing algorithms challenges classical cryptography security.

Peter Shor [3], in 1994, has already published an algorithm based on the quantum information notion to solve the most challenging factorization problem [4] in traditional cryptography. In conventional cryptography, the factorization problem determines the key's strength. Many

✉ Mandeep Kumar
mandeepk.ph21.cs@nitp.ac.in

Bhaskar Mondal
bhaskar.cs@nitp.ac.in

[1] Department of Computer Science & Engineering, National Institute of Technology Patna, Patna 800005, Bihar, India

Published online: 04 January 2025

cryptographic algorithms, including RSA [5] and ECC [6], have proven unsafe against QC. Thus, keys must be generated and distributed utilising information from the quantum system to safeguard against quantum assault. Therefore, the QKD offers a better solution for secure quantum communication.

It is very much essential to secure the communication network from eavesdropping. Eavesdropping in the virtual optical network (VON) can compromise the security of the complete infrastructure. Xiaosong Yu et al. [7] have integrated QKD in a virtual optical network to achieve secure transmission through the optical network. They used QKD to stop Eavesdropping against a VON. As a logical storage set, they used two key pools (KPs) shared by two separate node pairs [8] and the security of key management increases with the usage of KPs. They demonstrated that several variables, including blockage probability, key resource use, and substrate path lengths, significantly impact the optical network's performance. To achieve all these goals, the QKD system has to follow quantum physics law strictly.

Using photons subject to the laws of physics, Bennett and Brassard [9] developed a novel method for QKD. His work was based on Heisenberg's Uncertainty Principle (HUP). Quantum entanglement (QE), which satisfied Bell's theorem [10] of non-locality, was used by Ekert [11] in 1991 for QKD. Significant progress has been achieved in recent years regarding point-to-point QKD protocol, devices, system and communication channels etc. For instance, various QKD protocols have been proposed to provide secure transmission over a QN [12, 13]. QKD has tremendous potential in secure computing, finance and banking, the government sector, space research, healthcare, Quantum Internet (QI), etc.

This work aims to thoroughly survey the many application domains in which QKD can be helpful. The study primarily intends to investigate the relative importance of QKD in providing security in QN. Another goal is to research and build the best network architecture for QKD to increase security. This study is restricted to the QN, key distribution process and their applications.

The paper presents a survey on QKD, starting from the beginning to the current developments. The basic information of QKD, like the working mechanism and transmission media, are described in the Section 2. Section 3 provide a brief overview of different QKD protocol development over time. Section 4 provides the basic design architecture of the QKD network (QKDN) along with its key elements and protocols. Section 5 provide various applications area of QKD along with its design challenges and trade-off and different approach to analysing its security. Section 6 provides QKD-based future research directions. Section 7 a discussion on the QKD protocols, and Section 8 summarises the survey on the QKD.

2 QKD basics

This section presents a fundamental overview of the QKD mechanism, including the transmission media involved and the classification of QKD protocols. Here, we will offer an introductory explanation of QKD, delve into the various transmission media employed in its implementation, and explore the classification system that categorizes QKD protocols.

2.1 Mechanism

Information security can be achieved using either conventional cryptography or quantum cryptography. Each approach is based on fundamentally unique ideas. Classical cryptography, which has been used for many years, relies on mathematical concepts and computing

complexity to guarantee the confidentiality and integrity of data. As shown in Fig. 1, it frequently uses encryption techniques like symmetric and asymmetric key cryptography, where two communicating parties (Alice and Bob) share a key through a classical channel (CCH) [14]. Since it would take a lot of computing power to crack classical cryptography, it is assumed that it can withstand common attacks.

The concepts of quantum physics are used by quantum cryptography to achieve uncrackable encryption and improve the security of communication channels. QKD foundational ideas are used in quantum cryptography. The two communicating parties, Alice and Bob, can safely establish a key using QKD by taking advantage of certain features of quantum mechanics. Figure 2 shows that Alice and Bob use two channels for secure communication. The key is exchanged through the quantum channel (QCH), and encrypted data is shared over the CCH [11]. These algorithms were created primarily to resist attacks from QC.

The basic building block of any cryptography is the key exchange process. QKD protocol provides secure key exchange in quantum cryptography. Figure 3 shows a basic QKD process where Alice and Bob exchange keys using the principles of quantum mechanics. The two channels differ in their working principle, the QCH is used to transmit the physical particles (qubit), and the CCH is used to announce the orientation of the observables and encrypted data. The presence of any adversary in the system gets detected easily because after the measurement optimal quantum value of the system exceeds the upper bound $\pm 2\sqrt{2}$ [15].

The quantum value for the safe key exchange is given by a fundamental principle for testing quantum entanglement known as Bell's inequality [10]. To understand the optimal quantum value, let's consider some basic assumptions of local realism:

- Locality: There must be no influence on the outcome of one particle by the measurement performed on a distant particle.
- Realism: The properties of a particle exist independently of measurement.

Let mathematically formulate Bell inequality for two entangled quantum particles measured along axes x and y, and assuming hidden variables λ that predetermine outcomes, $(E(x, y))$ is the expectation value of the product of the measurement outcomes and given by:

$$E(a, b) = \int d\lambda \, \rho(\lambda) \, X(x, \lambda) \, Y(y, \lambda) \tag{1}$$

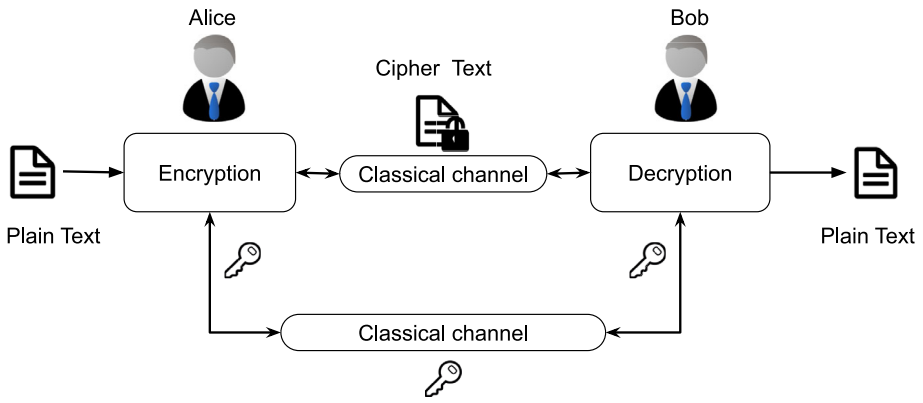


Fig. 1 Basics Classical Cryptogaphy

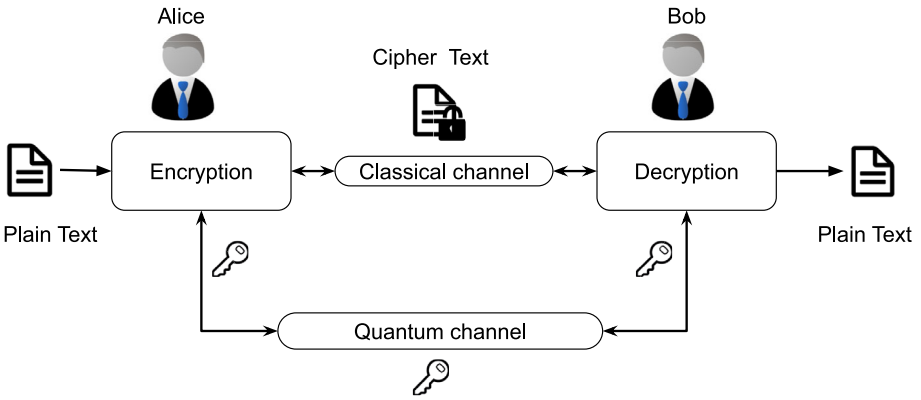


Fig. 2 Basics Quantum Cryptogaphy

where:

- $X(x, \lambda)$ and $Y(y, \lambda)$ are the predetermined outcomes for measurements along two measnument axis x and y, respectively.
- and $\rho(\lambda)$ is the probability distribution of λ.

Bell's Inequality is considered as a correlation of the linear combination of all expectation values, which is as follows:

$$E(x, y) - E(x, y') + E(x', y) + E(x', y') \leq 2 \tag{2}$$

The (2) provides the maximum correlation achievable by any classical theory. An improved version of the theory is given by CHSH inequality in the Section 3.2.

2.2 QKD transmission media

Within the field of communication technology, the two transmission media: guided and unguided are used. A QKD transmission media is relay on both types of media for secure key exchange.

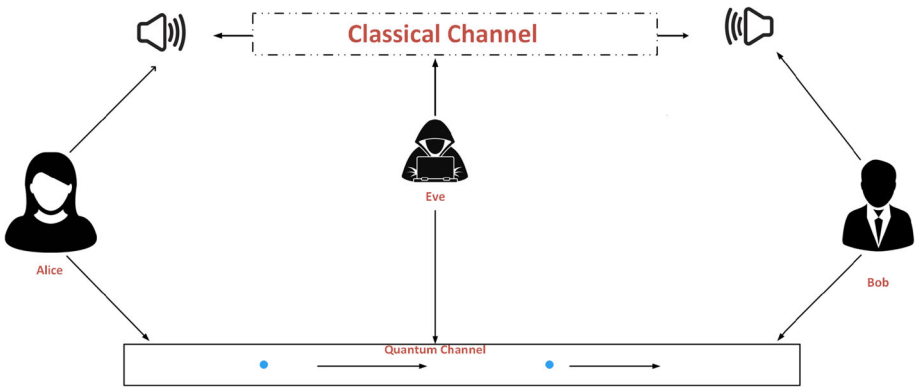


Fig. 3 Basic Key distribution using quantum channel

Guided media The optical fibre is used as guided media to transmit the quantum bit between legitimate parties. It offers a better choice to transmit qubits due to its high stability and minimal loss. Tian et al. [16] have experimentally demonstrated a high-rate discretely modulated CV-QKD over 80 km with a 2.5 Gbaud single-mode optical Fiber. Liu et al. [17] have demonstrated the key rate (KR) of 9.53^{-12} per pules over a distance of 1002 km using optical fibre. The QKD using guided media has some challenges due to its physical properties. The noise and absorption in the optical fibre affect the quantum particles to cover a long distance. Hence we need alternative tools and techniques like quantum amplifiers [18] for long-distance QKD using guided media.

Unguided media The unguided media, like free space, are more flexible than the guided media as it is available on demand and has a high coverage area. Liao et al. [19] have reported a launch of a low-Earth-orbit satellite to implement QKD over a distance of 1,200 kilometres with 20 times greater KR than that of expected guided media (optical fibre) of the same distance. Chen et al. [20] have demonstrated a space-to-ground with a KR of 47.8 kbit per second at a distance of 4,600 km. The network combines a fibre network of 2,000 km and a space-to-ground network of 2600 kilometres.

To move from experimental stages to real-world applications, free-space QKD still needs further study, even though fibre-based QKD has advanced to a higher level of development. Further research is required to develop free-space QKD in real-world circumstances. It is anticipated that establishing a worldwide QKDN and the QI [21] will be significantly aided by integrating QKD over optical fibre and free space.

2.3 Classification

Based on underlying principles, QKD can be classified in four basic aspect of uses, as shown in Fig. 4: physical principles, security principles, practical implementation, and protocol structure. Each aspect of use is further classified based on the quantum mechanics property. The Table 1 segregate all QKD protocols based on aforementioned classification criteria.

Physical principles: In this criteria, the QKD protocols rely on three physics principles such as HUP-based single photon protocols, entanglement-based [22] protocols and continuous-variable (CV) protocols [23]. The single-photon protocol encodes the key information in the polarization states of single photons, where HUP ensures the protocol's security. According to the HUP, a quantum particle's state will change as it is measured, and this characteristic is used to identify any eavesdropping attempts QKD protocols. The entanglement-based protocol uses the correlation between two quantum entangled particles and sends one to each side user to exchange the keys.

CV-based protocols encode data using the continuous variables of a quantum system, like the amplitude or phase of a light wave. Homodyne detection [24], which can identify the quadrature amplitude of the signal, is used to measure these variables. The uncertainty principle underlies the security of CV-based protocols since any attempt to measure the signal will change its state and be observable. Since they can be used with common optical equipment and are less susceptible to outside noise, CV-based protocols are more practical. In contrast to single-photon protocols, they often have lower security levels and key rates.

Security properties QKD protocols can also be classified based on their security properties, such as device-independent security protocols [25] and device-dependent security protocols. Device-independent security refers to protocols that can be proven secure against any eavesdropping attack, and it also does not require any assumptions about the devices used in the

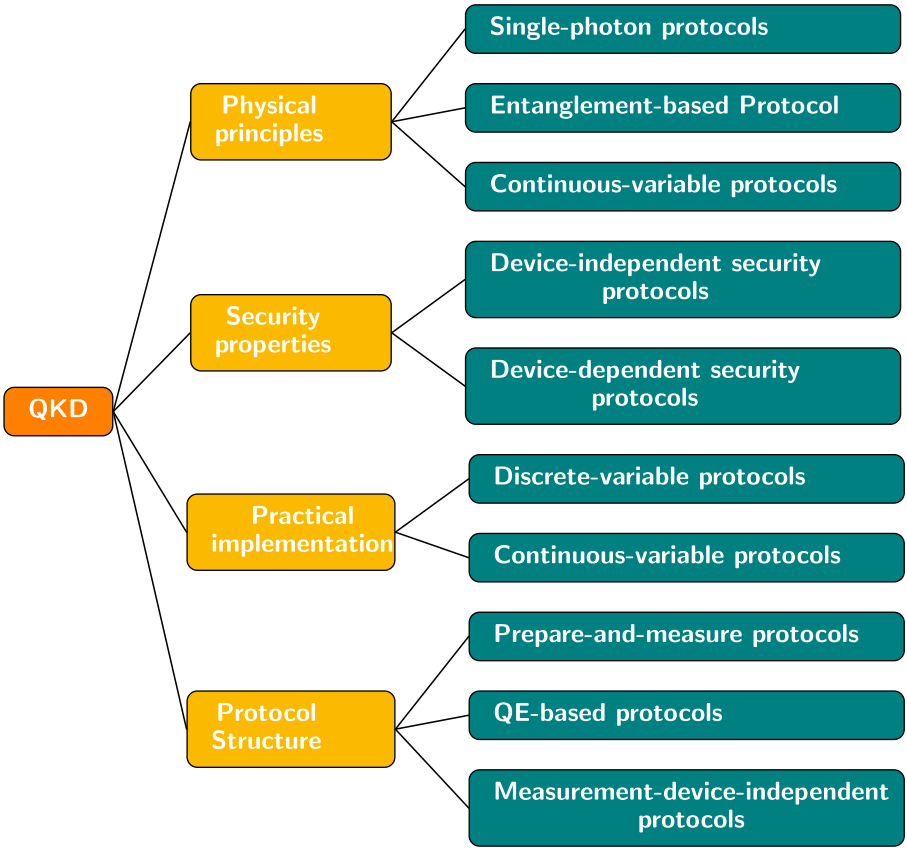


Fig. 4 QKD classification based on four components

Table 1 Classifiation of QKD protocol based on the principle of implementation

Classification criteria	Type	QKD protocols
Physical principle	Single photon protocols	[9, 27–31]
	Entanglement-based Protocols	[11, 32]
	Continuous-variable protocols	[33–36]
Security principle	Device-independent security protocols	[11, 30, 37]
	Device-dependent security protocols	[9, 27–29, 33, 34, 38–43]
Practical implementation	Discrete variable protocols	[9, 27–32, 34, 37–42]
	Continuous-variable protocols	[33, 35, 36, 44]
Protocol Structure	Prepare and measure protocols	[9, 27, 28, 31, 37–40, 45]
	QE-based protocol	[11, 32, 46]
	MDIP	[47, 48]

protocol. The device-dependent protocol depends on the accuracy of the measuring tool [26]. Device-dependent QKD techniques can employ commercially accessible devices and do not need extreme circumstances or high-quality sources of quantum states.

Practical implementation QKD protocols can also be classified based on their practical implementation, such as discrete-variable protocols or continuous-variable protocols. Discrete-variable protocols are implemented using discrete quantum states, such as single polarized photons, while continuous-variable protocols are implemented using continuous quantum variables, such as the amplitude and phase of coherent states.

Protocol structure According to the protocol structure, QKD protocols can be categorized into three categories of protocol: prepare-and-measure protocol (PMP), entanglement-based protocol, and measurement-device-independent protocol (MDIP). In PMP protocols, a shared key is created by the transmitter preparing quantum states and the receiver measuring them. The sender $Alice$ and receiver Bob share entangled states in entanglement-based protocols to create a shared key. The security of the protocol is unaffected by the measurement that the $Alice$ and Bob utilise in MDIP.

3 QKD protocols

This section provides a brief description of the developments in QKD as shown in the Table 2, making it easier to understand the different points of view and difficulties involved in creating a secure key distribution. Additionally, it offers opportunities to investigate fresh and effective QKD methodologies for secure communication.

3.1 BB84

BB84: Bennett et al. [9], in the year 1984, proposed the first QKD protocol in which they used polarized photons for key exchange. Figure 5 depicts two polarisation bases: one rectilinear basis with 0° and 90° representing 0 and 1, respectively, and another diagonal basis with 45° as 0 and 35° as 1, respectively. Alice and Bob use these polarization bases for measurement at their end. For a better understanding, we may witness the BB84 QKD protocol in action. The BB84 protocol uses three fundamental principles in order to exchange the quantum key.

1 According to the idea of non-cloning quantum states cannot be copied which means that an opponent or Eve cannot produce the key by copying the quantum state.
2 Measurement has caused the state to crumble. Bitstreams are created with the use of several measurement bases, which is a vital feature of QKD. The system's current state must be disturbed to extract information using the measurement basis he provided.

To test conditions 2 and 3, put the system in the following state.

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$$

Assuming that the system's original state is lost and that the computational basis of measurement is $\{|0\rangle, |1\rangle\}$. Assume the measurement result is 0. Then, if we utilise the $|\pm\rangle$ basis, we will receive a different state than before:

$$|0\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}}$$

Table 2 QKD Protocols with security analysis methods and key rate

QKD protocol & year	Characteristics	Attack resistance	Security analysis methods	Key rate
BB84 [9], 1984	Use polarization states	Man-in-middle	Conditional min-entropy	16.5 kbit/s
E91 [11], 1991	Based on entanglement	Intercept and resend (IR)	Delayed measurement and no-cloning theorem, and Bell's inequality	–
BBM92 [45], 1992	Use entanglement	IR	Use of nonorthogonal states, Parallel repetition theorem, and Bell's inequalities.	–
B92 [27], 1992	Uses two non-orthogonal states similar to BB84 [9]	Photon number splitting (PNS) and phase noise attacks.	Poisson distribution	$4\mu Tq$
SSP [28], 1999	Based on phase encoding and sequential transmission of single photons	IR	Glass slabs with Brewster's angle, delayed measurement	33 bits/s
GG02 [38], 2002	uses Gaussian modulated coherent states	IR, man-in-middle	Gaussian variables, sliced reconciliation protocol	$\frac{1}{2}\log_2(\frac{1}{\chi})$ where χ is noise in channel
Ping-Pong [39], 2002	Use entanglement	IR	Stinespring dilation theorem	$\frac{1-c}{1-c(1-d)}$ where c is control run and d is detection probability
DPS [40], 2003	Based on phase encoding	IR	Four nonorthogonal measurement settings	$1-\frac{1}{N}$ where N is number of sequential pulses
COW [41], 2004	Based on phase encoding	PNS, IR	Error correction, privacy amplification, binary entropy	$17.0 \pm 0.1kHz$
SARG04 [29], 2004	Use polarization states and four non-orthogonal states	PNS, cloning	Weak pulses implementation and QBER estimation	$\frac{1}{1-\chi}$
Decoy state [37], 2005	Use polarization states and decoy states	PNS, man-in-middle	Global hash function gottesman-lo-lïutkenhaus-preskill	$\mathcal{O}(\eta)$ where η: Transmission probability of channel

Table 2 continued

QKD protocol & year	Characteristics	Attack resistance	Security analysis methods	Key rate
S13 [30], 2013	Uses single photon interference and decoy states	IR and PNS	Private Reconciliation, Random Seed	–
RRDPS [31], 2014	Uses multiple phase shifts to encode	PNS	Random number generator	200 bits/s
Self-Referenced CV-QKD Protocol [33], 2015	Uses continuous variable of amplitude of phase	Individual, collective, side-channel	Conservative noise mode	63.26 kbit/s
Time-Bin QKD Protocol [42], 2015	Uses time-bin encoding	Gaussian collective attack	Franson interferometry	8.7 bits/coincidence
QKD Using Entanglement Parity Bits [32], 2017	Uses entanglement and parity checking	IR	Intrinsic efficiency, hash function	–
Twin-Field QKD Protocol [47], 2018	Uses single-photon interference	Beam-splitting	QBER, Encoding scheme	1.26 Mbps over 50km
QKD with pseudorandom bases [43], 2018	Uses pseudorandom bases	IR and PNS	Pseudorandomness of Legendre sequences, binary sequences	Greater than 16.5 kbit/s
Reference-Frame-Independent QKD [46], 2019	Use entanglement	PNS	Phase-randomized weak coherent source, weak decoy state	13.72 Mbit/s
Discrete-Modulation CV-QKD Protocol [34], 2020	Uses continuous variable of amplitude of phase	Gaussian attacks	Discrete modulation	Rigorous analysis based on different parameters [34]
Trans-Media CV-QKD Protocol [35], 2021	Uses continuous variable of amplitude of phase	IR	Modulation variance	–
TF-QKD with PPPs [44], 2022	Based on phase encoding	PNS and Detector blinding attacks	Phase-Matching	10^{13}/pulse
SCS-QKD [36], 2023	Based on subcarrier frequencies	PNS, Cross-talk attacks, jamming	TWCC	Can be obtained using AOPP method

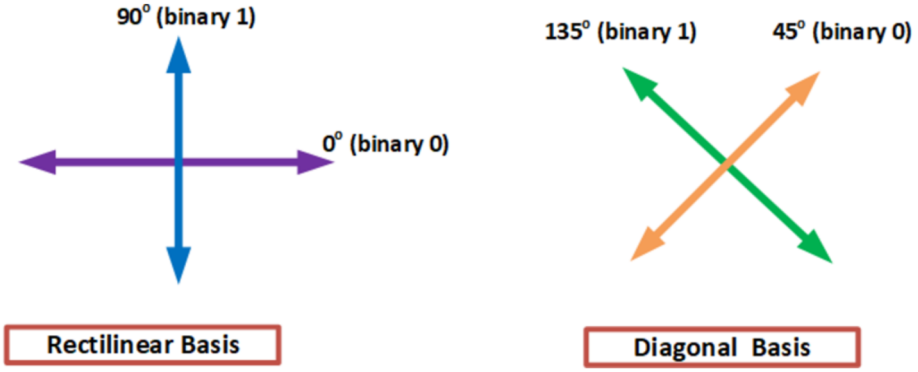


Fig. 5 Measurement basis for BB84 QKD Protocol [9]

On selecting the $|\pm\rangle$ as the measurement basis, there is only 50% chance of getting $|+\rangle$, meaning the state is altered during transmission. The protocol generates the key using the computational basis $\{|0\rangle,\ |1\rangle\}$ along with $|\pm\rangle$. We can see the relation between these two bases using the following:

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}},\ |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$$

Alice creates a key, with a string of $2n$ qubits randomly. She selects one of the following four states to develop every single qubit:

$$|0\rangle,\ |1\rangle,\ |+\rangle,\ |-\rangle$$

Among the two different bases, Alice randomly selects the basis for each qubit to generate each binary bit in the string. Considering the ordinary probability, the half n bits are created using $\{|0\rangle,\ |1\rangle\}$ basis and other n half bits are created using $|\pm\rangle$ basis. Now Alice and Bob tell their measurement basis all binary bit positions over a conventional communication channel. If Alice and Bob have used different basis for any particular binary bit positions, they discard that binary bit. After discarding the binary bit, both parties will have the same binary bit sequence, and this sequence of binary bits will be the secret key for both. Figure 6 depicts an overview of the BB84 protocol used to create keys on both the Alice and Bob sides.

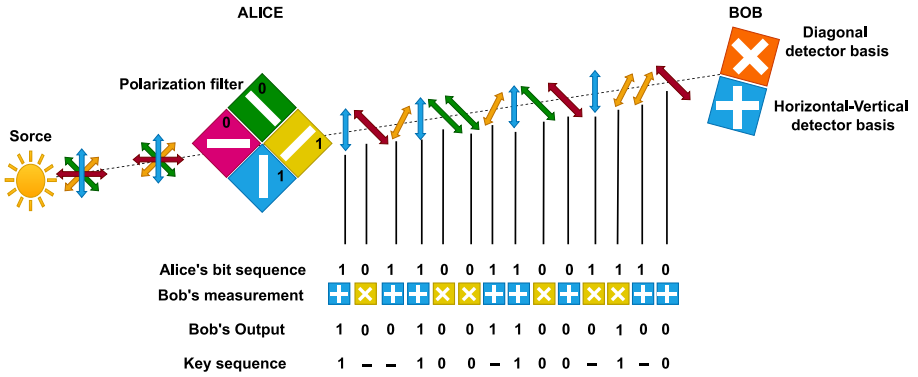


Fig. 6 Principle of the BB84 protocol [9]

3.2 E91

The E91 Protocol [11] was the first entanglement-based QKD protocol proposed by Artur Ekert in 1991. E91 uses the concept of Bell's non-locality to demonstrate the key exchange protocol. In this protocol, a source share spin-$\frac{1}{2}$ singlet pair of the particles among Alice and Bob, having a correlation defined by the (4) through a QCH. Alice and Bob, the two communicating parties, select a random orientation of their analyzers to measure the qubit received by the source. Upon the measurement, they get binary one-bit information as a result in +1 (spin up) and -1 (spin down). According to the quantum rules [10]:

$$S(a_i, b_j) = -a_i.b_j \tag{3}$$

and the quantity

$$S(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{+-}(a_i, b_j) - P_{-+}(a_i, b_j) \tag{4}$$

is the correlation coefficient of Alice and Bob's measurements performed along the unit vector direction a_i and unit vector direction b_j, respectively. Here the $P_{\pm\pm}(a_i, b_j)$ is the probability results $\pm$ along a_i and b_j each. Quantum mechanics predict anti-correlation results for the two pairs of photons if they measure in the same analyser orientation. Hence from (3) results obtained by Alice and Bob for the two pairs ($a_2,\ b_1$ and $a_3,\ b_2$) of same analyser orientation is:

$$S(a_2, b_1) = S(a_3, b_2) = -1 \tag{5}$$

Before going into the working protocol, let us follow CHSH [49]. CHSH defines a quantity composed of correlation coefficients shared among distinct parties for the different orientations of their analysers,

$$\mathcal{B} = S(a_1, b_1) + S(a_3, b_1) + S(a_3, b_3) - S(a_1, b_3) \tag{6}$$

and hence Quantum mechanics requires.

$$\mathcal{B} = \pm 2\sqrt{2} \tag{7}$$

In this protocol, the entangle pairs are measured by Alice and Bob by randomly selecting analyser orientation, respectively. They share the measurement bases (analyser orientation) through the public channel to each other. They agree to discard all the different analyser orientations and keep the results obtained through the same analyser orientation. From (5) and the result obtained after discarding some photons can be decoded into a secret string of bits. The final bit string will be the key to secure communication. And to test the presence of an eavesdropper, the CHSH is used, and if the $-2\sqrt{2} \leq \mathcal{B} \leq 2\sqrt{2}$ means no eavesdropper is listening to the communication.

3.3 BBM92

BBM92 protocol [45] uses pairs of entangled photons which can be considered an entanglement-based modification of [9]. Alice creates polarisation states at random in the prepare and measure-based BB84 technique, whereas randomness is inherent in the entangled photon pair measurement in the BBM92 approach. The entanglement-based QKD (EBQKD), like BBM92, is best for ground-to-satellite-based communication because it doesn't need a trusted node [50].

Charlie creates a spin-half singlet state pair of photons through a QCH and delivers them to Alice and Bob. Optical fibre, space, or water can all be possible QCH. Both Alice and Bob do

their measurements in an ad hoc manner. Both declare their base selections through the public channel after completing the measurement. The remaining measurements are eliminated, and only those that Alice and Bob selected as their foundation contribute to the key. The sifted key refers to the key that results from this operation. The state of polarisation entangled produced by this technique is:

$$|\psi\rangle = \frac{|HH\rangle + |VV\rangle}{\sqrt{2}}$$

To create a secure key, a quantum bit error (QBER) has to apply to get the sifting key. The formulas for calculating the QBER (Q) and sifted-KR (SKR) are

$$Q = \frac{1 - visibility}{2} \tag{8}$$

After Error correction, the secret key is given by

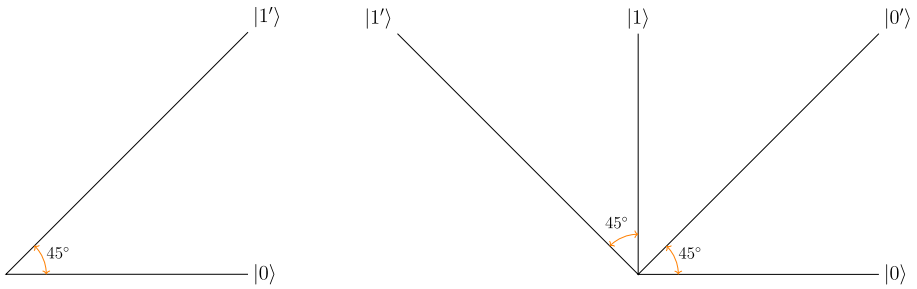
$$R_{sec} = n\left(\frac{1}{2} - 2 \times Q - s\right) \tag{9}$$

where n and s are the number of uncorrected bits and security parameter [51] respectively. It is clear from the visibilities that the lower value of R_{sec} directly results from the worsening atmospheric conditions.

3.4 B92

B92 [27] was an updated and simplified protocol for QKD. In this protocol, both the parties Alice and Bob use two different non-orthogonal bases $|0'\rangle$ and$|1'\rangle$ for the measurement . The steps of B92 is as follows:

1 Initially, Alice starts a stream of random basis $|0\rangle$, $|1\rangle$ and qubits $|0'\rangle$, $|1'\rangle$.
2 The two non-orthogonal states are shown in Fig. 7a, *Alice* measures these qubits by the stream of basis it is sending, then sends them to Bob via the QCH.
3 Bob produces a stream of random basis, as shown in Fig. 7b and evaluates the qubits Alice provides.
4 Bob will broadcast the measurement results over the CCH.
5 The measured qubit for a key will be chosen as the secret of the key if Bob's and Alice's basis are identical.



(a) Alice's basis (b) Bob's basis

Fig. 7 Measurement basis of Alice and Bob

3.5 SSP

Six-state protocol (SSP) [28] uses entangled pair of photons in which each party selects one of the three conjugate polarisations basis from [52] at random for all photons. This approach has an improved capacity to detect listening devices/eavesdroppers. Two nearby non-linear crystals experience a pump beam at 351 nm. This source of polarized entangled photon pairs is described in [53]. The crystal can generate pairs of photons that are polarised either horizontally or vertically. The down-conversion photons are created in the polarization-entangled state as

$$\frac{(|HH\rangle + |VV\rangle)}{\sqrt{2}}.$$

Using a calcite Glan-Thompson PBS [54], a Pockels cell, and a liquid crystal (LC), from each entangled pair, Alice and Bob get one photon and randomly perform measurement based on any three selected basis—H/V, L/R, or D/d. To find coincidences between the detectors of Alice and Bob, a collecting window is opened for all basis cycles at the end. The first such coincidence activates a digitizer, which stores both the LC and PC states. Our measured rate of 'raw' key generation and the cycle time serve as limits for the event rate. All electro-optic [55] phase changers and enhanced sources should enable higher rates. Alice and Bob sift through the raw key to only include instances where they precisely measure one photon simultaneously. One of the objectives was to detect intervening eavesdroppers.

3.6 GG02

An alternative QKD paradigm called continuous variable (CV) technology uses weak light pulse quadratures to encode quantum information. The GG02 [38] QKD protocol is as CV-QKD, which is based on single Gaussian beam protocol [56]. Under the appropriate circumstances, CV-QKD exhibits significant promise for higher KR and uses commercially available, well-known hardware, such as homodyne detectors [57].

Alice sends Bob a randomly modulated Gaussian beam via a noisy Gaussian channel. Since this enables the highest information rate, phase and amplitude have been modified using the Gaussian random numbers. Bob next determines the beam's phase or amplitude and tells Alice about his measurement choice. Once Bob and Alice obtain the two correlated sets of Gaussian variables [58], they can use those sets to derive a shared secret string of bits. The proposed protocol uses a low-loss optical network to send light pulses, which is the same as in the coherent optical telecommunication network because it does not require squeezing. All pulses will be valuable in that scenario, but $\frac{1}{2}$ of Alice's messages will be lost.

3.7 Ping-Pong

Ping-pong was first introduced by Boström et al. [39] in 2002. Alice and Bob agree to share photons of maximally entangled Bell state

$$|\psi^{\pm}\rangle = \frac{|10\rangle \pm |01\rangle}{\sqrt{2}} \tag{10}$$

mutually orthogonal to each other and a measurement operator $\hat{\sigma}_z^A$ used to flip between two states $|\psi^{\pm}\rangle$.

$$\hat{\sigma}_z^A |\psi^{\pm}\rangle = |\psi^{\mp}\rangle \tag{11}$$

Bob prepares two qubits in the maximally entangled state $|\psi^+\rangle$. He sands one photon to Alice, naming it "Ping!" (travel qubit) and keeps one with himself called (home qubit). Alice chooses to carry out the measurement operation (11) on the travel qubit, or she chooses to do nothing. The travel qubit is then returned to Bob named "pong!". The ping-pong protocol is as follows:

Step 1: Let the message sequence to transmit is $m^N = (m_1, \cdots, m_N)$ where $m_n \in \{0, 1\}$.
Step 2: for $n = n + 1$ Bob prepares two Bell states as shown in (10).
Step 3: Bob sends the travel qubit to Alice and stores the home bit. The mode of ending the qubit is using the QCH.
Step 4: Based on the probability of the state received, Alice, switch to Step A or Step *i*.
Step 5: Alice send message x^N to Bob
Step A: Alice measures on basis $\mathcal{A}_z$ and gets the output $i \in \{0, 1\}$
Step B: she transmits i to Bob using the public channel
Step C: After receiving i, he will get output j after measuring the home qubit in the measurement basis $\mathcal{A}_z$
Step D: if $i = j$: Aboard the transmission (Eve is detected)
Step E: else Set $n = n - 1$ and Goto Step 1.
Step i: Let $\hat{\mathcal{K}}_0 = \mathbb{I}$, $\hat{\mathcal{K}}_1 = \hat{\sigma}_z$, for $m_n \in \{0, 1\}$; and Alice perform the operation $\hat{\mathcal{K}}_{m_n}$ on a qubit and send it back to Bob
Step ii: Bob, on receiving the maximally entangled state, performs the Bell measurement on both qubits and results in a final state $|\psi'\rangle \in \{|\psi^+\rangle, |\psi^-\rangle\}$. Decoded message is

$$\left|\psi^{'}\right\rangle = \begin{cases} |\psi^+\rangle \text{ for } m_n = 0 \\ |\psi^-\rangle \text{ for } m_n = 1 \end{cases} \tag{12}$$

Step iii: if($n < N$) GOTO Step 2; else if($n = N$) GOTO Step 5

3.8 DSP

In this protocol [40], Alice splits a photon from a single-photon source [59] into three different routes, namely (a, b, and c), which are then recombined by utilizing a device called beam splitters (BS) or optical switches (SW). Between paths b and c, as well as between paths a and b, there are equal time delays of T. The BS splitting ratios are set up so that there is an equal chance of a photon passing through each path. For each pulse, 0 or 1 arbitrarily phase modifies the recombined photon. Bob splits the incoming photons into two directions and then uses 50:50 BS to join them. The pulse interval T equals the time delay due to the path lengths. Photon detectors (DET1, DET2) are kept at two output ports of the recombining BS, respectively.

Bob probably counts a photon four times in the step that is shown:

Step 1: A photon may pass through Alice's path and Bob's shortest path.
Step 2: A photon may pass across Alice's path *a* and Bob's longest path, as well as Alice's path *b* and Bob's shortest path.
Step 3: A photon may pass across Alice's path *b* and Bob's longest path, as well as Alice's path *c* and Bob's short path.
Step 4: A photon may pass through the Alice's path *c* and the Bob's longest path.

The steps of the secret key are as follows:

Step 1: Bob keeps track of the moment and the detector that clicks each time it happens—usually the second or third time.

Step 2: Alice is informed by Bob about the photon detection's time instance.
Step 3: Alice can determine which detector has been used on Bob's side using this information and her modulation data.
Step 4: When the DET1 and DET2 clicks correspond to "0" and "1", respectively, Alice and Bob will have the same binary bit string.

Bob provides Alice with the time instance in this protocol, which is not shared with the public.

3.9 COW

The purpose of COW protocol [41] is to obtain the secret key bits using the most straightforward measurement feasible in this circumstance—the timing of a pulsation's arrival. Quantum coherence is periodically examined to maintain security. Eve, who assaulted the line and learned some useful information about the binary bit values at the cost of adding errors, is responsible for the loss of coherence. The proposed protocol is as follows:

Step 1: Alice repeatedly sends binary 0 with the probability $(1 - \frac{1}{2}f)$, binary 1 with the probability of $(1 - \frac{1}{2}f)$ [41], and the decoy sequence with probability f.
Step 2: Exposing at the end of the conversation the bits, Bob acquired data line detection and the times when detector D_{2M} has triggered.
Step 3: Alice notifies the Bob of the bits he needs to delete from his raw key.
Step 4: By examining the D_{2M} detections, Alice computes Eve's information and estimates the coherence break using the visibilities $V_{(1-0)}$ and V_d associated with decoy and bit sequences (1, 0).
Step 5: Alice and Bob develop a secret key after running an error rectification and privacy amplification.

3.10 SARG04

SARG04 protocol [29] provides security against PNS attacks, which BB84 protocol fails to achieve. Unlike BB84 protocol, they do not announce measurement basis, instead, they announce one of the four non-orthogonal state $\mathcal{B}_{\omega_a,\omega_b} = \{|\omega_a x\rangle, |\omega_b z\rangle\}$, with $\omega_a, \omega_b \in \{+, -\}$ and with four state $|\pm x\rangle$ code for 0 or $|\pm z\rangle$ code for 1. Alice transmitted $|+x\rangle$ and proclaimed the set $\mathcal{B}_{++}$ for a certain qubit. If Bob has measured σ_x, which has a 50% chance of occurring, he has unquestionably obtained the result 1; yet, since this result is viable for both states in the set $\mathcal{B}_{++}$, he must reject it. If Bob measured σ_z and the result was 1, he is again unable to discern. However, if he tested σ_z and obtained a result of -1, he would know that Alice had sent $|+x\rangle$ and would have added a 0 to his key.

The protocol uses non-orthogonal qubit states, which can make key distribution protocol robust against PNS attacks. The quantum bit error rate (QBER) is lower down to 9% [60], but In Ref. [61], they have successfully obtained the QBER to 5%.

3.11 Decoy state

Lo et al. proposed decoy state QKD [37], similar to the BB84 [9] protocol. The only difference is that it utilizes decoy state (which is first proposed by Hwang [62]) to detect the existence of an eavesdropper by emitting some additional proton. In order to defend against the PNS attack for the BB84 QKD protocol in the event of substantial loss, the decoy-pulse technique

is applied. An authorized user deliberately and arbitrarily replaces signal pulses with multi-photon pulses.

3.12 S13

S13 protocol [30] differs from the very first proposed BB84 [9] protocol in that it uses asymmetric cryptography and the private reconciliation from the random seed in addition to being similar to the BB84 protocol for all quantum manipulations. It allows the creation of more robust, secure keys. This QKD protocol essentially uses two distinct processes: a key exchange derived from the first interpretation of the states that the Alice and the Bob exchanged. Second is the public reconciliation, where Alice and Bob use the knowledge made public to find the secret key. Thus, QKD is the only physically secure way to exchange secret keys. In contrast to the BB84, where the predicted is 50%, the reconciliation key's percentage of coincidence with the raw key's size is 100%. This protocol, known as the SARG04 [29], shares all quantum manipulations with the BB84 and only differs in the classical communication method.

3.13 RRDPS

The foundation of the proposed RRDPS QKD protocol [31] is an entirely separate idea. Alice encodes bit sequences into non-orthogonal states, and Bob randomly decides how to decode a single bit from the sequence. Eve cannot accurately guess the bit value because they cannot learn the entire sequence. By taking complementary decisions between two conjugate observable measurements, a feasible rate of safe key distribution is determined.

The proposed protocol [31] is as follow:

Step 1: Alice utilises a random binary number of l-bit sequence $(a_1 a_2 \cdots a_l)$ on weak signal and the encrypted signal is a single-photon state of l optical pulses

$$|\psi_1\rangle = \frac{1}{\sqrt{l}} \sum_{k=1}^{l} (-1)^{a_k} |k\rangle \tag{13}$$

Where every photon is in k^{th} pulse for the $|k\rangle$ state.

Step 2: After receiving the signal, Bob announces the number r generated by a random number generator (RNG) where $r \in \{1, \cdots, l-1\}$.

Step 3: Bob tries to determine values=$v_i \oplus v_j$ where $(i, j) \subset \{1, \cdots, l\}$ and must satisfy the condition

$$j - i = \pm r(\mod l)$$

where $\oplus$: summation modulo 2

Step 4: Bob uses a beam splitter to divide each pulse into two halves and then combines the k^{th} and k'^{th} half pulses to determine the phase difference of a photon.

$$(k' = k + r(\mod l), k = 1, \cdots, l)$$

Bob declares i, j, stores the phase difference as his sifted key S_B. The shifted key which Alice recorded is $S_A = a_i \oplus a_j$.

3.14 Self-Referenced (SR) CV-QKD protocol

Soh et al. proposed an SR-CV-QKD-based [33] that calculates the local oscillator power required for the transmission between the two communicating parties. The measurement basis for the communicating parties is aligned based on twin reference pules. SR-CV-QKD is a potential improvement over existing CV-QKD methods with a better KR.

3.15 Time-Bin QKD protocol

Zhong et al. [42] in 2015 proposed an encoding scheme that provides security against collective Gaussian assaults during key distribution. The protocol ensures a higher bit rate of 8.7 bits per coincidence. They were able to achieve this KR due to four key elements [42] without loss. It can withstand error correction with massive system error by optimising time-energy entanglement generation and using highly effective WSi [42] superconducting nanowire single-photon detectors.

3.16 QKD using entanglement parity bits

Alshowkan et al. [32] suggested a three-party QKD system that is deterministic, effective, and can help two untrusted users construct a key using a third party. This protocol uses a QCH comprising two maximally entangled states $\frac{|00\rangle+|11\rangle}{\sqrt{2}}$ and a single two-particle von Neumann measurement to transmit the secret key. They have used two controlled-NOT gates to the parity bit of the entangled spins to help prepare the secret states. Additionally, each user's system receives the inclusion of an ancillary state. As a result, by employing a controlled-NOT gate followed by controlled-U gates, the users can recreate their target states correctly.

3.17 Twin-Field QKD protocol

Lucamarini et al. [47] have used a continuous-wave laser to propose Twin-Field (TF) QKD protocol. The two arms of the interferometer receive the light beam and transmit it across them. The correct polarization is adjusted using polarisation controls, and it stays till the duration of the phase drift. The intensity of the photons entering the interfering beam splitter is regulated by adjustable attenuators. The preparation stage is connected to the beam splitter and detection stage by two similar single-mode optical fibre. The phase drift is seen at the detecting stage using a power meter (Key sight 7748A) with a sampling rate of 40 kHz and a power range of 110 dBm to 10 dBm.

3.18 QKD with pseudorandom bases

Trushechkin et al. [43] have proposed a QKD model with pseudorandom bases to prepare the state. Using a standard pseudorandom base sequence enables the protocol to avoid the sifting process and, as a result, lose the other half of the key. Furthermore, since their bases are constant, Alice and Bob can employ more than two bases. They observed that, for single-photon sources, the protocol offers a secret KR that is twice as high as those provided by the original BB84 protocol and, in some situations, slightly more significant than those offered by the BB84 protocol.

3.19 Reference-Frame-Independent QKD

Liu et al. [46] in 2019 proposed a reference-frame-independent (RFI) QKD protocol. RFI-QKD requires less alignment compared to the BB84 protocol [9]. However, the protocol requires three measurement bases from Bob and six encoding states provided by Alice. To overcome this, the RFI-QKD protocol is still safe even when Alice sends just three states, consisting of two eigenstates of the Z-basis and one eigenstate of the X-basis. With stochastic fluctuations in finite-key sizes, this updated method accounts for security against coherent assaults while producing comparable secret KR and distances covered. The viability of this method was shown in a proof-of-concept experiment employing time-bin encoding, which significantly lessens experimental complexity by doing away with the requirement for a high-speed phase modulator.

3.20 Discrete-Modulation CV-QKD protocol

Ghalaii et al. [34] have proposed a discrete-Modulation (DM) CV-QKD protocol based on quadrature phase shift keying modulation known as quantum scissor (QS). They optimised the necessary system parameters and discovered that the QS-equipped system could withstand more excess noise than the discrete-modulation system without a QS, allowing it to go farther at extra noise. They showed that attaining favourable secret KR in high loss and high excess noise operating regimes would be challenging without a non-Gaussian CV-QKD protocol with discrete modulation.

3.21 Trans-Media CV-QKD protocol

Guo et al. [35] have proposed a novel CV-QKD protocol based on trans-media (TM) to establish secure atmospheric and underwater communication using suitable photon subtraction operations. This operation was used to enhance the performance of the trans-media CVQKD scheme and it can also maximize transmission distance. They established a relationship between the trans-media CVKQD scheme's secret KR and transmission distance. The KR will vary because the photon reduction operation will result in the loss of quantum signals in the multi-media channel. Hence Alice and Bob cannot create a suitable secret KR because sufficient data was lost.

3.22 TF-QKD with PPPs

Zhou et al. [44] in 2022 have proposed TF-QKD with partial phase postselection. In decoy mode, phase postselection is added to boost performance. They have demonstrated the universal security of the suggested protocol in the finite-key situation against coherent attacks by applying an operator dominance condition, and numerical simulations support its potential benefits in terms of KR and reachable distance. The scheme also applies to an optimised four-phase twin-field protocol, confirming its potential benefits regarding feasible distance and KR.

3.23 SCS-QKD

Jiang et al. [36] have proposed a side-channel-secure (SCS) QKD with imperfect vacuum pulse source generators. The SCS-QKD protocol achieves a more secure distance with the

imperfect vacuum source at an intensity lower than 10^{-8}. They have demonstrated that the SCS-QKD protocol can be directly applied to two-way classical communication (TWCC) techniques, including the regular TWCC and active odd-parity pairing (AOPP) methods, to increase KR and secure distance. The KR in all lengths may be improved by around two times, and the safe distance can be increased by about 40 kilometres, according to their numerical simulation results.

The Table 2 briefly reviews the QKD protocols, including protocol essential characteristics, security against possible attack, security analysis methods used and the key rate. Table 3 provides the strength and weakness of each protocol.

4 QKD network

A QKDN comprises multiple QKD nodes connected through optical fibre or free space links [63]. The primary purpose of this network is to establish secure communication channels by negotiating keys between QKD nodes. This section provides QKDN architecture, elements of QKD, network interface and protocol. However, as networks using quantum repeaters and untrusted relays are not yet ready for real-world scenarios, this section will primarily focus on networks using optical switching and trusted relaying methods.

4.1 QKD network architecture

The essential requirement of secure communication is a QN inspired by the classical communication network. Figure 8 provides an overview of the QKDN with three basic layers: the application layer, the control and management layer, and the infrastructure layer. This all-encompassing viewpoint is based on [64]'s four-layer network architecture.

Application layer The application layer in Fig. 8 provides necessary cryptographic applications to the user. The QKDN manager receives initial security requirements from cryptographic applications, such as rate and update period. After receiving these requests, the QKDN management investigates if the appropriate QKD nodes have the necessary keys. If real-time secret keys are available for supporting cryptographic applications, the QKDN management instructs the QKDN controller to inform the pertinent QKD nodes to provide keys in the appropriate format. Otherwise, cryptographic applications must wait until the secret-key pool is replenished. Data transmission via the application link has been encoded using these keys. Notably, after each cryptographic programme has the keys, they are responsible for their usage alone, and the QKD nodes and QKDN manager are no longer held accountable. Depending on the secret-key resources that are available inside the network or system as well as the users' secret-key needs, a QKDN or system can support a certain number of users. As a result, there is a trade-off between user needs and key resources. For instance, the Cambridge QKD metro network [65] can accommodate more than 10000 users with the key requirement exceeding one kbps thanks to its 2.5 Mbps key resources for every connection.

Control and management layer All QKD nodes are governed by the QKDN controller, which also manages their activation, deactivation, and calibration. The QKDN manager is in charge of managing the entire QKDN. It oversees the QKDN controller and keeps track of the node's and link's conditions. The gathered statistical information is routinely updated and saved in a database. The QKDN controller or manager cannot access the keys kept in the QKD

Table 3 Strengths and Weaknesses of QKD Protocols

QKD Protocol & Year	Strength	Weakness
BB84 [9], 1984	The protocol is simple and easy to implement, and under ideal use cases, the protocol provides unconditional security	Vulnerable to PNS attack and requires additional bits to check security
E91 [11], 1991	Secure against man in middle attack due to Bell's inequality test	Face practical challenges due to resource constraints
BBM92 [45], 1992	Secure against man in middle attack due to CHSH test	Protocl is very much affected by noise in the communication channel.
B92 [27], 1992	It is a simplified BB84 protocol with two states.	It is vulnerable to the intercept-resend attacks.
SSP [28], 1999	It is secure against side-channel attack.	It is vulnerable to PNS attack.
GG02 [38], 2002	It provides a higher key rate in the noise channel also.	It is complex to implement.
Ping-Pong [39], 2002	It provides unconditional security under ideal scenario.	Under noise, channel protocol shows higher decoherence.
DPS [40], 2003	Protocol is simple to implement and shows a higher key rate.	It is vulnerable to IR attack.
COW [41], 2004	It is secure against side-channel attacks.	Due to the lack of synchronization between communicating parties, it is vulnerable to Trojan horse attack.
SARG04 [29], 2004	It is resistance to PNS attack.	It has a lower key rate compared to the BB84 protocol.
Decoy state [37], 2005	Provides a better key rate than BB84 protocol, and it is resistant to PNS attack.	Due to decoy state the complexity of the protocol is higher.
S13 [30], 2013	The protocol is robust against misalignments in quantum communication.	It requires better encoding and decoding schemes to avoid IR attack.
RRDPS [31], 2014	The protocol is robust against various attacks as it uses random number generation and phase shift for encoding.	The protocol requires a temporal encoding scheme in case to achieve higher precision.
Self-Referenced CV-QKD Protocol [33], 2015	It reduces alignment issues from the phase-amplitude.	The protocol is complex to implement.
Time-Bin QKD Protocol [42], 2015	Time bin encoding allow easy protocol implementation over optical fiber.	Time synchronization is critical.
QKD Using Entanglement Parity Bits [32], 2017	Additional parity bit provide better security against eavesdropping.	Additional overhead in key distribution due to parity bit.
Twin-Field QKD Protocol [47], 2018	The protocol allows key distribution over a long-range (more than 500km).	The protocol is vulnerable to phase error.

Table 3 continued

QKD Protocol & Year	Strength	Weakness
QKD with pseudorandom bases [43], 2018	Measurement basis selection made by the parties become unpredictable to eavesdroppers.	
Reference-Frame-Independent QKD [46], 2019	The protocol is robust against misalignments in quantum communication.	Additional operations used in the protocol lead to efficiency loss.
Discrete-Modulation CV-QKD Protocol [34], 2020	Protocol provide higher key rates.	The protocol takes advantage of discreet modulation and continuous variables, due to which implementation complexity is higher.
Trans-Media CV-QKD Protocol [35], 2021	The protocol allows key distribution in different media like free space and optical fiber.	It is pron to error due to channel environment factors.
TF-QKD with PPPs [44], 2022	It allows longer transmission range using phase encoding.	It requires higher phase correction due to increased transmission range.
SCS-QKD [36], 2023	Provide higher key rate and resistance to noise.	The protocol is difficult to implement due to its complexity.

nodes [66, 67], nor can they be moved between various physical locations. Consequently, even using the control and administration layer, the security of keys remains guaranteed.

Infrastructure layer The Infrastructure Layer, shown in Fig. 8, is the basic structure of the QKDN and includes several physical objects [64] created especially for QKD networking. These physical objects are deployed in the QKD nodes to protect the network against physical

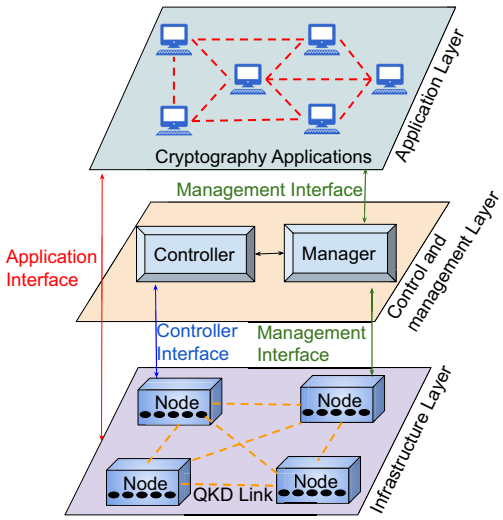


Fig. 8 QKDN architecture

threats. QKD nodes can be connected by free-space cables or optical fibre. Each pair of QKD nodes select a secret key from a randomly generated symmetric random bit string. As a result, QKD protocols or physical devices created separately by several suppliers may be adopted [68]. Since keys are made up of traditional bit strings, they are immediately stored in the corresponding QKD nodes [64]. Each QKD node keeps track of specific parameters related to its secret keys. This contains the time stamp and identification of the physical device in charge of creating and storing keys and identifier, size, rate, and type of keys [69]. The relevant connection parameters, such as the length and kind of links as well as the QCH error rate, are also recorded by each QKD node.

4.2 QKD network elements

On the basis of the overall design of the QKDN shown in Fig. 8, the relevant QKDN components are elaborated.

QKD node The QKD nodes have been categorised as either backbone nodes or access nodes in a heterogeneous QKDN that consists of several network segments of variable sizes [70]. Figure 8 shows that each QKD node comprises various physical devices. These gadgets include multiplexers/demultiplexers, optical switches, QKD transceivers, key managers, and secure infrastructure. Local secret keys are created using a transmitter and a receiver, and then sent to the corresponding connected key managers [64]. The key manager manages keys produced by the transceivers, making them available to cryptographic applications [68, 71]. A limited-range optical switch enables time-division multiplexing (TDM) of QCH, time-sharing devices, and node bypass [72] by permitting the connecting of QCH between transmitters and receivers. Wavelength-division multiplexing (WDM) and TDM are two multiplexing techniques used to combine and divide numerous channels, such as quantum and classical. An M-port QKD router can be built using multiple wavelength-division multiplexers [73]. The secure infrastructure's efficient security measures ensure the reliable operation of QKD nodes.

QKD link As shown in Fig. 8 purpose of the QKD link is to link up two transmitters and receivers, each of which typically has a QCH for transmitting quantum states and a CCH for synchronisation and key distillation [64]. The QKD link can be implemented as a free space link or over an optical fibre link.

QKD controller From Fig. 8 it quickly depicted how a QKDN controller performs typically as a centralised server in charge of coordinating all QKD nodes' operations. Its responsibilities include calibrating, decalibrating, and activating QKD nodes. It also manages routing control, including failure recovery rerouting and secret-key relaying. The QKDN controller also oversees Quality of Service (QoS) control, which includes end-to-end QoS assurance and QoS-differentiated customisation [74].

QKD manager The QKDN manager shown in Fig. 8 functions as a centralised server in charge of administering and keeping track of the whole QKDN, which includes all QKD nodes, QKD links, and key management links. Along with that, it oversees the QKDN controller. Its responsibilities include managing the security, performance, and accounting of the QKDN and faults and configurations. The main areas where the QKD QKDN manager and QKDN controller diverge are their emphasis on standard network management tasks and their

ability to give directives to the QKDN controller in response to received secret-key requests. Nevertheless, a separate QKDN manager cannot adapt to various network conditions and requirements because it does not provide unique control policies and functionalities directly.

QKD application layer As shown in Fig. 8, the cryptographic application at the top layer represents the users with unique security needs. These users may submit a key request describing the required key rate, size, and update period. To obtain the secret keys, a cryptographic application must often be close to a QKD node. A traditional channel that safely transfers encrypted data over the apps is called an "application link".

4.3 QKD network interface and protocol

The general architecture of QKDN is depicted in Fig. 8 along with several interfaces (such as application, control and management, and infrastructure) that connect the various layers. In this section, we'll go into more detail about the QKDN's interfaces and look at a few popular protocols that support them. It's important to note that the paper does not address the internal interfaces unique to each QKDN element or device, albeit some can be found in [213]. Given the variety of QKDN protocols, it should be acknowledged that they might not always concur with those covered in the following sections.

Management Interface Protocol The QKDN manager interacts with cryptographic applications and gathers security requests through the management interface. This can be accomplished using the SNMP [75], which allows data to be gathered from QKD nodes and cryptographic applications. Using SNMP makes it easier to perform activities like getting device information, keeping an eye on resources, and getting secret key information. In addition, the common object request broker architecture (CORBA) [75], particularly in multi-vendor or multi-domain systems, guarantees interoperability among various QKDN components and devices.

Control Interface Protocol The control interface in Fig. 8 represents communication between the controller and nodes in the infrastructure layer. This interface enables the implementation of different control functions, including control, QoS control, and routing control, by facilitating the exchange of control and configuration messages between the QKDN controller and the QKD nodes. As shown in [76–78], the SDN controller can act as the QKDN controller in real-world QKDN. ETSI GS QKD 015 [79, 80] and ITU-T Y.3805 [81] both contain specifications for the QKD control interface offered by SDN. The control interface for an SDN controller can be implemented using a protocol pair consisting of the OpenFlow protocol [82] and the NETCONF protocol [83]. These protocols make transmitting control and configuration request/response messages easier. A QKDN controller with SDN support can control Open Flow-capable QKD nodes [67]. Extensible Markup Language (XML)-based NETCONF protocol enables transaction-based installation, modification, and deletion of QKD node settings.

Application Interface Protocol The connection between the infrastructure and application layers in a QKDN is represented by the application interface in Fig. 8. It makes it possible for the local cryptographic applications and the key manager in a QKD node to communicate. This interface transfers Secret keys from the local key management to the cryptographic programs. ETSI GS QKD 004 [79] contains the requirements for the application interface. The application interface can use the Representational State Transfer (REST) API for secret-key

delivery. To send secret keys to cryptographic apps, this API can use the HTTPS secure version of the HyperText Transfer Protocol and the JSON data format. The REST API is renowned for its ease of use, portability, and widespread use across various application disciplines. ETSI GS QKD 014 [84] contains a complete REST API specification for key distribution in a QKDN.

5 On the road to the QKD: development

QKD can provide unprecedented security for sending sensitive financial data in the banking and finance, healthcare, space technology, and government sectors, protecting against potential cyber threats and guaranteeing the integrity of transactions. QKD has the potential to revolutionise secure medical data Significant improvements have been made in several fields discussed in this section.

5.1 Application area

Various QKD-protected applications have emerged in various sectors due to integrating QKDNs with existing Information and Communications Technology (ICT) systems. In addition to establishing QKD linkages in athletic events like the 2010 FIFA World Cup [85], these applications also include securing crucial connections for financial institutions and governmental organisations. Typical QKDN application areas are shown in Fig. 9 and described below:

1. *Research and development:* The fact that QKD can offer information security without restrictions has initiated significant attention. The primary objective is to create QKD

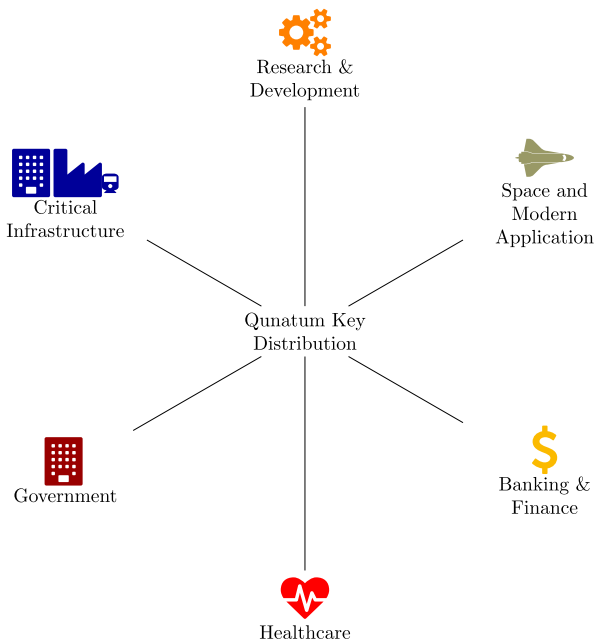


Fig. 9 Application area of quantum key distribution

systems that can support research and development applications, act as educational platforms, and enable quick prototyping of novel QKD protocols. A QKD set is presented in [86] using National Instruments (NI) cards and open-source LabView code. The plug-and-play system was tested using this modular design, and the BB84 was successfully implemented. The goal was to research and establish a high level of robustness even outside of a lab setting.

2. *Space and modern applications:* The secure communication provided by QKD holds potential for a wide range of applications, including space and modern applications like (mobile networks). For space-based communications, QKD can provide secure access to satellites, communication between ground stations [19, 87], and satellite-to-satellite facilitation [88], among other services. Additionally, transcontinental video conferencing was successfully demonstrated using satellite-based QKDNs [89] in conjunction with fibre-based QKDNs. The projects focusing on space-based quantum communications have also been announced in [88]. The Tokyo QKDN [69] has also used QKD to protect cellphones in a multiuser mobile network. This demonstrates QKD's adaptability and expanding use across various communication platforms, including satellite- and terrestrial-based systems.
3. *Banking and finance:* Banking and finance sectors handle highly sensitive and valuable information, such as client information, transactions, and proprietary information [90, 91]. The QKD system provides the highest level of security and future-proofing for protecting this data. The first bank transfer took place in 2004 between an Austrian bank and Vienna City Hall, where a QKD system made it possible to distribute secret keys upon request [90]. The usual authentication procedures used by online banking systems are susceptible to attacks like phishing, QKD can be used to strengthen them.
4. *Healthcare:* In healthcare organisations, highly dependable networks are necessary to transfer sensitive information, such as patient records containing personal information like names, addresses, dates of birth, social security numbers, and clinical data. However, these broadcasts are vulnerable to cyber-attacks without sufficient security. Such assaults can result in significant financial and credit losses for healthcare organisations while posing hazards to individuals, including compromise of their personal information and health. Healthcare organisations can use QKD to protect their data in the coming era of quantum computing. A storage system that provides extraordinary storage longevity was introduced in [92] to ensure the long-term safety of sensitive human genomes and health data. Furthermore, a study [93] investigated the use of QKD in a cloud setting to provide access security and storage for personal health records.
5. *Government:* The most stringent data security regulations are in governmental organisations, particularly when protecting long-lasting official secrets. QKD provides a solution for these organisations that will guarantee long-term data protection and uphold data sovereignty. Government organisations frequently use specialised security systems, including Virtual Private Networks (VPNs), to ensure their communication systems operate with high confidentiality, integrity, and authenticity. The Swiss government successfully deployed QKD in 2007 to protect a special line for tabulating national election votes [94]. A voting system based on QKD was proposed in [95] and offered a defence against man-in-the-middle assaults. Finally, several studies have investigated QKD's use to improve VPN security [96, 97].
6. *Critical Infrastructure:* A critical national infrastructure includes a variety of industries that offer essential services to society, including telecommunications, electricity, and transportation. These infrastructures are, nevertheless, vulnerable to dangers like fraudulent data manipulation and service interruptions. Such dangers can potentially harm the

economy and interfere with corporate and governmental operations. To address these issues, QKD can provide forward secrecy and long-term security for vital infrastructures. Aeronautical telecommunication networks can benefit from using QKD to increase security. Additionally, [98] has discussed the application for multi-source data security protection.

5.2 QKD challenges

QKD is needed to secure the QI Communication where both parties are quantum devices. The security of the encryption keys used by parties to communicate with one another is a persistent challenge. Following are some typical challenges encountered by researchers throughout the quantum key exchange process:

1. Qubit rate: To overcome the challenge of a finite quantum key generation rate, a lot of effort has been given by the readers. The numerical asymptotic Quantum KR calculation approach from Ref. [99] has been developed in Ref. [100] to account for the KR. The finite key analysis is conducted using Renner's paradigm [101].
2. Detection of adversary: After the key generation at the finite rate, the parties have to ensure the presence of the adversary for the confirmation of the secure key exchange. Zhang et al. [102] carried out a security proof without the photon-number cutoff assumption and with described efficiency mismatch. Their approach further demonstrates that, without efficiency mismatch in the detector model, the KR rises if the loss resulting from the detection inefficiency is taken into account as being independent of the adversary, as opposed to the perspective where, for the security proof, this loss is linked to the opponent's action.
3. Distance: Key Distribution Distance: Distance is a major factor in Key distribution; it can affect the exponential loss of photons in optical fibres. In some practical implementations, it typically restricts secure transmission to around 100-200 kilometres [36, 89]. Widespread implementation of QKD communication is severely hampered by distance constraints, particularly for long-distance communication networks. It may also lead to errors in the system due to an increase in the distance. Developing new technologies like quantum repeaters or satellite-based [19] QKD systems can overcome this problem and extend the range.
4. Error correction due to noise: A QKD is more prone to error, which also affects key generation time due to the optical misalignment, the noise inside the quantum detectors, any physical disturbance of the QCH, or eavesdropping; therefore, an error key reconciliation approach is needed to eliminate the errors. Mehic et al. analysis of the key reconciliation procedures [103] which emphasised communication and processing effectiveness.
5. Implementation and key management: The practical implementation of QKD is affected by the requirement for complex and expensive quantum devices, such as single-photon sources and detectors, which are currently limited by inefficiency, noise, and operational complexity. Storage and management of quantum bits for the key distribution process are challenging. The qubit's energy deteriorates with time, and it can cause errors in the QKD process. The raw qubits require proper storage and management; otherwise, they become vulnerable to eavesdropping. Hence, implementation and key management require advanced hardware support to amplify qubits.
6. Quantum Repeaters: During the time, qubits lose information embedded in it. Hence, repeaters must retain the energy stored in qubits to extend QKD over long distances. However, development in the field of retaining information from qubits after the decay

in energy is still challenging. Without effective quantum repeaters, QKD's scalability is restricted to its use in large-scale networks.

7. Sequential security proof: The sequential framework [104] in which device-independent QKD (DIQKD) operates requires Alice and Bob to enter their inputs into their respective boxes and receive their outputs one at a time. For the sequential security proofs in particular, it is necessary to assume that the $(i-1)^{th}$ output is observed before the box gets the i^{th} input. Security proofs that are applied sequentially typically provide better parameters than proofs that are applied parallelly. Still, there is uncertainty about how to apply sequential proof techniques to leakage scenarios without making some very odd assumptions.
8. Integration of quantum work with classical communication techniques: Until quantum information is in its early development phases, it is very challenging to integrate quantum work with the classical communication network.

5.3 Vulnerability in QKD

A QKD system's security is independent of the difficulty of the underlying mathematical calculations. But many attacks that take advantage of the technical and engineering flaws in the system's constituent parts can be made against QKD systems. Simply by neglecting the laws of quantum physics, there may be numerous vulnerabilities in QKD that could offer a target for eavesdropping attacks. Though QKD provides robust security, it faces critical vulnerabilities in practical implementation, such as quantum repeaters, key exchange is limited by distance. If challenges like key storage and management are not handled properly, it will be vulnerable to attacks.

Vybornyi et al. [105] have demonstrated vulnerabilities in QKD, based on the effect of backflash light [106]. Since single photon avalanche diodes (SPADs) [105] are the commercially available single-photon counting solution used in QKD applications. The photon emission that results from the avalanche of charge carriers during a photon detection can be used by an Eve to obtain the information without introducing errors inside the key. They offer a method for calculating the backflash emission and various ways to minimize its effects.

Some more vulnerabilities in QKD are due to modulation leakage in the system [107], coherent states of light [108] and experimental vulnerability [109], etc. Therefore, any error in the experimental method or quantum bit encoding may make the QKD vulnerable to information leakage. Based on the attack vulnerabilities (like PNS, IR, decoherence, trojan horse and misalignment), some practically tested protocols are BB84 [9], E91 [11], BBM92 [45], B92 [27], SSP [28], Ping-Pong [39], DPS [40], COW [41], SARG04 [29], Decoy State and [37]. It is important to note that when creating the quantum key, one must consider all possible scenarios that could lead to QKD vulnerability.

5.4 Design trade-off for QKD

Design trade-offs in quantum key exchange algorithms involve security, computational efficiency, KR, and protocol complexity. These trade-offs emphasise the importance of carefully weighing and evaluating various key exchange algorithms based on the application's requirements, including security, performance, compatibility, and future-proofing against developing risks. Here are a few typical major quantum key exchange design trade-offs as shown in Fig. 10.

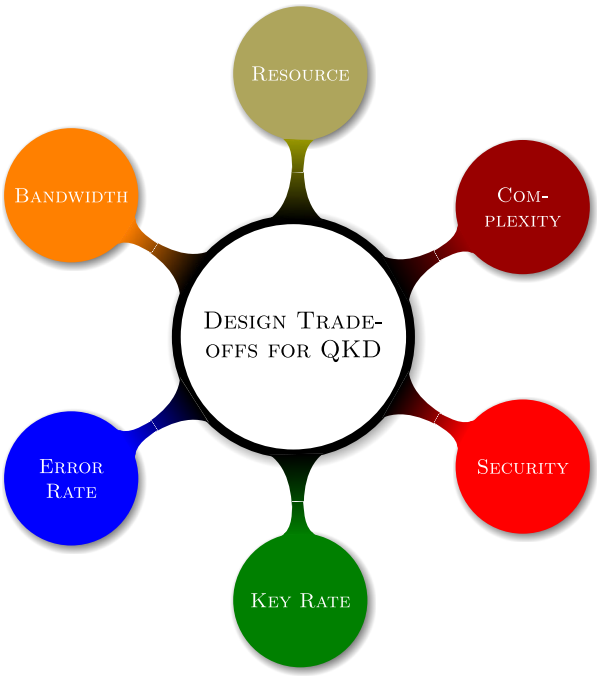


Fig. 10 Design trade-offs for QKD

- *Security*: The Security of the QKD protocol depends on the strength of the key. QKD algorithms vary in their security strength. BB84 [9] protocol is based on a single-photon and is less secure than E91 [11], which is an entangled-based protocol. The security strength of these protocols is measured by the size of the key and the computational effort required by an adversary to break the key. Additionally, the quantum secret key must be available anywhere at any time for diverse ICT applications across many areas [110].
- *Complexity*: The key distribution system in a QN can be complex to set up and maintain. The computational complexity of a key exchange algorithm influences the time required to produce and exchange keys. Computing power and time are needed for some methods to accomplish the key exchange. This may impact the responsiveness of the system. Additionally, an algorithm's implementation and susceptibility to attacks might be influenced by its complexity. Incorrect implementation of more complicated algorithms may result in additional sources of vulnerability. The single-photon-based protocol like BB84 [9] is more prone to IR attacks, but an Entanglement-based protocol like E91 [11] is safe against IR attacks. Entanglement-based QKD protocols are more complex than single-photon QKD protocols.
- *Key Rate*: For increased security, encryption keys generated by QKD can be paired with the one-time-pad encryption technique or utilised in a symmetric cypher scheme. The KR obtained by the underlying QKD mechanism in a typical application scenario is crucial in both situations. In symmetric cyphers, where the key must be as long as the message, higher secure KRs enable more frequent encryption key updates and a corresponding rise in one-time pad transmission bandwidth [111]. George et al. [112] addressed the KR issue in QKD. Using the Renner security analysis framework [113], they employed

a general numerical method to determine the asymptotic KR of device-dependent QKD protocols in finite-dimensional Hilbert spaces in the finite key regime.

- *Error Rate*: At a specific rate (the KR), quantum communication channels can communicate secret keys. But noise and other factors might produce problems on these channels. To solve this problem, the QBER is calculated by giving up a portion of the sorted keys to confirm that it is lower than a predetermined threshold value. There are several methods for QBER estimation. For instant, in BB84 protocol [9], Alice and Bob can first fix the errors to precisely define the QBER without losing some of the data. The QKD procedure will be stopped and resumed from the first step if the estimated QBER is higher than the threshold value since there is a chance that someone could be listening in on the QCH and contaminating the quantum states [114]. In the experimental execution, Abushgra et al. [115] have experimentally demonstrated that the length of plaintext dramatically affects QBER. For the demonstration, they have used SARG04 protocol [29].
- *Resource*: Resource limitations, like compute power, memory, and storage, can have a substantial impact on how well quantum key exchange systems perform [116]. These resource limitations may provide difficulties and perhaps jeopardise the system's effectiveness and efficiency. The system can function at its peak level thanks to effective resource management, which boosts critical generating rates, transmission ranges, and overall security. Additionally, due to technological immaturity, specifically with regard to essential quantum memory, current research focuses on quantum-repeater-based QKD [116]. Because non-ideal single-photon sources and detectors have intrinsic weaknesses that can't be ignored in real-world situations, trusted-relay-based QKD security is still an issue.
- *Bandwidth*: The performance of the QKD in terms of KR differed with bandwidth as in Ref. [117]. In a high-speed CV-QKD system, the noise in the channel depends on bandwidth which affects KR. Tang et al. [117] used a GHz bandwidth balanced homodyne detector (BHD) to provide a better secure KR under the various clock rate.

5.5 Security analysis methods

5.5.1 Conditional min-entropy security measure over the weak laser light

The QKD protocol must be secure against different types of attacks like (PNS attacks, IR attacks). Table 2 shows PNS and IR attacks on different QKD protocols. Huang et al. [118] have shown that a man-in-middle attack or IR is possible on BB84 protocol and some more analogous QKD protocols. To detect any attack during the key exchange they used digital certificates [118].

Inoue et al. [119] have shown that the BB84 protocol, which takes advantage of weak laser light, is resistant to PNS attacks. The transmission distance is restricted by PNS attacks, which include putting in place a lossless transmission line and blocking the pulses from which more photons cannot be captured. They used coherent pulse train differential-phase-shift (DPS) to stop the prior attack and overcome the distance restriction.

In QKD, the fundamental theoretical obstacle to demonstrating security is to provide a lower bound for a value known as the smooth conditional min-entropy [120] given by $\mathcal{H}^{a}_{min}(A_d \mid E)$. Alice's information obtained by the adversary (Eve) during the communication [121] and $a \in \{0, 1\}$ is the security parameter. A robust quantum proof extractor [122] is employed in the PA stage of the protocol after a sufficiently enough lower bound on the

smooth conditional min-entropy has been obtained. This PA step-up protocol ensures that the adversary does not know the final key generated from Alice.

5.5.2 Parallel repetition theorem for device independent Leakage

Jain et al. [104] have proposed a theorem for the quantum partition bound known as efficiency bound for the product distributions for the complexity of interactive quantum communication facilitated by entanglement. It is related to the parallel repetition theorem used in non-local games where the game with l number of players is defined by $\mathcal{V}$ and probability distribution is ρ. The predicate $\mathcal{V}$ is the communication complexity, computed on $(\mathcal{B}^1 \times \cdots \times \mathcal{B}^l) \times (\mathcal{Y}^1 \times \cdots \times \mathcal{Y}^l)$ where $l \leq 2$ players having inputs $y^1 \cdots y^l \in \mathcal{Y}^1 \times \cdots \times \mathcal{Y}^l$. The required out are $o^1 \cdots o^l$ in $\mathcal{B}^1 \times \cdots \times \mathcal{B}^l$ so that the predicate $\mathcal{V}(o^1 \cdots o^l, y^1 \cdots y^l)$ is satisfied without communicating.

To provide security against leakage, each honest party device is modelled as a black box. Every independent device provides its input and receives output after playing a non-local game based on the direct product theorem [104]. For every honest party in DIQKD, the boxes are provided by an eavesdropper (Eve). The measurement criteria for each black box may vary from player to player. For the basic assumption, boxes of any parties in DIQKD will not communicate with others. Discarding the assumption if the box is allowed to communicate through each other, they will start sending the input data to Eve even if the parties are sharing entangled qubit pairs. Hence the proposed protocol (direct product theorem) gives proof of the leakage in DIQKD using the parallel repetition theorem.

5.5.3 Global hash function for increasing qubit error rate

Due to the impact of the eavesdropper (Eve) on the quantum communication network the qubit error rate increase in the channel. Hence, the security analysis after the post-processing of the QKD includes a variety of factors, including error estimates, information correction, data checks, and privacy amplification. Zang et al. [123] have performed a security analysis of the BB84 QKD protocol. They secure a QBER of 0.0 using a sampling ratio of 0.2 and error correction using the Cascade scheme. In order to correct the shifted binary bit, Cascade has run four rounds, among 77 leaked binary bits, 10 error binary bits were detected and corrected. They also used a global hash function for the privacy module [123].

5.5.4 Gottesman-Lo-Lïutkenhaus-Preskill (GLLP) method for qubit error rate

Chang et al.[124] proposed methods for security analysis in order to achieve accuracy. They modified the error rate in the QN given by the following equation:

$$em_{ij} = \frac{1 - M(1 - 2e_{exp})}{2} \tag{14}$$

$$M = \frac{1}{\sqrt{1 + sin^2\theta_b}} \tag{15}$$

Where em_{ij} is the modified error rate, also known as fictitious bit-error rate, applied when Alice and Bob measure in basis i and j, respectively.

$$e_{exp} = \frac{1 - N_{ij}(1 - Q)}{2} \tag{16}$$

Equtaion (16) shows the experimental error rate where N_{ij} is theoretical probability [124], M is system's completeness and Q is QBER in the best-case scenario.

A vacuum+weak decoy-state protocol [125] is also used to demonstrate their analysis. Based on the analysis in Ref. [125] they have selected two error values λ: for the top bound the value is 0.127 and for the lower bound modulation error $\lambda \leq 0.062$. While the maximum distance is 20 km, the security analysis based on their theory with a commercial system λ= 0.127 may be made secure over 120 km. Their model is similar to the loss-tolerant protocol.

For the non-randomness phase in QKD, they consider infinite decoy-state method [126] to obtain asymptotic KR:

$$R = q\{-f(E_\mu)Q_\mu h(E_\mu) + Q_1(1 - h(e_1^U))\} \tag{17}$$

where q = 1/2 and the modified phase error rate of GLLP analysis can be used to overcome the capacity limit of the secret key. The GLLP framework [124] provides two methods to overcome the capacity of the limit of the key: one is the error tolerance method, and the second is the lower bound on the secret key rate. During the transmission via the quantum channel, the error tolerance method estimates the amount of information leaked to the eavesdropper. The communicating party discarded the error bit or terminated the transmission based on the leaked information. On the other hand, the lower bound determines the length of the final secret key.

There is still a lot of work to be done, according to numerous studies to assure the security of the quantum key exchange. Finally, the security of quantum cryptography is based on the fundamental laws (non-cloning theorem and uncertainty) of physics.

6 Future research directions

This survey conducts a study on QKD protocols along with QKDNs. By demonstrating the enormous potential of QKD and QKDNs to offer reliable security for a range of applications and open up a new vista. This section provides a variety of open topics related to QKD and other related areas, which serve as potential areas of future research. There are numerous open challenges which are visually summarized in Fig. 11.

6.1 Key distribution

The security of any communication system relay on the key and key exchange process. Much work has been proposed on the QKD based on different principles of quantum mechanics. Section 3 provides various protocols in brief. The QKD faces primary challenges like key exchange while there is noise presence in the network while maintaining KR. Other issues regarding the key distribution are mentioned in Section 5. To calculate the KR, a software base solution has been proposed in [127], it provides safety against the Trojan-horse attack in the BB84 protocol. Another strategy for increasing the secret KR and removing significant obstacles is presented in [128]. The method generated secret keys at a rate of 64 Mbps over a distance of 10.0 km and at a rate of 3.0 Mbps over a distance of 102.4 km with real-time key distillation. It was accomplished by utilising the detector's performance and coupling it to fast acquisition and real-time key distillation electronics.

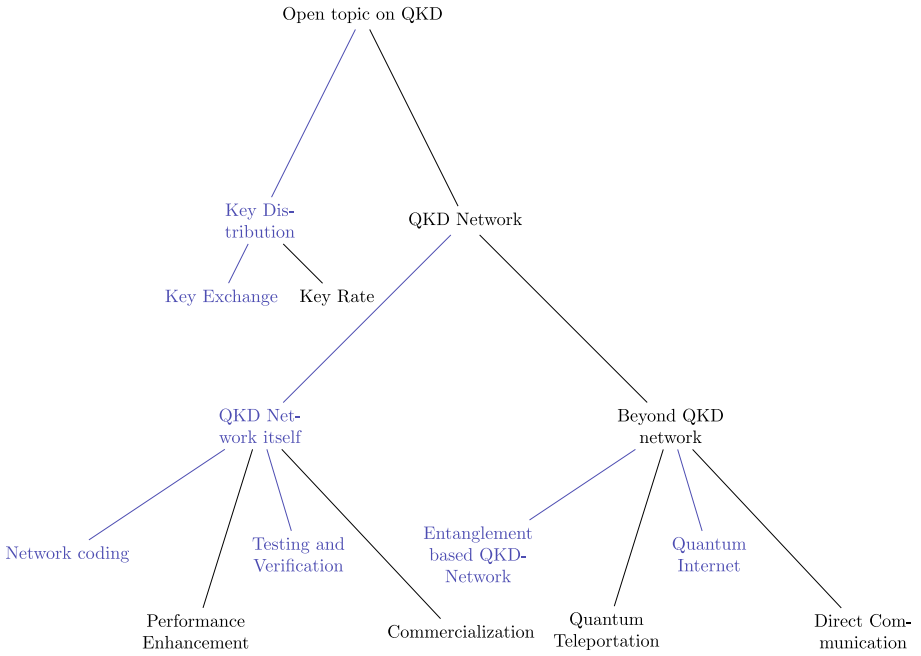


Fig. 11 Open topics in QKD for future research

6.2 QKD network itself

A QN provides communication between two quantum nodes by enabling secure communication. It facilitates the exchange of information using QCH and public channels. Several issues, such as network coding, performance enhancement, testing and verification, and eventual commercialization of the technology, currently hinder the development of QKDNs.

In classical networks, network coding has been extensively studied [129], but to use it in QKDNs, a number of unique problems need to be solved. The use of network coding [299], which facilitates the effective multicast communication of secret keys from numerous transmitters to multiple receivers, can reduce the reliance on trustworthy relays in QKDNs. This development might make it easier to implement useful public multi-user QKD systems [12]. Despite the potential of QN coding, a novel paradigm first proposed in [130], the majority of studies have mostly concentrated on its theoretical features [131].

Certain developments are required to guarantee enhanced QKDN performance, enable forward secrecy, and provide long-term safety for a growing user population within the future QI. It will be necessary to create new QKD devices and protocols in order to expand the range and secret KR of QKDNs. It is possible to increase adaptability, compatibility, and agility in particular by implementing an advanced QKDN that permits device reconfiguration to accept different QKD protocols [13]. In order to enable the extensive deployment of QKDNs, it is also necessary to integrate QKD with current optical networks [132]. Further research and development are necessary since the development of global QKDNs depends on the discovery of satellite-constellation-based QKDNs.

A number of options were put out by Walenta et al. [133] to guarantee that QKDN devices adhered to recognised security certification criteria. Measurement techniques for various

characteristics of individual QKD system components were described in ETSI GS QKD 011 [134]. However, a key challenge is assuring the authenticity, impartiality, and dependability of testing and verification for QKDNs. As a result, platforms, tools, and testing and verification protocols that are widely used and standardised are required for various QKDNs. An impartial evaluation centre should ideally be developed to test QKDNs under various conditions and verify the functionality stated by network operators.

The mass commercialization of QKDNs faces a substantial barrier due to the security implementation since attackers could use network flaws to impair its functionality [135]. To overcome implementation weaknesses, it is crucial to develop and update advanced countermeasures continuously, ensuring the deployment of secure QKDNs in commercial and public settings.

6.3 Beyond QKD

Extensive research has been conducted on the practical implementation of QKD, including existing QKDNs. However, future quantum applications require further cutting-edge research as shown in Fig. 11. The practical challenges which need to be considered most are entanglement-based QKDN, Quantum teleportation, QI and direct communication.

The effectiveness and security of entanglement-based QKDNs are continually being improved. These networks rely on quantum entanglement's delicate and complex characteristics to securely transfer information. Future research intends to create cutting-edge methods that can increase the scope and scalability of these networks while minimising the number of real-world challenges. For a fully entanglement-based QKDN [92, 136] to achieve commercial maturity and provide practical services, sustained long-term efforts are necessary. It is necessary to improve the development of key hardware elements, including quantum processors and quantum memory, to enable the smooth operation of completely entanglement-based QKDNs.

A fascinating phenomenon that enables the transmission of quantum states between particles, known as quantum teleportation [137], has captured the attention of scientists worldwide. Future work will improve teleportation protocols' fidelity and investigate their applications in quantum computing and cryptography [138]. Quantum secure direct communication (QSDC) [139], which enables secure transmission between two parties, is another promising area. The goal is to create security protocols to fend off intrusions and guarantee privacy. An additional important research goal is the creation of a QI [140]. Long-distance quantum information transmission is made secure thanks to this cutting-edge communication infrastructure. Researchers are looking into methods for building dependable QN and connecting quantum devices. To overcome the restrictions of quantum decoherence and signal loss, quantum repeaters and memories must be developed.

7 Discussion

QKD and QKDN are advanced promising technologies for increasing the security and performance of communication systems. However, they also encounter several practical difficulties that restrict their applicability and scalability. As demonstrated in Sections 3, each protocol description includes some technical information, particularly when the protocol has a distinctive architecture like the COW protocol [41]. Incorporating the decoy states during pulse transmission is essential to the COW protocol. Using decoy states requires more time during the submission or reconciliation steps but provides more security against PNS attacks. It has

become more difficult to cope with secret KR and short distances due to loss and noise in the transmission channel. Single photons or weak coherent pulses, which are easily attenuated or distorted by the environment, are needed by QKD to transport the quantum information. Many methods have been put forth to address this issue, including decoy-state QKD [37] and measurement-device-independent QKD like twin-field QKD [47].

The methods used to assess each QKD protocol's resilience to attack challenges also differ among the QKD protocols. QKD protocols are frequently evaluated the efficiency and security based on the implementation challenges in the QKDN (internal channel noise and attacks). One of these factors, the simplicity factor was used to verify the runtime execution at a constrained number of qubits for the earlier QKD protocols. On the other hand, the network design and existing infrastructure preclude QKD implementation. The present internet protocols and standards, which rely on traditional bits and encryption techniques, are incompatible with QKD. The network needs include quantum repeaters, trustworthy nodes, hybrid encryption methods, and software- and hardware-defined networking in order to integrate QKD in QKDN.

QKD and QKDN are based on the assumption that the devices are accurately defined and that the eavesdropper is bound by the principles of quantum mechanics. However, due to faults in the devices or new threats, these hypotheses might not be accurate in practice. A number of techniques, including device-independent QKD ([11, 30, 37]), composable security proofs, and finite KR analysis ([127, 128]), have been suggested to guarantee the practical security of QKD.

Application scenarios like blockchain [141], and market demand for QKD and QKDN are still limited. QKD is currently a niche technology that is not yet commercialized. The key challenges include a lack of knowledge of QKD goods and services as well as a lack of standardization, education, legislation, and certification. Some attempts have been undertaken, which are covered in the aforementioned areas of this study, to raise the market demand and application scenarios for QKD and QKDN. Communication system performance and security may be greatly enhanced using QKD and QKDN. This survey offers readers the required guidelines for doing research for safe quantum communication.

8 Conclusion

We have surveyed the basic features of QKD and QKDN, both of which hold great promise for boosting the efficiency and security of communication systems. A few of the real-world obstacles that prevent them from being scaled up or used effectively have also been emphasized, including secret KR, distance, cost, compatibility, and security. When compared to traditional key distribution, QKD offers substantial security benefits. An eavesdropper cannot replicate the quantum bits utilised in the key exchange as Bell's inequality and CHSH defines the correlation $S = \pm 2\sqrt{2}$ for secure key exchange. As a key generated by a QKD is unconditionally safe, adversaries cannot benefit from advances in computing power. QKD gives the sender and receiver a way to detect eavesdroppers during crucial exchanges and quantum physics serves as the theoretical foundation for QKD security. The security premise of QKD holds as long as no new laws of physics have been discovered by eavesdroppers. This is in contrast to conventional key distribution techniques, which encrypt the key using computational security.

This survey also discussed some of the current initiatives in the field of QKD and QKDNs which includes brand-new protocols, QKDN elements, QKDN protocols, and standards. It

also highlighted the challenges, and vulnerabilities in designing and implantation of the QKD protocols. There are numerous ways to design a QKD system (QKD and QKDN) since quantum states that are arbitrarily chosen from any two or more non-orthogonal quantum bases can be used to encode information. New forms of QKD offer ways to get around the security restrictions of the present technology and are the subject of current research. Research efforts aimed at enhancing the quality of emitters, detectors, and fibre will continue to be made as QKD's popularity grows and commercial QKD systems become more widespread. This will allow QKD to operate over longer distances and at a higher KR. This paper offers diverse research directions for those who are interested in learning more about these intriguing topics which can serve as a helpful overview and a source of insightful information

Author Contributions Mandeep Kumar has drafted the manuscript and generated all the tables. Bhaskar Mondal has generated all the figures. Both authors have worked on literature surveys, simulations, and proofreading.

Funding The authors hereby declare that there was no full or partial financial support from any organization.

Availability of data and materials No data was generated during the research to disclose. No Code is available to share.

Declarations

Ethical Approval No human and/ or animal studies have been presented in the manuscript. Hence, no ethical approval is needed.

Competing interests The authors do not have any financial or personal conflict of interest to disclose related to this manuscript.

References

1. Dai W, Peng T, Win MZ (2020) Quantum queuing delay. IEEE J Sel Areas Commun 38(3):605–618
2. Sun S, Huang A (2022) A review of security evaluation of practical quantum key distribution system. Entropy 24(2)
3. Shor PW (1994) Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. IEEE, pp 124–134
4. Kumar M, Mondal B (2024) Study on implementation of shor's factorization algorithm on quantum computer. SN Comp Sci 5(4):413
5. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystems. Commun ACM 21(2):120–126
6. Miller VS (1985) Use of elliptic curves in cryptography. In: Conference on the theory and application of cryptographic techniques. Springer, pp 417–426
7. Yu X, Wang Y, Lu L, Zhao Y, Zhang H, Zhang J (2021) VON embedding in elastic optical networks (EON) integrated with quantum key distribution (QKD). Opt Fiber Technol 63:102486
8. Cao Y, Zhao Y, Colman-Meixner C, Yu X, Zhang J (2017) Key on demand (KoD) for software-defined optical networks secured by quantum key distribution (QKD). Opt Express 25(22):26453–26467
9. Bennett CH, Brassard G (1984) Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE international conference on computers, systems, and signal processing, Bangalore, pp 175–179
10. Bell JS (1964) On the einstein podolsky rosen paradox. Phys Physique Fizika 1(3):195
11. Ekert AK (1991) Quantum cryptography based on bell's theorem. Phys Rev Lett 67:661–663
12. Nguyen HV, Trinh PV, Pham AT, Babar Z, Alanis D, Botsinis P, Chandra D, Ng SX, Hanzo L (2017) Network coding aided cooperative quantum key distribution over free-space optical channels. IEEE Access 5:12301–12317
13. Qin J-Q, Jiang C, Yu Y-L, Wang X-B (2022) Quantum digital signatures with random pairing. Phys Rev Appl 17(4):044047

14. Althamir M, Alabdulhay A, Yasin MM (2023) A systematic literature review on symmetric and asymmetric encryption comparison key size. In: 2023 3rd International Conference on Smart Data Intelligence (ICSMDI). IEEE, pp 110–117
15. Peruzzo G, Sorella SP (2023) Entanglement and maximal violation of the chsh inequality in a system of two spins j: a novel construction and further observations. Phys Lett A 474:128847
16. Tian Y, Zhang Y, Liu S, Wang P, Lu Z, Wang X, Li Y (2023) High-performance long-distance discrete-modulation continuous-variable quantum key distribution. Opt Lett 48(11):2953–2956
17. Liu Y, Zhang W-J, Jiang C, Chen J-P, Zhang C, Pan W-X, Ma D, Dong H, Xiong J-M, Zhang C-J, Li H, Wang R-C, Wu J, Chen T-Y, You L, Wang X-B, Zhang Q, Pan J-W (2023) Experimental twin-field quantum key distribution over 1000 km fiber distance. Phys Rev Lett 130(6):210801
18. Wang Y, Huang Y, Guo C, Jiang M, Kang X, Su H, Qin Y, Ji W, Hu D, Peng X et al (2023) Search for exotic parity-violation interactions with quantum spin amplifiers. Sci Adv 9(1):0353
19. Liao S-K, Cai W-Q, Liu W-Y, Zhang L, Li Y, Ren J-G, Yin J, Shen Q, Cao Y, Li Z-P et al (2017) Satellite-to-ground quantum key distribution. Nature 549(7670):43–47
20. Chen Y-A, Zhang Q, Chen T-Y, Cai W-Q, Liao S-K, Zhang J, Chen K, Yin J, Ren J-G, Chen Z et al (2021) An integrated space-to-ground quantum communication network over 4,600 kilometres. Nature 589(7841):214–219
21. Bugalho L, Coutinho BC, Monteiro FA, Omar Y (2023) Distributing multipartite entanglement over noisy quantum networks. Quantum 7:920
22. Horodecki R, Horodecki P, Horodecki M, Horodecki K (2009) Quantum entanglement. Rev Mod Phys 81(2):865
23. Huang L, Wang X, Chen Z, Sun Y, Yu S, Guo H (2023) Countermeasure for negative impact of a practical source in continuous-variable measurement-device-independent quantum key distribution. Phys Rev Appl 19(1):014023
24. Lee J, Park J, Kim J, Kim M, Nha H (2023) Non-gaussian entanglement criteria for atomic homodyne detection. Phys Rev A 107(2):022423
25. Vazirani U, Vidick T (2019) Fully device independent quantum key distribution. Commun ACM 62(4):133–133
26. Slater JA, Branciard C, Brunner N, Tittel W (2014) Device-dependent and device-independent quantum key distribution without a shared reference frame. New J Phys 16(4):043002
27. Bennett CH (1992) Quantum cryptography using any two nonorthogonal states. Phys Rev Lett 68(0):3121–3124
28. Enzer DG, Hadley PG, Hughes RJ, Peterson CG, Kwiat PG (2002) Entangled-photon six-state quantum cryptography. New J Phys 4(1):45
29. Scarani V, Acin A, Ribordy G, Gisin N (2004) Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys Rev Lett 92(5):057901
30. Serna EH (2013) Quantum key distribution from a random seed. arXiv preprint arXiv:1311.1582
31. Sasaki T, Yamamoto Y, Koashi M (2014) Practical quantum key distribution protocol without monitoring signal disturbance. Nature 509(7501):475–478
32. Alshowkan M, Elleithy KM (2017) Deterministic and efficient quantum key distribution using entanglement parity bits and ancillary qubits. IEEE Access 5:25565–25575
33. Soh DB, Brif C, Coles PJ, Lütkenhaus N, Camacho RM, Urayama J, Sarovar M (2015) Self-referenced continuous-variable quantum key distribution protocol. Phys Rev X 5(4):041010
34. Ghalaii M, Ottaviani C, Kumar R, Pirandola S, Razavi M (2020) Discrete-modulation continuous-variable quantum key distribution enhanced by quantum scissors. IEEE J Sel Areas Commun 38(3):506–516
35. Guo Y, Peng Q, Liao Q, Wang Y (2021) Trans-media continuous-variable quantum key distribution via untrusted entanglement source. IEEE Photonics J 13(2):1–12
36. Jiang C, Yu Z-W, Hu X-L, Wang X-B (2023) Side-channel-secure quantum key distribution with imperfect vacuum sources. Phys Rev Appl 19:064003
37. Lo H-K, Ma X, Chen K (2005) Decoy state quantum key distribution. Phys Rev Lett 94(4):230504
38. Grosshans F, Grangier P (2002) Continuous variable quantum cryptography using coherent states. Phys Rev Lett 88(4):057902
39. Boström K, Felbinger T (2002) Deterministic secure direct communication using entanglement. Phys Rev Lett 89(4):187902
40. Inoue K, Waks E, Yamamoto Y (2002) Differential phase shift quantum key distribution. Phys Rev Lett 89(3):037902
41. Stucki D, Brunner N, Gisin N, Scarani V, Zbinden H (2005) Fast and simple one-way quantum key distribution. Appl Phys Lett 87(19):194108

42. Zhong T, Zhou H, Horansky RD, Lee C, Verma VB, Lita AE, Restelli A, Bienfang JC, Mirin RP, Gerrits T et al (2015) Photon-efficient quantum key distribution using time-energy entanglement with high-dimensional encoding. New J Phys 17(2):022002
43. Trushechkin AS, Tregubov PA, Kiktenko EO, Kurochkin YV, Fedorov AK (2018) Quantum-key-distribution protocol with pseudorandom bases. Phys Rev A 97(15):012311
44. Zhou Y, Yin Z-Q, Wang R-Q, Wang S, Chen W, Guo G-C, Han Z-F (2022) Twin-field quantum key distribution with partial phase postselection. Phys Rev Appl 18:054026
45. Bennett CH, Brassard G, Mermin ND (1992) Quantum cryptography without bell's theorem. Phys Rev Lett 68(5):557
46. Liu H, Wang J, Ma H, Sun S (2019) Reference-frame-independent quantum key distribution using fewer states. Phys Rev Appl 12:034039
47. Lucamarini M, Yuan ZL, Dynes JF, Shields AJ (2018) Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. Nature 557(7705):400–403
48. Cui Z-X, Zhong W, Zhou L, Sheng Y-B (2019) Measurement-device-independent quantum key distribution with hyper-encoding. Science China Physics, Mechanics & Astronomy. 62(11):110311
49. Clauser JF, Horne MA, Shimony A, Holt RA (1969) Proposed experiment to test local hidden-variable theories. Phys Rev Lett 23:880–884
50. Scherer A, Sanders BC, Tittel W (2011) Long-distance practical quantum key distribution by entanglement swapping. Opt Express 19(4):3004–3018
51. Bennett CH, Brassard G, Crepeau C, Maurer UM (1995) Generalized privacy amplification. IEEE Trans Inf Theory 41(6):1915–1923
52. Lo H-K (2001) Proof of unconditional security of six-state quantum key distribution scheme. arXiv preprint quant-ph/0102138
53. Kwiat PG, Waks E, White AG, Appelbaum I, Eberhard PH (1999) Ultrabright source of polarization-entangled photons. Phys Rev A (Coll Park) 60(2):773
54. Kanyang R, Fang C, Yang Q, Shao Y, Han G, Liu Y, Hao Y (2022) Electro-optical modulation in high q metasurface enhanced with liquid crystal integration. Nanomaterials 12(18):3179
55. Mittelstädt A, Schliwa A, Klenovskỳ P (2022) Modeling electronic and optical properties of III-V quantum dots-selected recent developments. Light Sci Appl 11(1):1–14
56. Levy U, Silberberg Y, Davidson N (2019) Mathematics of vectorial gaussian beams. Adv Opt Photonics 11(4):828–891
57. Usenko V, Lasota M, Filip R (2016) Continuous-and discrete-variable quantum key distribution with nonclassical light over noisy channels. In: 2016 39th International conference on Telecommunications and Signal Processing (TSP). IEEE, pp 753–756
58. Poxleitner M, Hinrichsen H (2021) Gaussian continuous-variable isotropic state. Phys Rev A (Coll Park) 104(3):032423
59. Lounis B, Moerner WE (2000) Single photons on demand from a single molecule at room temperature. Nature 407(6803):491–493
60. Acin A, Gisin N, Scarani V (2004) Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks. Phys Rev A (Coll Park) 69(1):012309
61. Stucki D, Gisin N, Guinnard O, Ribordy G, Zbinden H (2002) Quantum key distribution over 67 km with a plug&play system. New J Phys 4(1):41
62. Hwang W-Y (2003) Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett 91(5):057901
63. Mehic M, Niemiec M, Rass S, Ma J, Peev M, Aguado A, Martin V, Schauer S, Poppe A, Pacher C et al (2020) Quantum key distribution: a networking perspective. ACM Comput Surv (CSUR) 53(5):1–41
64. Tysowski PK, Ling X, Lütkenhaus N, Mosca M (2018) The engineering of a scalable multi-site communications system utilizing quantum key distribution (QKD). Quantum Sci Technol 3(2):024001
65. Dynes J, Wonfor A, Tam W-S, Sharpe A, Takahashi R, Lucamarini M, Plews A, Yuan Z, Dixon A, Cho J et al (2019) Cambridge quantum network. npj Quantum Inf 5(1):101
66. Cao Y, Zhao Y, Lin R, Yu X, Zhang J, Chen J (2019) Multi-tenant secret-key assignment over quantum key distribution networks. Opt Express 27(3):2544–2561
67. Cao Y, Zhao Y, Wang J, Yu X, Ma Z, Zhang J (2019) SDQaaS: software defined networking for quantum key distribution as a service. Opt Express 27(5):6892–6909
68. Sasaki M, Fujiwara M, Ishizuka H, Klaus W, Wakui K, Takeoka M, Miki S, Yamashita T, Wang Z, Tanaka A et al (2011) Field test of quantum key distribution in the tokyo QKD network. Opt Express 19(11):10387–10409
69. Tajima A, Kondoh T, Ochi T, Fujiwara M, Yoshino K, Iizuka H, Sakamoto T, Tomita A, Shimamura E, Asami S et al (2017) Quantum key distribution network for multiple applications. Quantum Sci Technol 2(3):034003

70. Dianati M, Alléaume R (2007) Architecture of the secoqc quantum key distribution network. In: 2007 First international conference on quantum, nano, and micro technologies (ICQNM'07). IEEE, pp 13–13
71. Stucki D, Legre M, Buntschu F, Clausen B, Felber N, Gisin N, Henzen L, Junod P, Litzistorf G, Monbaron P et al (2011) Long-term performance of the swissquantum quantum key distribution network in a field environment. New J Phys 13(12):123001
72. Dong K, Zhao Y, Yu X, Nag A, Zhang J (2020) Auxiliary graph based routing, wavelength, and time-slot assignment in metro quantum optical networks with a novel node structure. Opt Express 28(5):5936–5952
73. Chen L-Q, Chen J-Q, Chen Q-Y, Zhao Y-L (2023) A quantum key distribution routing scheme for hybrid-trusted QKD network system. Quantum Inf Process 22(1):75
74. Mehic M, Fazio P, Rass S, Maurhart O, Peev M, Poppe A, Rozhon J, Niemiec M, Voznak M (2019) A novel approach to quality-of-service provisioning in trusted relay quantum key distribution networks. IEEE/ACM Trans Netw 28(1):168–181
75. Chunnilall CJ, Alleaume R, Brunner H, Degiovanni I, Fung C, Gramegna M, Hubel H, Huttner B, Lucamarini M, Peev M et al (2018) Quantum key distribution (QKD); components and internal interfaces. ETSI group report QKD 003 (2018-03)
76. Martin V, Aguado A, Lopez D, Peev M, Lopez V, Pastor A, Poppe A, Brunner H, Bettelli S, Fung F et al (2018) The madrid SDN-QKD network. In: Proceedings of the international conference on quantum cryptography (QCrypt'18)
77. Tessinari RS, Bravalheri A, Hugues-Salas E, Collins R, Aktas D, Guimaraes RS, Alia O, Rarity J, Kanellos GT, Nejabati R et al (2019) Field trial of dynamic DV-QKD networking in the SDN-controlled fully-meshed optical metro network of the bristol city 5GUK test network. In: 45th European conference on optical communication (ECOC 2019). IET, pp 1–4
78. Aguado A, Lopez V, Lopez D, Peev M, Poppe A, Pastor A, Folgueira J, Martin V (2019) The engineering of software-defined quantum key distribution networks. IEEE Commun Mag 57(7):20–26
79. Tessinari R, Woodward R, Shields A (2023) Software-defined quantum network using a QKD-secured SDN controller and encrypted messages. In: Optical fiber communication conference. Optica Publishing Group, pp 2–38
80. Fernández-Palacios JP, Jiménez F, Rivas-Moscoso JM, Pastor A, Folgueira J, López D, Brito JP, Martín V (2022) A multi-technology/multi-domain qkd deployment over a telco production network: practical issues and outcomes. In: Photonic networks and devices. Optica Publishing Group, pp 2–4
81. Cao Y, Zhao Y, Zhang J, Wang Q (2022) Software-defined heterogeneous quantum key distribution chaining: an enabler for multi-protocol quantum networks. IEEE Commun Mag 60(9):38–44
82. McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, Rexford J, Shenker S, Turner J (2008) OpenFlow: enabling innovation in campus networks. ACM SIGCOMM Comput Commun Rev 38(2):69–74
83. Enns R, Bjorklund M, Schoenwaelder J, Bierman A (2011) Network configuration protocol (NETCONF). Technical report
84. Dervisevic E, Lauterbach F, Burdiak P, Rozhon J, Slívová M, Plakalovic M, Hamza M, Fazio P, Voznak M, Mehic M (2022) Simulations of denial of service attacks in quantum key distribution networks. In: 2022 XXVIII International conference on Information, Communication and Automation Technologies (ICAT). IEEE, pp 1–5
85. Lo H-K, Curty M, Tamaki K (2014) Secure quantum key distribution. Nat Photonics 8(8):595–604
86. Rodimin V, Kiktenko E, Usova V, Ponomarev MY, Kazieva T, Miller A, Sokolov A, Kanapin A, Losev A, Trushechkin A et al (2019) Modular quantum key distribution setup for research and development applications. J Russ Laser Res 40:221–229
87. Wang J-Y, Yang B, Liao S-K, Zhang L, Shen Q, Hu X-F, Wu J-C, Yang S-J, Jiang H, Tang Y-L et al (2013) Direct and full-scale experimental verifications towards ground-satellite quantum key distribution. Nat Photonics 7(5):387–393
88. Bedington R, Arrazola JM, Ling A (2017) Progress in satellite quantum key distribution. npj Quantum Inf 3(1):30
89. Liao S-K, Cai W-Q, Handsteiner J, Liu B, Yin J, Zhang L, Rauch D, Fink M, Ren J-G, Liu W-Y et al (2018) Satellite-relayed intercontinental quantum network. Phys Rev Lett 120(3):030501
90. Poppe A, Fedrizzi A, Ursin R, Böhm H, Lorünser T, Maurhardt O, Peev M, Suda M, Kurtsiefer C, Weinfurter H et al (2004) Practical quantum key distribution with polarization entangled photons. Opt Express 12(16):3865–3871
91. Sharma A, Lenka S (2017) Transmission and control for QKD in online banking systems. J Enterp Inf Manag
92. Sasaki M (2018) Quantum key distribution and its applications. IEEE Security & Privacy 16(5):42–48

93. Thangapandiyan M, Anand PR, Sankaran KS (2018) Quantum key distribution and cryptography mechanisms for cloud data security. In: 2018 International Conference on Communication and Signal Processing (ICCSP). IEEE, pp 1031–1035
94. Republic, Geneva Switzerland S (2023) Securing data transfer for elections: ethernet encryption with quantum key distributio. https://marketing.idquantique.com/acton/attachment/11868/f-020f/1/-. Accessed 12 June 2023
95. Sundar DS, Narayan N (2014) A novel voting scheme using quantum cryptography. In: 2014 IEEE Conference on Open Systems (ICOS). IEEE, pp 66–71
96. Niemiec M, Machnik P (2016) Authentication in virtual private networks based on quantum key distribution methods. Multimed Tools Appl 75:10691–10707
97. Aguado A, López V, Martinez-Mateo J, Peev M, López D, Martín V (2018) Vpn service provisioning via virtual router deployment and quantum key distribution. In: 2018 Optical fiber communications conference and exposition (OFC). IEEE, pp 1–3
98. Wang L, Wang D, Gao J, Huo C, Bai H, Yuan J (2019) Research on multi-source data security protection of smart grid based on quantum key combination. In: 2019 IEEE 4th International Conference on Cloud Computing and Big Data Analysis (ICCCBDA). IEEE, pp 449–453
99. Winick A, Lütkenhaus N, Coles PJ (2018) Reliable numerical key rates for quantum key distribution. Quantum 2:77
100. George I, Lin J, Lütkenhaus N (2021) Numerical calculations of the finite key rate for general quantum key distribution protocols. Phys Rev Research 3(25):013274
101. Renner R (2008) Security of quantum key distribution. Int J Quantum Inf 06(01):1–127
102. Zhang Y, Coles PJ, Winick A, Lin J, Lütkenhaus N (2021) Security proof of practical quantum key distribution with detection-efficiency mismatch. Phys Rev Research 3(13):013076
103. Mehic M, Niemiec M, Siljak H, Voznak M (2020) Error reconciliation in quantum key distribution protocols
104. Jain R, Kundu S (2022) A direct product theorem for quantum communication complexity with applications to device-independent QKD. In: 2021 IEEE 62nd annual symposium on Foundations of Computer Science (FOCS). IEEE, pp 1285–1295
105. Vybornyi I, Trichili A, Alouini M-S (2021) In: Le KN (ed) Backflash light as a security vulnerability in quantum key distribution systems. Springer, Cham, pp 83–97
106. Meda A, Degiovanni I, Tosi A, Yuan Z, Brida G, Genovese M (2016) Backflash light characterization to prevent qkd zero-error hacking. arXiv preprint arXiv:1605.05562
107. Jain N, Derkach I, Chin H-M, Filip R, Andersen UL, Usenko VC, Gehring T (2021) Modulation leakage vulnerability in continuous-variable quantum key distribution. Quantum Sci Technol 6(4):045001
108. Trushechkin AS, Kiktenko EO, Kronberg DA, Fedorov AK (2021) Security of the decoy state method for quantum key distribution. PHYS-USP+ 64(1):88
109. Kumar R, Mazzoncini F, Qin H, Alléaume R (2021) Experimental vulnerability analysis of QKD based on attack ratings. Sci Rep 11(1):1–12
110. Cavaliere F, Prati E, Poti L, Muhammad I, Catuogno T (2020) Secure quantum communication technologies and systems: From labs to markets. Quantum Rep 2(1):80–106
111. Diamanti E, Lo H-K, Qi B, Yuan Z (2016) Practical challenges in quantum key distribution. NPJ Quantum Inf 2(1):1–12
112. George I, Lin J, Lütkenhaus N (2021) Numerical calculations of the finite key rate for general quantum key distribution protocols. Phys Rev Res 3(1):013274
113. Leverrier A, García-Patrón R, Renner R, Cerf NJ (2013) Security of continuous-variable quantum key distribution against general attacks. Phys Rev Lett 110(3):030502
114. Sibson P, Erven C, Godfrey M, Miki S, Yamashita T, Fujiwara M, Sasaki M, Terai H, Tanner MG, Natarajan CM et al (2017) Chip-based quantum key distribution. Nat Commun 8(1):13984
115. Abushgra AA (2021) Sarg04 and ak15 protocols based on the run-time execution and qber. In: 2021 IEEE 5th International conference on Cryptography, Security and Privacy (CSP). IEEE, pp 176–180
116. Yu X, Liu Y, Zou X, Cao Y, Zhao Y, Nag A, Zhang J (2022) Secret-key provisioning with collaborative routing in partially-trusted-relay-based quantum-key-distribution-secured optical networks. J Lightwave Technol 40(12):3530–3545
117. Tang X, Kumar R, Ren S, Wonfor A, Penty RV, White IH (2020) Performance of continuous variable quantum key distribution system at different detector bandwidth. Opt Commun 471:126034
118. Huang J, Wang Y, Wang H, Li Z, Huang J (2009) Man-in-the-middle attack on bb84 protocol and its defence. In: 2009 2nd IEEE International conference on computer science and information technology, pp 438–439
119. Inoue K, Honjo T (2005) Robustness of differential-phase-shift quantum key distribution against photon-number-splitting attack. Phys Rev A 71(4):042305

120. Tomamichel M, Colbeck R, Renner R (2010) Duality between smooth min-and max-entropies. IEEE Trans Inf Theory 56(9):4674–4681
121. Zapatero V, Leent T, Arnon-Friedman R, Liu W-Z, Zhang Q, Weinfurter H, Curty M (2022) Advances in device-independent quantum key distribution. arXiv preprint arXiv:2208.12842
122. De A, Portmann C, Vidick T, Renner R (2012) Trevisan's extractor in the presence of quantum side information. SIAM J Comput 41(4):915–940
123. Zhang P, Mao X (2020) Security analysis and optimization of BB84 QKD system post-processing. J Phys: Conf Ser 1621(1):012017
124. Chang Z, Wang F, Wang X, Liu X, Wu R, Zhang P et al (2021) Security analysis method for practical quantum key distribution with arbitrary encoding schemes. arXiv preprint arXiv:2109.04758
125. Ma X, Qi B, Zhao Y, Lo H-K (2005) Practical decoy state for quantum key distribution. Phys Rev A 72(15):012326
126. Hwang W-Y (2003) Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett 91(4):057901
127. Winick A, Lütkenhaus N, Coles PJ (2018) Reliable numerical key rates for quantum key distribution. Quantum 2:77
128. Grünenfelder F, Boaron A, Resta GV, Perrenoud M, Rusca D, Barreiro C, Houlmann R, Sax R, Stasi L, El-Khoury S et al (2023) Fast single-photon detectors and real-time key distillation enable high secret-key-rate quantum key distribution systems. Nat Photonics 17(5):422–426
129. Ahlswede R, Cai N, Li S-Y, Yeung RW (2000) Network information flow. IEEE Trans Inf Theory 46(4):1204–1216
130. Pan X-B, Chen X-B, Xu G, Dou Z, Li Z-P, Yang Y-X (2022) Quantum multicast communication over the butterfly network. Chin Phys B 31(1):010305
131. Pathumsoot P, Matsuo T, Satoh T, Hajdušek M, Suwanna S, Van Meter R (2020) Modeling of measurement-based quantum network coding on a superconducting quantum processor. Phys Rev A 101(5):052301
132. Sharma P, Agrawal A, Bhatia V, Prakash S, Mishra AK (2021) Quantum key distribution secured optical networks: a survey. IEEE Open Journal of the Communications Society. 2:2049–2083
133. Walenta N, Soucarros M, Stucki D, Caselunghe D, Domergue M, Hagerman M, Hart R, Hayford D, Houlmann R, Legré M et al (2015) Practical aspects of security certification for commercial quantum technologies. In: Electro-optical and infrared systems: technology and applications XII; and quantum information science and technology, vol 9648. SPIE, pp 199–209
134. Etsi F (2016) Quantum Key Distribution (QKD); Component characterization: characterizing optical components for QKD systems. https://www.etsi.org/deliver/etsi_gs/qkd/001_099/011/01.01.01_60/gs_qkd011v010101p.pdf. Accessed 15 May 2023
135. Chun H, Choi I, Faulkner G, Clarke L, Barber B, George G, Capon C, Niskanen A, Wabnig J, O'Brien D et al (2017) Handheld free space quantum key distribution with dynamic motion compensation. Opt Express 25(6):6784–6795
136. Pirker A, Dür W (2019) A quantum network stack and protocols for reliable entanglement-based networks. New J Phys 21(3):033003
137. Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK (1993) Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels. Phys Rev Lett 70(13):1895
138. Van Meter R (2012) Quantum networking and internetworking. IEEE Netw 26(4):59–64
139. Long G-L (2017) Quantum secure direct communication: principles, current status, perspectives. In: 2017 IEEE 85th Vehicular technology conference (VTC Spring). IEEE, pp 1–5
140. Pirandola S, Laurenza R, Ottaviani C, Banchi L (2017) Fundamental limits of repeaterless quantum communications. Nat Commun 8(1):1–15
141. Kumar M, Mondal B (2024) Quantum blockchain architecture using cyclic qscd and qkd. Quantum Inf Process 23(3):101