Optical and Quantum Electronics (2025) 57:264
https://doi.org/10.1007/s11082-025-08168-2

Feasibility discussion of quantum cryptography for Internet of Things security: a literature review

Yuer Yang[1,2,3] · **Yifeng Lin**[1,2] · **Jiancheng Xiao**[2] · **Zhihua Zhong**[4]

Received: 26 May 2024 / Accepted: 17 March 2025

Abstract
As the consequences of Internet of Things (IoT) failures may be severe, research on IoT security issues is of great significance. It is a fact that the increasing number of IoT devices brings security concerns. Encryption measures to address these emerging and growing security problems have been studied. Encryption methods have been seen primarily in the field of quantum cryptography. According to this advanced modern cryptography technique, their advantages and disadvantages are discussed and analyzed. This literature review is committed to providing solutions for IoT security problems with quantum cryptography techniques when questioning their feasibility. Some possible future research directions are proposed.

Keywords Quantum cryptography · Internet of Things · Security · Feasibility discussion

1 Introduction

Nowadays, depending on the rapid development of the Internet in technology, there has been an exponential increase in the Internet of Things (IoT) Li et al. (2018), Dai et al. (2019), Nord et al. (2019), Nauman et al. (2020), Kumar et al. (2019) and intelligent devices Xu et al. (2019). This situation Kassim (2020) alters the attention of authorities toward smart things. The widespread use of smart things and the tremendous increase in internet usage have made the IoT concept even more meaningful Manavalan and Jayakrishna (2019), Khanna and Kaur (2019), Li et al. (2015). It's undeniable that collecting a large number of smart things and making them connected according to certain rules needs high-security countermeasures on network, infrastructure and privacy of

Yuer Yang and Yifeng Lin have contributed equally to this work.

✉ Zhihua Zhong
zhong.z.af@m.titech.ac.jp

[1] Department of Computer Science, The University of Hong Kong, Hong Kong, China

[2] College of Cyber Security, Jinan University, Guangzhou, China

[3] School of Economics, Jinan University, Guangzhou, China

[4] School of Computing, Tokyo Institute of Technology, Tokyo, Japan

Published online: 16 April 2025

data Kassim (2020), Hassan (2019), Hassija et al. (2019), Atlam and Wills (2020) since, after all, based on the increasing trend in IoT, cyber security threats and attacks have also increased rapidly Hassija et al. (2019), Amanullah et al. (2020). One of today's most important needs is properly monitoring security measures Tahsien et al. (2020). Therefore, many cryptographic methods are used in the IoT, including classical cipher Arseni et al. (2016), blockchain Dai et al. (2019), machine learning (Hussain et al. (2020), Mohanta et al. (2020), Ahmad and Alsmadi (2021)), deep learning Amanullah et al. (2020), Al-Garadi et al. (2020), Aversano et al. (2021), Magaia et al. (2020), and reinforcement learning Uprety and Rawat (2020). Although classical encryption methods and some modern encryption algorithms have been developed mature, it is challenging to use them to prevent IoT from being attacked nowadays. Traditional encryption and decryption methods are no longer suitable for today's large-scale data and high data transmission requirements. Maintaining high-speed and high-efficiency transmission while using a suitable encryption and decryption scheme to solve security issues has contradicted the rapid development of IoT nowadays Fang et al. (2020). Many scholars have devoted themselves to solving the contradiction between high speed and safety and have proposed various solutions or optimization schemes Bhatt and Sharma (2019), Malina et al. (2021), Kumar et al. (2022).

The security problems of the IoT mainly include data leakage, identity authentication, side-channel attacks, long-term non-update of devices, and malicious code attacks Bhatt and Sharma (2019), Costin and Zaddach (2018). IoT applications collect a lot of users' data, most of them including personal information, to provide convenience; Therefore, encryption is required to protect the data. Since today's data sharing is indispensable Zheng et al. (2019), identity authentication has become an inevitable need Shah and Venkatesan (2018), Aman et al. (2018), Li et al. (2019). In addition to software security, hardware security should also be considered because even if users' data are successfully encrypted, the possibility of the device itself being hacked still remains Bhatt and Sharma (2019). Side-channel attacks, especially on devices that have not been updated for a long time, will become a major threat Ko and Mickens (2018). In addition, there are many IoT devices in the world, and the number is expected to increase significantly in the near future. Many people pay less attention to future device updates,Pham et al. (2021), Makhshari and Mesbah (2021), which also provides the breeding ground for malicious code. Quantum cryptography can solve the above security problems and maintain the original excellent performance of the IoT and its devices as much as possible.

Quantum information Benenti et al. (2019) is the core science of the so-called second quantum revolution Jaeger (2018) (Quantum 2.0) Pirandola et al. (2020). Based on the most powerful features and resources of quantum mechanics, new disruptive theories emerged rapidly, such as quantum entanglement Horodecki et al. (2009), Erhard et al. (2020), Stav et al. (2018), teleportation Pirandola et al. (2015) and the no-cloning theorem Wootters and Zurek (1982). Based on such characteristics, at the end of the last Bennett et al. (1983, 1992); Zbinden et al. (1998) and the beginning of this century Gisin et al. (2002), quite a few scholars proposed the idea of using quantum cryptography to deal with security issues. This kind of inspiration has subverted traditional cryptography thought. With the joint efforts of academia and industry, quantum cryptography, based on it, has gradually landed and has become a popular cryptography system.

Quantum cryptography, an interesting field using rules of quantum mechanics to develop a cryptosystem, is regarded as one of the most secure ones Feynman et al. (1982). It cannot be breached by anyone without getting noticed by the sender or the receiver of the message Kearney and Perez-Delgado (2021). Based on photons and their fundamental quantum properties He et al. (2018), quantum cryptography is to develop an indestructible

cryptosystem, as it is impossible to measure the quantum state of any system without alarming the system. Currently, cryptographic algorithms are using the principles of mathematics to try and develop efficient cryptosystems. An example of a mathematics-based cryptographic algorithm is where the secret key combines a large set of prime factors of large numbers generated at random. Cracking such keys is still an extraordinary task for a normal computer Balygin et al. (2018) though it is not impossible to make it cracked by a powerful quantum computer, which does not exist nowadays. At the same time, scientists are now turning from mathematics to physics Bhatt and Sharma (2019), Haight (2022) and trying to develop systems that can better replace those in use today to prevent future quantum computers from ergodic cracking.

IoT and smart devices have many loopholes regarding the security of the devices, users, or the network mentioned above. The current classical architecture of the IoT does not provide any provisions to detect the eavesdropper in the communications channel, which makes quantum cryptography valuable in IoT. For instance, there can be some attacks where only one device in the whole IoT network can be infected with some virus, and other devices trust the infected device and continue communications until it is detected Bhatt and Sharma (2019). Not being detected before a long period of time may result in a large amount of information being transmitted to any malicious entity. Some viruses may affect the systems in a manner that can only be removed by rebooting the systems, which could not or would not be done for a very long time Bhatt and Sharma (2019); Donno et al. (2016). Nevertheless, due to the features of quantum cryptography stated above, malware detection can be more effective based on it, where it alerts immediately if one device is affected. Hence, there are multiple different points of vulnerability, and IoT systems are highly susceptible to attacks Sengupta et al. (2020); Deogirikar and Vidhate (2017); Nawir et al. (2016), which can be prevented by quantum cryptography, generally speaking. In this paper, we study the possible solution of IoT security through quantum cryptography, enabling it to solve IoT security problems with quantum cryptography techniques when questioning their feasibility. To better describe this literature review, four major contributions are listed as follows.

1) This paper analyzes the traditional and recent common quantum cryptography algorithms.
2) Detailed scientific problems and implementations of quantum cryptography in the IoT are introduced.
3) This paper evaluates and analyzes the realization of quantum cryptography in IoT security, which provides feasibility analysis and evidence of quantum cryptography applications in IoT.
4) Quantum cryptography and the existing deficiencies of quantum cryptography in IoT security are refined. Research trends and possible future directions are expounded and discussed.

The rest of this literature review will follow the structure below. Section 2 enumerates the more common quantum cryptography schemes in recent years and mainly discusses which schemes can theoretically be applied in the IoT. Section 3 further elaborates on the realization of quantum cryptography in the IoT. Section 4 evaluates the security of the IoT based on quantum cryptography, discusses its advantages and disadvantages, and further gives a feasibility analysis. Some possible future work and possible discussion are proposed in Sect. 5. Section 6 provides the conclusion of quantum cryptography in IoT.

2 Quantum cryptographic algorithms

This section will theoretically introduce quantum cryptography schemes, including Shor's factorization algorithm and the basic concepts of key distribution. Based on these concepts, the elaboration of quantum key distribution (QKD) was expanded, including discrete variable quantum key distribution (DV-QKD) and continuous variable quantum key distribution (CV-QKD). Finally, this section will present security at the theoretical level of quantum cryptography.

2.1 Shor's algorithm for factoring

Shor's algorithm Ekert and Jozsa (1996) was one of the most famous algorithms in the field of quantum computing, whose major contribution was to reduce the time complexity of the algorithm significantly. It suggested an efficient way of factoring large non-prime numbers in polynomial time, which takes up exponential time when performed classically. The motivation of this algorithm was that the current cryptographic algorithms, such as the Rivest-Shamir-Adleman (RSA) algorithm, Ízdemir et al. (2021), were based on the principle of factoring large numbers that cannot solve the problem in polynomial time on the traditional computer. However, the computational speed of quantum computers is very fast and efficient in calculating the factors, and hence these algorithms, which take a long time to execute classically, can be easily reached shortly Politi et al. (2009), Smolin et al. (2013), Skosana and Tame (2021), de Lima Marquezino et al. (2019). That is to say, although Shor's algorithm is time-consuming when executed classically, it is very friendly to the computational process of quantum computers due to its suitability, making this algorithm an indispensable and important contribution.

To better illustrate the contribution of the algorithm, Table 1 was used to compare the time complexity of it on quantum computers and classical computers Bhatt and Sharma (2019), Bhatia and Ramkumar (2020), respectively, where L was the length of the number N in bits. The problem of sexuality had been excluded because quantum computers and classical computers are not comparable in terms of time-consuming due to their different computing resources. It can be seen that Shor's algorithm provided exponential time complexity optimization for non-prime number decomposition in quantum cryptographic schemes.

The algorithm steps are as follows, where **Step** B can be executed in a classical way.

Step A Given an odd composite number N, the target is to find an integer $d \in (1, N)$, which divides N ($d|N$).
Step B Convert the problem of factoring to that of finding the period.
Step C Find the period using the quantum Fourier transform Nam et al. (2020) which is responsible for quantum speedup.

Table 1 The time complexity analysis of Shor's algorithm on quantum computers and classical computers

Situation	Quantum computers	Classical computers
Best	$O(\log N)$	$O\left((\log N)^k\right)$
Worst	$O(L^3)$	$O\left(e^{L^{\frac{1}{3}}(\log L)^{\frac{2}{3}}}\right)$

Consequently, the algorithm depends on three main factors. They are modular arithmetic, quantum parallelism, and quantum Fourier transform.

2.2 Basic notions of quantum key distribution (QKD)

QKD is the Bennett-Brassard 1984 protocol (BB84 protocol) Bennett and Brassard (2020) presented by physicist Bennett and cryptographer Brassard, based on the measurement principle of quantum mechanics. QKD guarantees the security of keys fundamentally. This section considered both DV systems (such as qubits or other quantum systems with finite dimensions) and CV systems (such as bosonic modes in the electromagnetic field), which are both described by an infinite-dimensional Hilbert space. Here, several general aspects that apply to both systems were mentioned. A generic prepare-and-measure QKD protocol Wang et al. (2019) contains two major steps - quantum communication and classical postprocessing Curty and Lo (2019). During quantum communication, the sender (Alice) encoded instances of a random classical variable α into non-orthogonal quantum states over a quantum channel (optical fiber, free-space link) controlled by the eavesdropper (Eve), who tried to steal the encoded information. The linearity of quantum mechanics Peng et al. (2020) forbids the performance of perfect cloning; therefore, Eve can only get partial information while disturbing the quantum signals. At the output of the communication channel, the receiver (Bob) measured the incoming signals and obtained a random classical variable β. After plenty of channels were used, Alice and Bob shared the raw data, described by two correlated variables α and β. The remote parties can estimate the parameters, including transmissivity and noise, of the channel using parts of the raw data. This parameter estimation stage is vital for evaluating the amount of postprocessing to extract a private shared key from the remaining data. Based on the information above, they performed a stage of error correction (EC), which allows them to detect and eliminate errors, followed by a stage of privacy amplification (PA) that allows them to reduce Eve's stolen information to an insignificant amount. Relying on the variable guessed, there are direct reconciliation (DR) or reverse reconciliation (RR). In DR, Bob processed his outcomes to infer Alice's encodings. Usually, this procedure is assisted using forward classical communication (CC) from Alice to Bob. In contrast, Alice posted her encoding variable in RR to infer Bob's outcomes. Usually, this procedure is assisted by a final round of backward CC from Bob to Alice.

2.3 Quantum key distribution (QKD)

Quantum Key Distribution (QKD) is a revolutionary cryptographic technique that leverages the principles of quantum mechanics to enable secure communication between two parties. Unlike classical cryptographic methods, which rely on mathematical complexity for security, QKD uses the fundamental properties of quantum states to ensure that any eavesdropping attempt can be detected. The most well-known QKD protocol is the BB84 protocol, developed by Charles Bennett and Gilles Brassard in 1984. In this protocol, the sender (Alice) transmits a sequence of quantum bits (qubits) to the receiver (Bob) using a quantum channel, such as polarized photons. These qubits are encoded in one of two bases, chosen randomly by Alice. Bob also randomly selects bases to measure the incoming qubits. After the transmission, Alice and Bob publicly compare their chosen bases (but not the actual qubit values) to sift out the bits where their bases are matched, forming a raw key. The security of QKD arises from the no-cloning theorem of quantum mechanics,

which states that an unknown quantum state cannot be copied without disturbing it. Therefore, any attempt by an eavesdropper (Eve) to intercept and measure the qubits will introduce detectable errors, alerting Alice and Bob to the presence of an intruder. Once the raw key is established, further classical post-processing steps, such as error correction and privacy amplification, are performed to eliminate any potential information leakage and produce a final secure key. This key can then be used for symmetric encryption, ensuring that the communication remains confidential and tamper-proof. QKD has the potential to provide unconditional security, making it a promising solution for safeguarding sensitive information in an era where quantum computers could potentially break traditional cryptographic systems. However, practical implementations of QKD face challenges such as distance limitations, noise in quantum channels, and the need for specialized hardware, which are areas of ongoing research and development.

To better understand how QKD works in practice, it is essential to delve into the underlying quantum mechanics principles. QKD is a basic technique used in quantum cryptography. As is well acknowledged, quantum computing uses a stream of photons, so-called "spin" Borregaard et al. (2019) to transmit data. There are basically 4 types of spins: Horizontal, vertical, 45° diagonal, and −45° diagonal Hietarinta et al. (2019). The horizontal and vertical filters are put under the rectilinear scheme, and the 2 diagonal filters are put under the diagonal scheme. Generally, the horizontal and 45° filters represent binary 1, and the vertical and −45° filters represent binary 0. By shielding the single photon source with two different bases + and ×, four different polarized photons can be obtained, namely ↑, ↓, ↘, ↗. Similarly, two bases can be used to measure photons Ma et al. (2020): + and ×, which are named measurement bases. Photons have four polarization angles, namely ↑, ↓, ↘, and ↗. The corresponding relationship between a binary bit and the polarization angle is shown in Table 2 Fedorov (2019), where 0/1 means that there is a 50% probability of measuring 0 and a 50% probability of measuring 1 Table 2 .

2.3.1 Discrete variable QKD (DV-QKD)

In the context of DV-QKD, the word "discrete" refers to the fact that the quantum variables being used to transmit information are discrete, as opposed to continuous. In this case, the quantum variables are typically the polarization states of individual photons, which can have one of two discrete values like horizontal or vertical polarization. The DV protocol can be regarded as the earliest or simplest form of QKD. Although the famous BB84 protocol was proposed in 1984 Bennett and Brassard (2020), the first idea of using quantum physics for security services dated back to the early 1970 s when Wiesner was exploring the idea of making banknote counterfeit-resistant Brassard (2005). The first paper on quantum cryptography was published in 1982 Bennett et al. (1983). This subsection will briefly describe the DV-QKD protocol.

Table 2 The correspondence between binary bits and polarization angles

Index	Bit	Base	Polarization angle	Measured by +	Measured by ×
1	0	+	↑	0	0/1
2	1	+	↓	1	0/1
3	0	×	↗	0/1	0
4	1	×	↘	0/1	1

A qubit is represented as a vector in a bi-dimensional Hilbert space, which is drawn by the vectors shown in Eq. (1).

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}, |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1}$$

As is shown in Eq. (2), any pure qubit state can thus be expressed as a linear superposition of these basis states Chernega et al. (2022), where $\theta \in (0, \pi)$, $\phi \in (0, 2\pi)$, and i is the imaginary unit.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + \mathrm{e}^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{2}$$

When $\theta = 0$ or $\theta = \pi$, the basis states $|0\rangle$ and $|1\rangle$ are recovered, respectively, which are placed at the poles of the sphere. When $\theta = \frac{\pi}{2}$, the qubit pure state is a vector lying on the equator of the sphere. By identifying the four vectors aligned along the $\hat{x}$ and $\hat{y}$ axes, which are obtained in correspondence of four specific values of ϕ, four examples are shown in Eq. (3), Eq. (4), Eq. (5), and Eq. (6), respectively.

$$\phi = 0 : |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} \tag{3}$$

$$\phi = \pi : |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -1 \end{pmatrix} \tag{4}$$

$$\phi = \frac{\pi}{2} : |+i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ i \end{pmatrix} \tag{5}$$

$$\phi = \frac{3\pi}{2} : |-i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ -i \end{pmatrix} \tag{6}$$

The basis vector in Eq. (1) is the eigenstate of the Pauli operator (matrix) Bartlett et al. (2002). The normalized form of the "Z bases" is shown in Eq. (7). Likewise, Eq. (8) and Eq. (9) are also the normalized eigenstates of the Pauli operator (matrix). The eigenstates are idiomatic in QKD.

$$\sigma_z = Z = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{7}$$

$$\sigma_x = X = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \tag{8}$$

$$\sigma_y = Y = \frac{1}{\sqrt{2}}\begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \tag{9}$$

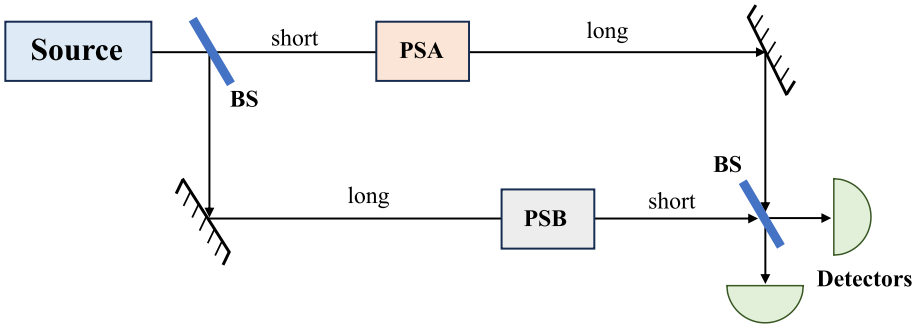

Fig. 1 The PSA - PSB Detection System. In this way, the detectors can detect which channel has been selected. This figure was drawn based on Pirandola (2020)

Table 3 Encryption and decryption information of sender and receiver

Sender's basis	Sender's bit	Sender's state	Receiver's Z	Receiver's X
Z	0	$\|0\rangle$	0	0/1
Z	1	$\|1\rangle$	1	0/1
X	0	$\|+\rangle$	0/1	0
X	1	$\|-\rangle$	0/1	1

Based on the above information, Table 3 can be made when an attack was performed in the channel with the monitoring shown in Fig. 1 Pirandola et al. (2020), where 0/1 means that there is a 50% probability of measuring 0, and a 50% probability of measuring 1. According to the measurement results of the measurement base, the communication partner can know whether an attacker was eavesdropping. In addition, Eq. (10) and Equation Eq. (11) explain why the quantum cryptosystem can still detect the retransmission even if an attacker intercepts the retransmission in the channel. This provides theoretical support for IoT security.

$$|\theta\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi}\sin\left(\frac{\theta}{2}\right)|1\rangle \tag{10}$$

$$|\theta\rangle^{\perp} = \sin\left(\frac{\theta}{2}\right)|0\rangle - e^{-i\phi}\cos\left(\frac{\theta}{2}\right)|1\rangle \tag{11}$$

There is an interesting principle Robertson (1929) in quantum mechanics known as the uncertainty principle, which states that all the properties of a particle, including position and momentum, cannot be measured without disturbing its current state Bhatt and Sharma (2019), Busch et al. (2007), and photons are subject to this principle as well. If people try to measure the spin of the photon, the spin will change, which may change the status of the photon. Thus, people can know that the stream of communicating photons was interrupted by an unwanted entity.

2.3.2 Continuous-variable QKD (CV-QKD)

In contrast to discrete variables, continuous variables are physical quantities that can take on any value within a certain range or continuum in the context of quantum communication. Continuous variables refer to the use of quantum states that are characterized by continuous values, such as the amplitude and phase of a light wave or the position and momentum of a particle. In the following discussion of the CV-QKD protocol, the variance of the vacuum state was set to 1. The CV quantum system was described by an infinite-dimensional Hilbert space. Therefore, we focused on considering n bosonic modes in the electromagnetic field with the tensor product Hilbert space and their corresponding n pairs of field operators, where k is a natural number from 1 to n. Each mode can be shown in Eq. (12). These operators can be arranged into an n-mode vector, which is shown in Eq. (13). Generally speaking, the variables $\hat{q}_k$ and $\hat{p}_k$ are two physics in CV-QKD that respectively represent the position and momentum of quantum states. The variables $\hat{a}_k$ and $\hat{a}'_k$ are two light field modes. The equations show how to convert two light field modes into position and momentum operators.

$$\hat{q}_k := \hat{a}_k + \hat{a}'_k, \hat{p}_k := i\left(\hat{a}'_k - \hat{a}_k\right) \tag{12}$$

$$\hat{\boldsymbol{x}} := (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2, \cdots, \hat{q}_n, \hat{p}_n)^{\mathrm{T}} \tag{13}$$

Using standard boson exchange relations, for field creation and annihilation operators Yang (2018), it is easy to verify that any pair of entries of a vector satisfies the exchange relation shown in Eq. (14) below, where Ω is a symplectic form Belin et al. (2019).

$$\hat{x}_l, \hat{x}_m t = 2i\Omega_{lm}, \Omega = \bigoplus_{k=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{14}$$

For a single mode, one can consider different classes of quantum states, and the most significant is the coherent states Wu et al. (2020). As the variance of the vacuum state was set to 1, these can be with minimum (vacuum) noise uncertainty Fischer (2019), symmetrically distributed in the two quadratures, and characterized by their complex amplitudes in the phase space. This subtly provides a method for monitoring in the IoT, a monitoring scheme based on coherent states.

The basic one-way CV-QKD protocol can be classified according to the quantum status employed (coherent or compressed), the type of encoding employed (Gaussian modulation or discrete alphabet), and the type of measurement used (homodyne or heterodyne detection). In particular, Gaussian protocols based on Gaussian modulation of Gaussian states have received increasing attention in recent years, not only because Gaussian states are frequently generated in quantum optics laboratories but also because they are relatively easy to study based on their description of mean values, which are of benefit Clements et al. (2018), Nichols et al. (2019), Yuan et al. (2022).

2.4 Theoretical security of quantum cryptographic

To better illustrate its security, we adopt an intuitive approach to QKD security based on uncertainty and entanglement. This subsection introduces (quantum) information entropy

Vedral (2002), Kak (2007), Isonguyo et al. (2018) and mathematical scaling to provide evidence of feasibility more grounded.

One of the fundamental principles of quantum physics that is intuitively relevant to privacy is Heisenberg's uncertainty principle. The uncertainty principle states that for some physical quantities (such as position and momentum), their values cannot be measured accurately at the same time. In computers, properties of the uncertainty principle can be simulated through the use of randomness and probability like pseudo-random number generation and probabilistic algorithms. Since Maassen-Uffink, in its modern information-theoretic form, states that for any two measurements X, Z with eigenvectors $|x\rangle$ and $|z\rangle$ respectively, there is Eq. (15) where H is the information entropy based on probability p, calculated as Eq. (16).

$$H(X) + H(Z) \geqslant -\log_2 \max_{x,z} |\langle x|z\rangle|^2 \tag{15}$$

$$H(X) = -\sum_x p_x \log_2 p_x \tag{16}$$

Importantly, the bound on the right-hand side of Eq. (15) is independent of the initial state, and the first idea of directly exploiting this uncertainty principle for security proofs dates back to 2004 Grosshans and Cerf (2004), Koashi (2009), Coles et al. (2017). However, it turns out that when the most general coherent attack is considered, it is possible for an adversary to gain access to quantum memory and use this to purify the state held by honest parties. The information entropy is discussed in the famous EPR paper, meaning that $H(X|B) := H(XB) - H(B)$ in equation Eq. (17) represents the condition of the classical quantum state after the measurement Von Neumann entropy Brown et al. (2021). This is in contrast to the classical memory system B on the left side of equation Eq. (17), which also exhibits a lower bound. Fortunately, entanglement turns out to be one-to-one Qian et al. (2018), because for three-way quantum states A, B, and C, the more A is entangled with B, the less A is entangled with C, and vice versa. Furthermore, it is now possible to recover the Maassen-Uffink bound in a tripartite setting by showing that it is this EUR with quantum side information that Eq. (18) is used to infer the security of QKD. This section infers the security of quantum cryptography from a purely mathematical point of view and concludes that it can be done by calculating the number of bit differences between Alice and Bob on a random sample of the original key. It is not difficult on a networked device. The mathematical proofs in this subsection provide sufficient support for the theoretical feasibility of quantum cryptography on the IoT.

$$H(X|B) + H(Z|B) = 0 \tag{17}$$

$$H(X|B) + H(Z|C) \geqslant -\log_2 \max_{x,z} |\langle x|z\rangle|^2 \tag{18}$$

3 Implementation of quantum cryptography in the IoT

This section will introduce the non-communication quantum cryptographic equipment and then separately introduce the specific applications of the discrete variable quantum key distribution (QKD) scheme and the continuous variable QKD scheme in the IoT.

3.1 Device-independent QKD (DI-QKD)

In general communications networks, it is often seen that two computers do not communicate directly. They are called device-independent (DI) smart devices Zhou et al. (2020), Liu et al. (2018), Arnon-Friedman et al. (2018), Zhou et al. (2020), Niu et al. (2018), Cao et al. (2020), Wei et al. (2020). But as a matter of fact, there are always some intermediate measurement devices that help the message to go from the source to the destination. Today, in such a case, we can not trust third-party devices to be completely safe and secured anymore since, after all, they may be tampered with by some malicious entity or by the developers themselves. Also, the risk of side-channel attacks is a concern. The device-independent QKD aims at modifying the original QKD to be safe in the case of untrusted third-party devices. The aim of QKD is for two computers, Alice and Bob, to share a common cryptographic key through communications over public channels. It is known that the BB84 protocol (the quantum cryptographic protocol) is safe even under the channel noise and possible detector faults at the end of Bob, with the assumption that the apparatus used on Alice's side is perfectly working to produce photons. But when we work in reality, this assumption does not hold well because there are high possibilities of faulty apparatus at Alice's side, too, which could hamper the security of the private string shared by Alice and Bob for communications. For the solution to this problem, we need some devices with the capabilities of self-testing. After passing these tests, the device is said to be secure for communications. Also, cross-checking the polarizations and their probability distributions can be a solution. There are various implementations for the solution to these problems.

Device-Independent Quantum Key Distribution (DIQKD) represents a significant advancement in the field of quantum cryptography, offering a higher level of security compared to traditional QKD protocols. Unlike conventional QKD schemes, which rely on detailed assumptions about the internal workings of the devices used, DIQKD achieves security without requiring any trust in the devices themselves. This is accomplished by leveraging the principles of quantum nonlocality, particularly through the violation of Bell inequalities, to certify the presence of entanglement and ensure the integrity of the key distribution process. In DIQKD, the security proofs are based solely on the observed correlations between measurement outcomes, making it immune to many types of side-channel attacks that exploit device imperfections. This robustness makes DIQKD particularly appealing for practical implementations where device characterization is challenging or where adversaries may have sophisticated control over the hardware.

However, DIQKD poses significant experimental challenges, primarily due to the stringent requirements for high detection efficiencies and low noise levels to achieve a meaningful violation of Bell inequalities. Recent advancements in photon source technology, single-photon detectors, and error correction techniques have brought DIQKD closer to practical realization. Despite these challenges, DIQKD holds immense promise for future secure communication systems, as it provides a framework for achieving information-theoretic security even in the presence of untrusted devices. This makes it a cornerstone of research in quantum cryptography, with ongoing efforts focused on improving its feasibility and performance in real-world scenarios.

DIQKD fundamentally relies on the violation of Bell inequalities, which serves as a witness to the presence of quantum entanglement between distant parties. This

entanglement is a critical resource for ensuring that any eavesdropping attempt by an adversary will inevitably disturb the quantum correlations, thereby revealing their presence. This feature allows DIQKD to provide security guarantees that are independent of the physical implementation of the devices, a property known as "device independence." This is a stark contrast to traditional QKD protocols, such as BB84 or decoy-state QKD, where the security proofs depend on assumptions about the devices' behavior, such as the exact form of the prepared states or the efficiency of the detectors.

Moreover, DIQKD has profound implications for the scalability and interoperability of quantum networks. In a future quantum internet, where multiple parties and devices from different manufacturers may be interconnected, DIQKD offers a unified framework for ensuring end-to-end security without requiring detailed knowledge of each component's internal workings. This is particularly important for large-scale deployments, where device characterization and standardization may be impractical. Additionally, DIQKD can be integrated with other quantum communication protocols, such as quantum repeaters and entanglement distribution networks, to enable secure communication over global distances. Despite its current experimental challenges, such as the need for near-unit detection efficiency and low noise rates, ongoing research in quantum optics, error mitigation, and fault-tolerant techniques is steadily overcoming these barriers. As a result, DIQKD is poised to play a pivotal role in the realization of ultra-secure quantum communication infrastructures, paving the way for a new era of privacy and data protection in the quantum age.

3.2 DV-QKD protocols in IoT

In 2007, three groups simultaneously reported the demonstration of two decoy status BB84 in a one-way QKD real system Lo et al. (2005), Zhao et al. (2006), Peng et al. (2007). They employed phase encoding and demonstrated secure key generation over 107 kms using fiber optics on spools in the lab. Including limited statistics in the parameter estimation, a key rate of 12 bit/s is achieved. At the same time, the relevant research team also carried out delay tests on the corresponding hardware systems Rosenberg et al. (2007), Ellis et al. (2007). The test results are shown in Fig. 2. Figure 2 presents the normalized cross-correlation between Alice's modulation signal and Bob's homodyne detector output for the same quadrature (e.g., x or p), measured over 4 ms with a 25 MHz sampling frequency. The strong synchronization and linear correlation (Alice's vs. Bob's Gaussian keys on x/y-axes) validate quadrature-specific key generation in the CV-QKD system. Observed minor phase noise in the cross-correlation contributes to excess noise, underscoring the importance of precise synchronization and phase stability. These results demonstrate the feasibility of homodyne detection and cross-correlation techniques for high-fidelity QKD implementations. Overall, the response is optimistic and timely Zhang et al. (2019). This satisfies the hardware requirements of IoT devices, allowing IoT security to be as secure as possible while remaining as high-performance as possible.

After research and judgment, the possible equipment composition is as follows. The transmitter consists of 10 laser diodes, each generating a 1 ns pulse with a center wavelength of 1550 nm and a repetition rate of 2.5 MHz. Four laser diodes were used to generate the signal and high-intensity decoy status, respectively, and a polarization controller was used to convert the output polarization of the laser diodes to the corresponding polarization of one of the four BB84 statuses. Two additional laser diodes align the two sets of polarization bases, which are time-division multiplexed. Using a network of multiple BSs and PBSs

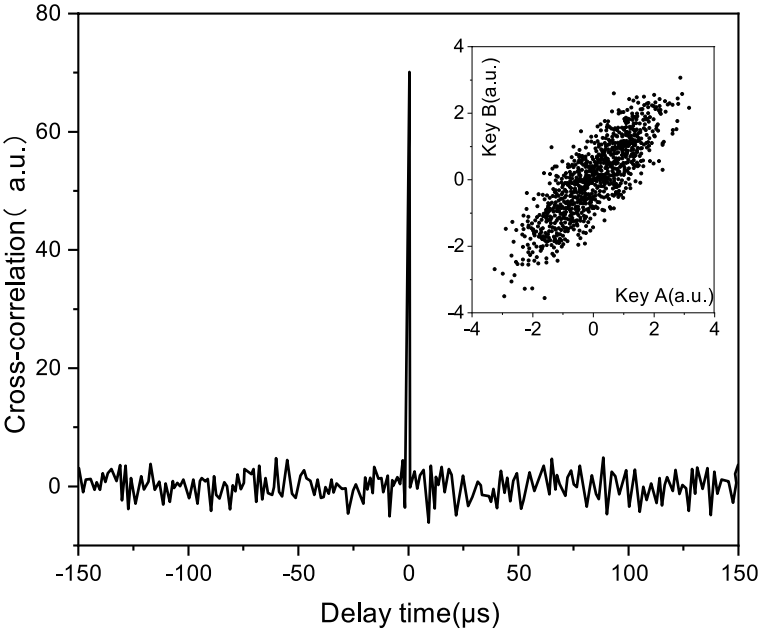

Fig. 2 The DV-QKD-based IoT device latency test. The experiments were re-conducted and the figure was re-drawn according to Zhang et al. (2019)

would require routing the outputs of the 10 laser diodes to a single fiber and an additional DWDM filter to ensure equal wavelengths of emitted photons. Additionally, to reduce cost, the receiver consists of two single-photon detectors and a switch randomly selecting a polarization base.

Other examples that have applied the discrete variable quantum cryptography allocation scheme to practice are shown in Fig. 3. We will briefly introduce the principles of the following four examples.

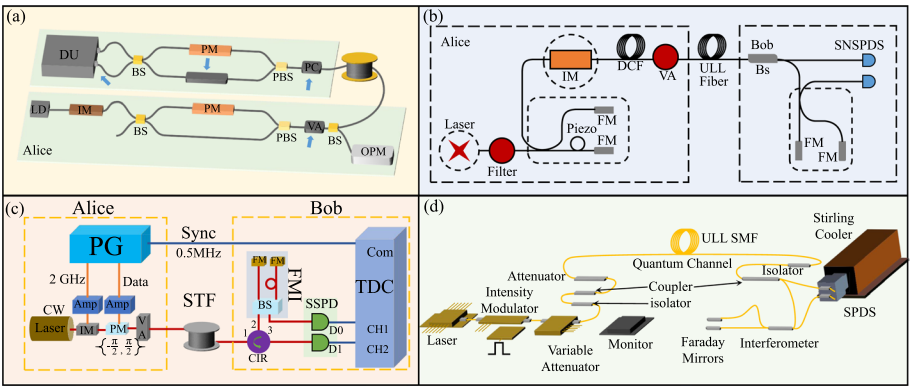

Fig. 3 Some real instances of DV-QKD. This figure was re-drawn from Pirandola (2020)

Examples (a) to (d) all rely on the basic principles of quantum mechanics, especially quantum superposition and quantum entanglement. The core of quantum communication is to use quantum states (such as the polarization state or phase state of photons) to encode information to ensure the security and non-eavesdropping of communication. The security of quantum communication is based on the No-Cloning Theorem. Any eavesdropping on the quantum state will introduce disturbances, which will be detected by the communicating parties (Alice and Bob). The above four examples all use photons as carriers of quantum information, encode quantum information by changing their polarization state, phase state, or time state, and establish a quantum channel between the communicating parties (Alice and Bob). However, in different examples, the sender Alice performs different operations on the photon and uses different instruments, which leads to different processing of the received photon signal by the receiver Bob.

In example (a), Alice uses a phase modulator (PM) and a beam splitter (BS) to phase modulate and separate photons. After the photons pass through a polarization beam splitter (PBS), they form different polarization states. After receiving the photons, Bob uses a phase modulator and a beam splitter to demodulate the photons and extract the key information by detecting the phase and polarization state of the photons. Finally, the communicating parties Alice and Bob generate a shared key by comparing the measurement results.

In example (b), Alice uses an intensity modulator (IM) and a phase modulator (PM) to modulate the intensity and phase of the photons. Unlike example (a), a beam splitter (BS) is not used to separate the photons. The photons are transmitted to Bob via optical fiber. Bob uses a superconducting nanowire single photon detector (SNSPDS) and an interferometer to detect and demodulate the photons. Finally, the two parties use a Stirling refrigerator and a synchronization signal (Sync) to ensure the synchronization and stability of photon transmission and finally generate a shared key.

In example (c), Alice modulates and isolates photons through modulators and isolators to ensure that photons are transmitted to Bob through the quantum channel in a single-photon state. Compared with examples (a) and (b), an isolation operation is introduced here, not just the modulation of photons. After receiving the photon signal, Bob uses a single-photon detector (SPDS) and an interferometer to detect and demodulate the photons. Both parties perform data synchronization and error correction through the classical channel (Com) to ensure the accuracy and security of key distribution and finally generate a shared key.

In example (d), the Alice phase modulates photons through a Faraday interferometer and uses a variable attenuator to adjust the photon intensity. Although the phase and intensity of photons are modulated here like in example (b), the instruments used are different. Example (b) is more suitable for high-speed, low-noise quantum communication, while example (d) focuses more on the flexibility of phase modulation and precise control of photon intensity. The photons are transmitted to Bob through optical fiber. After Bob receives the photon signal, he uses a single photon detector (SPDS) and an interferometer to detect and demodulate the photon. Both parties extract the key and generate a shared key by monitoring the intensity and phase information of the photon.

Table 4 compares four discrete variable quantum cryptography allocation schemes. From the table, we can conclude that although the above four examples are all discrete variable quantum cryptography allocation schemes, they operate on photons differently in the implementation process, use different instruments, and have different transmission media, so their applicable scenarios are also different.

Table 4 The comparison of four discrete variable quantum cryptography allocation schemes

Examples	Core components	Photon modulation technology	Photon detection technology	Transmission media	Special technologies
(a)	Phase modulator (PM), beam splitter (BS), polarization beam splitter (PBS)	Phase and polarization modulation	Phase modulator and beam splitter Demodulation	Free space or fiber	Polarization state detection
(b)	Intensity modulator (IM), phase modulator (PM), superconducting nanowire single-photon detector (SNSPDS)	Intensity and phase modulation	Superconducting nanowire single-Photon detector (SNSPDS)	Fiber	Stirling cooler
(c)	Modulator (Modulator), isolator (Isolator), single photon detector (SPDS)	Modulator modulation	Single photon detector (SPDS)	Quantum channel and classical channel	Classical channel synchronization and error correction
(d)	Faraday interferometer, variable attenuator, single photon detector (SPDS)	Faraday interferometer phase modulation	Single photon detector (SPDS)	Optical fiber	Variable attenuator adjusts photon intensity

3.3 CV-QKD protocols in IoT

The mainstream continuous variable quantum cryptography allocation scheme is point-to-point (p2p for short) on the IoT, which also aligns with the original end-to-end design of IoT smart devices.

The first version of CV-QKD on IoT or connected smart devices was based on coherent status modulation and homodyne detection. The optics consisted of bulk optics, operating at a wavelength of 780 nm. This pioneering work and some follow-up experiments constituted the first generation of important CV-QKD systems. Although the concept of CV-QKD has been successfully demonstrated, its relatively low mechanical stability due to telecom-incompatible wavelengths makes it unsuitable for implementing robust long-distance and high-speed QKD systems in optical fibers. To overcome these obstacles, a new generation of CV-QKD systems was proposed. The new system utilizes telecom wavelengths, is primarily based on telecom components, incorporates an optimized error correction scheme, and incorporates multiple active feedback control systems to enhance mechanical stability. With these innovations, the key rate was up to 1 Mbps for a distance of 25 kms and about 300 bps for a distance of 100 kms. Two different field tests of CV-QKD over a commercial fiber optic network for distances up to 50 km at a speed of over 6 kbps, also the longest field test of CV-QKD to date Pirandola et al. (2020), achieving a key rate of 2 orders of magnitude than previous tests. Later, some scholars demonstrated CV-QKD on a 202-kilometer ultra-low-loss fiber, narrowing the gap between the ultra-long distance achievable by the DV-QKD protocol. This record-breaking CV-QKD implementation doubled the previous distance record and showed the way to long-range and large-scale secure QKD using room temperature standard telecom components. The third generation of CV-QKD systems was based on generating the phase reference (or LO) power at the receiving station, while previous generations generated the LO power at the transmitting station and thus co-propagated with the signal in the fiber. As a result, the system has also evolved from a simple proof-of-concept demonstration to a more technologically advanced demonstration using telecom components.

Other examples that have applied the continuous variable quantum cryptography allocation scheme to practice are shown in Fig. 4. The three examples given in Fig. 4 provide different technical means to realize signal modulation, transmission, and processing. The CV-QKD system requires high-precision signal control and flexible receiving and processing capabilities. Examples (a) and (b) provide hardware-level solutions, while example (c) enhances the flexibility and configurability of the system through software-defined methods. The combination of these technologies can significantly improve the performance and security of the CV-QKD system and ensure the efficiency and reliability of the quantum key distribution process. The working principles of examples (a), (b), and (c) will be briefly introduced below.

Example (a) Frequency conversion or demodulation is achieved by mixing the input signal with the LO signal. In communication systems, this technique is often used to convert high-frequency signals to intermediate frequencies or baseband signals for subsequent processing. LO provides a stable reference frequency, and by mixing with the input signal, the phase and amplitude information of the signal can be extracted, thereby achieving signal demodulation or frequency down-conversion.

Example (b) The optical signal is modulated and controlled through a series of optical components. The laser (L) generates the optical signal, the Faraday mirror (FM)

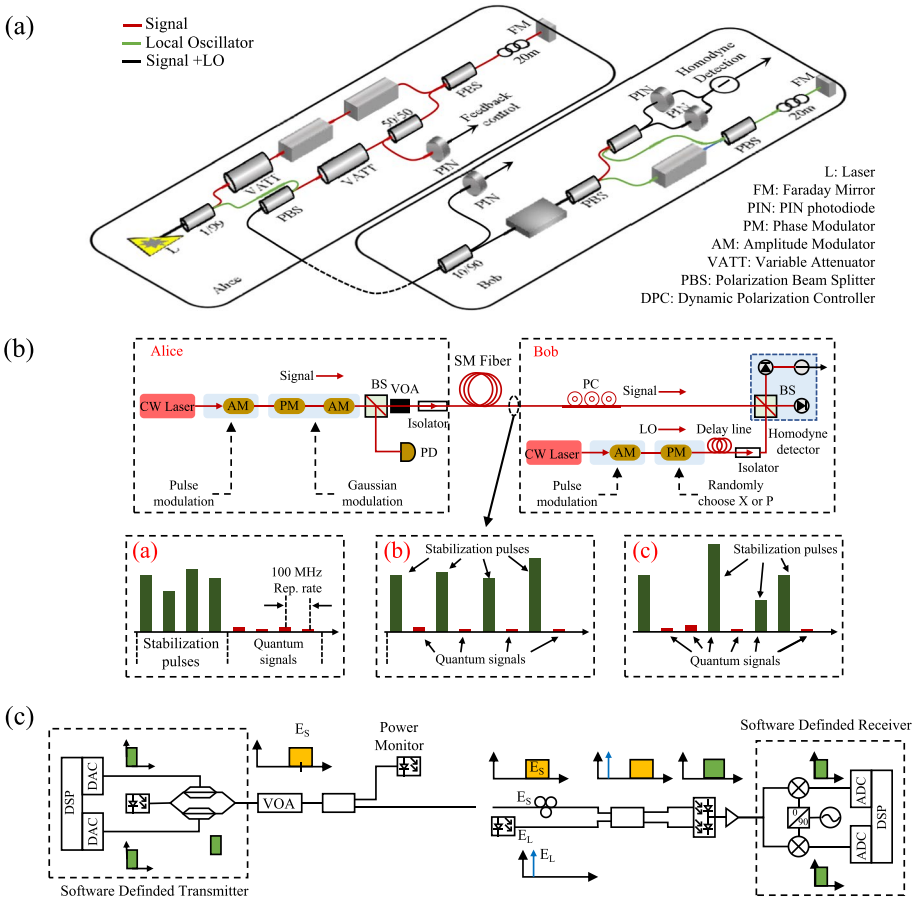

Fig. 4 Some real instances of CV-QKD. This figure was re-drawn from Zhang et al. (2024)

is used to eliminate the change in polarization state, the PIN photodiode (PIN) converts the optical signal into an electrical signal, the phase modulator (PM) and the amplitude modulator (AM) modulate the phase and amplitude of the optical signal respectively, the variable attenuator (VATT) is used to adjust the intensity of the optical signal, and the polarization beam splitter (PBS) and the dynamic polarization controller (DPC) are used to control the polarization state of the optical signal. These components work together to ensure that the optical signal remains stable during transmission, which is suitable for quantum communication or fiber-optic communication systems.

Example (c) Signal reception and processing are implemented through software. Unlike traditional hardware receivers, software-defined receivers use digital signal processing technology to flexibly process different communication protocols and signal formats through programming. This type of receiver usually consists of an RF front end, an analog-to-digital converter (ADC), and a digital signal processor (DSP). The RF front end is responsible for receiving signals, the ADC converts analog signals into digital signals, and the DSP demodulates, decodes, and otherwise processes the signals through software algorithms. Software-defined receivers are highly flexible and configurable, and are

suitable for a variety of communication systems, especially in scenarios that require rapid adaptation to new protocols or signal formats.

All three examples above involve modulation, transmission, and processing of signals. Whether by mixing signals with LO, modulating optical signals using optical components, or processing signals through software-defined receivers, their goal is to achieve effective control and utilization of signals. These technologies all play a key role in communication systems, especially in scenarios that require high precision and high flexibility, such as quantum communications or modern wireless communication systems. Nevertheless, their specific implementation methods and application scenarios are different. Example (a) focuses on the frequency conversion of electrical signals, example (b) focuses on the modulation and control of optical signals, and example (c) implements signal reception and processing through software. Examples (a) and (b) rely more on hardware components, while example (c) relies on software algorithms and digital signal processing techniques. In addition, examples (a) and (c) can be applied to a wide range of communication systems, while example (b) is more suitable for optical or quantum communication systems.

3.4 QKD and network

The integration of quantum key distribution (QKD) networks and classical networks is an important research direction in the current field of quantum communication. From the perspective of network architecture, the integration of QKD networks and classical networks is mainly reflected in how to achieve a secure distribution of quantum keys on the existing classical communication infrastructure while ensuring the collaborative work of the two networks. First, QKD networks usually require dedicated quantum channels to transmit quantum states, while classical networks rely on optical fibers or wireless channels to transmit classical information. In order to achieve the integration of the two, a common architecture is to share the same optical fiber infrastructure with the QKD network and the classical network, and transmit quantum signals and classical signals in the same optical fiber through wavelength division multiplexing (WDM) technology. For example, the team at the University of Tokyo successfully realized the co-fiber transmission of QKD and classical communications in 2017. The experiment showed that under appropriate power control, quantum signals and classical signals can coexist in the same optical fiber without significant interference Wang et al. (2017).

Secondly, the integration of QKD networks and classical networks is also reflected in the coordination of key management and distribution. Classical networks usually use public key encryption algorithms (such as RSA or ECC) for key exchange, while QKD networks use the principles of quantum mechanics to achieve unconditionally secure key distribution. In order to combine the two, researchers proposed a hybrid key distribution architecture, in which the keys generated by QKD are used to encrypt key data in the classical network, while the classical network is responsible for key management and distribution. For example, the European SECOQC project demonstrated a QKD-based hybrid key distribution network in 2008, which combined QKD-generated keys with classical key management systems to achieve large-scale secure communications Peev et al. (2009). In recent years, the hybrid key distribution architecture has been further optimized.

Finally, the integration of QKD networks and classical networks also needs to solve the compatibility problem of network topology. Classical networks usually adopt hierarchical or distributed topologies, while QKD networks usually adopt point-to-point or star topologies due to their physical limitations. In order to integrate QKD in classical

networks, researchers proposed a QKD network architecture based on trusted relays, in which nodes in the classical network can serve as trusted relays to expand the coverage of the QKD network. For example, a team from the University of Science and Technology of China successfully implemented a QKD network based on trusted relays in 2016, which achieved quantum key distribution over 400 kms through trusted nodes in the classical network Yin et al. (2017).In summary, the integration of QKD networks and classical networks has made important progress in the physical layer, key management layer, and network topology layer, laying the foundation for the development of the future quantum Internet.

4 Evaluating quantum cryptography for IoT security

In this section, we will explore the challenges associated with implementing quantum cryptography on IoT devices after comparing quantum and traditional cryptography. Detailed scientific problems will be presented. While analyzing theoretic issues, we manage to uncover practical challenges that may arise when applying quantum cryptography to IoT devices. Based on these discussions, the feasibility of quantum cryptography for IoT security can be assessed.

4.1 Differences between quantum and traditional cryptography

There are significant differences between quantum cryptography (QKD) and traditional cryptography (such as RSA and AES) in terms of security, performance, deployment, technical complexity, and application scenarios. The two are compared in Table 5 in different dimensions. Quantum cryptography is based on the principles of quantum mechanics, has unconditional security and real-time eavesdropping detection capabilities, and can completely resist quantum computing attacks. However, its key generation rate is low, the transmission distance is limited, the real-time performance is poor, and the deployment cost is high. It requires dedicated hardware and independent quantum network infrastructure, and the technical implementation is complex, and it has poor compatibility with the existing Internet of Things. In contrast, traditional encryption technology relies on the computational complexity of mathematical problems. Although RSA is vulnerable to quantum computing attacks, AES can partially resist quantum threats by increasing the key length. In addition, traditional encryption technology is efficient, low-cost, easy to deploy, and has a mature ecosystem, which is suitable for large-scale Internet of Things and resource-constrained devices. In the future, the development direction of quantum cryptography includes reducing costs, extending transmission distances, and hybrid encryption schemes combined with post-quantum cryptography (PQC) (Xu et al. 2024), while traditional encryption technology is committed to scheme designing (Chen et al. 2024), protocol optimization (Wang et al. 2023), and hardware acceleration (He et al. 2025). In general, quantum cryptography has potential in high-security scenarios, but its widespread application still needs to overcome challenges such as performance, cost, and compatibility, while traditional encryption technology needs to further improve security to cope with the threats of the quantum computing era. The two can complement each other to achieve a more comprehensive security solution.

Table 5 The comparison between quantum and traditional cryptography

Dimensions	Quantum cryptography (QKD)	Traditional cryptography (RSA & AES)
Security	Based on quantum mechanics, unconditionally secure; Real-time eavesdropping detection; Resistant to quantum attacks	Relies on computational complexity of mathematical problems; Vulnerable to quantum attacks; AES requires key lengthening for quantum resistance
Performance	Low key generation rate; Limited transmission distance; Poor real-time performance	High efficiency, fast key generation and encryption; No distance limitation; Suitable for high-throughput scenarios
Deployment	High cost; Requires standalone quantum network	Low cost; Easily integrated into existing networks
Technique	Complex implementation, requires expertise; Poor compatibility with IoT infrastructure	Mature technology, easy to develop and maintain; Extensive support libraries and standardized protocols
Applications	High-security scenarios; Small-scale private networks	Large-scale IoT; Resource-constrained devices; Future quantum internet
Development	Chip-based, integrated photonics to reduce costs; Satellite QKD for extended distance; Hybrid encryption schemes	Post-Quantum Cryptography (PQC) development; Hardware acceleration (GPU, TPU) for performance optimization

4.2 IoT security challenges and quantum solutions

IoT devices are inherently vulnerable to attacks majorly due to their limited computational resources, long lifecycle (often exceeding a decade) Han et al. (2024), and reliance on classical cryptographic algorithms such as RSA and ECC, which are susceptible to quantum computing attacks Ataullah and Chauhan (2024); Reshi and Sholla (2024). For example, Shor's algorithm Politi et al. (2009); de Lima Marquezino et al. (2019) could break RSA-2048 in seconds using a quantum computer with 4099 logical qubits, posing a critical threat to IoT systems handling sensitive data. Quantum cryptography, particularly Quantum Key Distribution (QKD), offers a promising solution by leveraging quantum mechanics to detect eavesdropping attempts and ensure information-theoretic security. Hybrid approaches combining QKD with post-quantum cryptography (PQC) are emerging as a practical strategy to future-proof IoT security, balancing quantum-resistant algorithms like configurable lattice-based ML-KEM Kim et al. (2024); Xu et al. (2025) with quantum-enhanced key distribution.

While guaranteeing the theoretic security of quantum solutions for IoT devices, there can be extra challenges in practical implementations. For instance, while it is possible to guarantee theoretical security by mathematic proof, real-life implementations require more attention to IoT devices. This includes considerations such as limited computational resources, potential hardware vulnerabilities Van Schaik et al. (2024), and the need for efficient and secure communication protocols tailored to IoT environments.

4.3 IoT-specific limitations of QKD

No practical implementations of quantum cryptography schemes are absolutely perfect. The performance of the schemes depends on the applicability of the security proofs like mathematic proofs and assumptions to the real devices. Generally speaking, based on their security proofs, quantum hacking encompasses all attacks in which an eavesdropper is allowed to gain more information about messages sent between the trusted parties than those assumed to be the case. As security proofs were constructed on physical principles, it only makes sense when one or more of the assumptions required by the security proof are held. Meanwhile, Eve might be able to gain more information about the message than Alice and Bob. These assumptions included the existence of an authenticated channel between Alice and Bob, including the isolation of the trusted devices. The devices were expected to perform in that way. In addition, certain forms of quantum hacking had already been mentioned in this review, i.e., the PNS attack against DV-QKD protocols. Exploitable imperfections in the trusted parties' devices made it possible to perform quantum hacking based on side channels. These could be dangerous within the trusted devices that might contribute to Eve's information about the signal. Moreover, added noise within the devices could be partially controlled by Eve, who would like to influence the key data. The partially controllable losses and noises threatened the security of QKD protocols if overlooked. Usually, quantum hacking serves two purposes: to gain information about the secret key directly or to disguise other attacks on a protocol by altering the trusted parties' estimation of the channel properties. The trusted parties could either incorporate the side channels into their security analysis so as not to underestimate Eve's information or modify their protocol to include countermeasures.

While QKD provides robust security, its integration into IoT faces technical hurdles. Most IoT devices operate under constraints such as low power budgets, limited processing capabilities, and cost sensitivity Kurte et al. (2025). Current QKD implementations require specialized hardware (like single-photon detectors) and stable quantum channels, which are incompatible with resource-constrained IoT nodes. Recent advancements aim to address these issues through miniaturized quantum components and hybrid networks. For instance, quantum random number generators (QRNGs) can be embedded in IoT chips to generate unique encryption keys, enhancing resistance against brute-force attacks de Curtò et al. (2024). Additionally, satellite-based QKD enables long-distance secure communication for IoT infrastructure, though challenges like high latency and cost remain.

4.4 QKD attacks in IoT context

Side Channel Attacks. APD-based detectors sometimes emit light when they detect a pulse, which is known as a backflash. The flashback light can inform Eve about Bob's measurements in several ways. On the one hand, the polarization of the backlash can indicate which components of Bob's system it passed through, which can tell Eve which detector it came from. On the other hand, what can also provide Eve with this information is the propagation time of the backlash after entering Bob's detector and the difference in the outgoing light profile Path-related changes. This can tell Eve which measurement base Bob has chosen, and for some detector settings, it can even reveal Bob's measurements. Some scholars Pinheiro et al. (2018) have tested commercially used InGaAs/InP APDs from two aspects and found that anti-flash can be detected in a large proportion of avalanche events. Building on this work by characterizing commercial Si APDs, they also found that the flashback probability was significant ($\geqslant 0.065$). Related studies have also found that backlash is broadband and can, therefore, be reduced using spectral filters. Using photomultiplier tubes instead of APDs in Bob's detectors solved this attack well. In the future, quantum-based semantic security may be needed. How to make sure the communication security and the channel security without decrypting or even reading secret messages is worth studying.

Compared with the original communication requirement, the 5th generation (5 G)-enabled IoT connects billions of devices for high-speed data transfer nowadays. Therefore, it is necessary to update the communication routines to meet the requirements of high-speed transfer. To enhance its security and prevent side-channel attacks, quantum cryptography has been studied with attention to the routines. Chawla and Mehra (2023) summarized the quantum cryptography routine from a classical one to a post-quantum-based one. To prevent the side channel attack in high-speed transfer, Shaller et al. (2023) made plans to standardize and transition from conventional cryptography to post-quantum cryptography. Mujdei et al. (2024) followed their plans to design a new routine, which reduced the complexity of polynomial multiplication. They accomplished the implementation by applying lattice to post-quantum cryptography. In traditional lattice ciphers, encryption and decryption operations require a large number of matrix operations and vector operations including matrix multiplication, vector addition, and vector multiplication. The complexity of these operations is high, making traditional lattice passwords more time-consuming and inefficient in practical applications. Nonetheless, it is easy for lattice to accomplish these operations. Consequently, introducing post-lattice quantum cryptography can reduce the complexity to the polynomial level.

Fake Status. The false status and detector efficiency do not match the BB84 and most DV protocols since its security is based on the fact that Eve and Bob's choices are independent. If Eve can exploit some flaw in Bob's device so that it affects Bob's choice or even chooses it for him, then this independence would no longer exist, and the security of the protocol could be broken. A paper Makarov and Hjelme (2005) proposed several schemes that allow an eavesdropper to control or influence Bob's detector bases or measurements. That's where Eve doesn't try to get information without disturbing the signal state. Instead, sending a state designed to exploit Bob to detect a flaw in the device can give him the results she wants him to receive. However, the problem was mainly manifested in the adaptation of the IoT. If future smart devices can provide an interface based on quantum cryptography to eliminate false states when they leave the factory, the problem will be easily solved.

4.5 CV-QKD attacks in IoT context

Attacks on Local Oscillator. Assuming that to measure Alice's signal state, Bob perturbs them with a local oscillator (LO), implementations of CV-QKD typically send the LO over a quantum channel due to the difficulty of maintaining coherence between Alice's source and Bob's LO. Since CV-QKD's security proof does not consider this (since, theoretically, there is no need to send LO over the channel), this left some side channels that Eve could exploit. Scholars indicated that the strength of the LO must be monitored to prevent Eve from replacing the signal state and LO with the compressed state, masquerading as intercept and retransmit attacks by reducing trusted party-related errors that would expect such an attack. A beamsplitter-based wavelength-dependent attack on the LO was proposed. By exploiting the wavelength dependence of the beamsplitter in Bob's device, they found they could engineer Bob's results while preventing Bob from being accurately determined. They proposed a countermeasure in which wavelength filters were randomly applied, and any differences in channel characteristics between the applied and unapplied cases were monitored. Another attack on LO was designed by Jouguet et al. (2013), which exploited the fact that an LO pulse triggers Bob's clock. By changing the shape of the LO pulse, Eve can delay the triggering of the clock. This could cause Bob to miscalculate shot noise, allowing Eve to perform an intercept and resend attack undetected. As a countermeasure, It was suggested that Bob measure shot noise in real-time by randomly applying strong attenuation to the signal. Based on this, Huang et al. (2014) showed that an attack exploiting the wavelength dependence of the beam splitter can be used to defeat Bob's attempts to measure shot noise in real time. However, they found that adding a third decay value to the strong decay (rather than just turning it on or off) can prevent their attack. Xie et al. also found that jitter effects in the clock signal lead to incorrect calculation of shot noise. To completely prevent LO attacks, Qi et al. (2015) and Soh et al. (2015) proposed and analyzed a method for Bob to generate LO locally. Alice sent phase reference pulses periodically, and Bob applied phase rotation to their results during post-processing to ensure they were the same as Alice's source. This scheme was modified by Marie and Alléaume (2017) to reduce phase noise. Ren et al. (2019) suggested that even the local LO may be vulnerable to hacking if the trusted party assumes that the phase noise is credible and Eve cannot be used. In this case, Eve can reduce the phase noise by increasing the strength of the phase reference pulse and compensate for the reduced phase noise by increasing her attack on the signal state so that the total noise measured by Bob remains the same.

To prevent Eve's attacks, Bob should check whether the messages sent from Alice are complete. As the secret messages on the local oscillators must disappear after they are read, no matter whether the readers decrypt them successfully or not, Bob can find out that something is missing if Eve attacks the local oscillators. In most cases, the communication is safe. Nonetheless, if Eve always performs attacks, the communication between Alice and Bob may always be unavailable. This remains an issue to be addressed in the future.

Saturation Attacks on Detectors. Let us consider a saturation attack on Bob's homodyne detector. This attack exploits the fact that the CV-QKD security proof assumes a linear relationship between the incident photon quadrature and the measurement (the quadrature value corresponds linearly to the measurement), but in reality, homodyne detectors have limited linear range. Above a certain quadrature value, the homodyne detector will saturate, which means that the measurement will be the same whether the quadrature value is at or above the threshold level. For example, a quadrature value of 100 shot noise can give the same measurement results as a quadrature value of 200 shot noise. Qin et al. (2016) considered taking advantage of this by using an intercept and resend attack, then rescaling and permuting the measured states (multiplying them by some factor, then adding a constant displacement to them). By partially overlapping Bob's measurements with the saturation region, Eve can alter the distribution of measurements, thereby reducing false estimates by trusted parties. Countermeasures were also proposed Qin et al. (2016), including using a Gaussian post-selection filter Fiurášek and Cerf (2012) to ensure that the measurements used for key generation fall within the linear range of the detector and using random attenuation of Bob's signal to test whether the measurements were correct. Linearly related to the input. Qin et al. (2018) extended their previous work to consider a slightly different attack in which an incoherent laser was used to shift Bob's measurements into the saturation range.

Attacks on detectors mainly focus on obfuscating channel information. By changing the lengths of some line segments of the whole channels, the detectors may give incorrect judgments. In this way, Quantum cryptography users are recommended to maintain their channels and notes more often.

4.6 DV-QKD attacks in IoT context

Malicious Software Attacks. Malicious software attack includes computer virus and Trojan Horses. A kind of hacking that can be used against the DV-QKD protocol is the Trojan Horses Gisin et al. (2006); Deng et al. (2005); Jain et al. (2014), which includes a variety of different types of attacks that involve sending a quantum system into the devices of one or two trusted parties to obtain information. In BB84 and B92, the use of large photon pulses to obtain information about the basis of Alice's selection and the measurement basis of Bob's selection was considered. This information was obtained by sending a photon pulse through the main channel to a trusted device and measuring the reflection. Given that qubits were encoded by phase shifting, if Eve can pass her pulse through Alice's phase modulator, measuring the resulting pulse will provide some information about the state of the signal. It is possible because Alice's phase modulator ran for a finite amount of time (instead of just running long enough to modulate the signal state), giving Eve a window to send her own pulses, similar to modulating signal state or signal pulse. Gisin et al. (2006) described in detail the process by which Eve obtained information about base selection through reflectometry. The information might be partial, giving only the basis for use, or it may give the key bits directly. Even when only the

base can be obtained, the security of the protocol will still compromised because Eve is now able to always choose the same measurement base as Alice for interception and retransmission attacks and obtain complete information about the key without introducing any errors. Alternatively, Eve could be able to target Bob's device. For B92 or SARG04, it is sufficient to know Bob's measurement basis to obtain complete information about the key. In BB84, if Eve can determine the measurement base that Bob will use before the signal state reaches his device, she can perform an undetectable intercept and retransmit attack by choosing the same base as he. In IoT, even if Eve only gets information about Bob's basis after measuring the state of the signal, it helps in practical PNS attacks because it reduces the need for quantum memory (Eve can measure photons and receive them immediately without waiting until all CCs are done. This won't help eavesdroppers who are only limited by the laws of physics, but it can help people with current technology. To prevent malicious software attacks, some network security schemes, local programmable malware detection frameworks, and malicious software detection techniques are required. It is worth combining them with quantum cryptography.

4.7 Combination with blockchains

Blockchains were first proposed in 2008 by an anonymous person or group of people using the pseudonym Satoshi Nakamoto Nakamoto (2008). For 17 years, blockchains have been playing an increasingly important role in cryptography. The recent period has witnessed the combination of quantum cryptography and blockchains arise Cherbal et al. (2024). Therefore, it is necessary to introduce this combination here.

Blockchains are decentralized and distributed digital ledgers that use cryptography to secure and verify transactions. They allow multiple parties to access and update the same information in a secure and transparent manner, without the need for a central authority or intermediary. The storage of blockchains can be regarded as a linked table. When a transaction is updated, a new block is added to the blockchain that contains the updated transaction. This new block is linked to the previous block in the chain, creating a chain of blocks that cannot be altered without breaking the entire chain. Meanwhile, when a block is modified, the following blocks will be updated accordingly. Each block contains a cryptographic hash of the previous block in the chain, which serves as a unique identifier for that block and ensures that any attempt to alter or delete a block would be immediately detected by the rest of the network. The "51% principle" refers to the idea that a blockchain network is secure as long as at least 51% of the network's computing power (or hash rate) is controlled by honest nodes. The consensus algorithm used by most blockchains, such as Proof of Work (PoW) or Proof of Stake (PoS), requires a majority of nodes to agree on the validity of transactions and new blocks in order for them to be added to the blockchain. If a group of malicious nodes controls less than 51% of the network's computing power, they will not be able to successfully carry out an attack due to the "51% principle".

Based on the security analysis mentioned above, it is possible to use blockchains and quantum cryptography to protect IoT devices at the same time. Generally speaking, blockchains protect IoT devices from a holistic perspective. Quantum cryptography focuses on the detailed data stored on the IoT devices. Sharma et al. (2023) presented the QIoTChain, which is capable of preventing attackers and data leaking. Blockchains can provide integrity and reliability, making it used to protect the whole system from a general aspect. Quantum cryptography can enhance the confidentiality of IoT data. This protected the data from a detailed aspect. Irshad et al. (2023) aimed to protect the cloud IoT devices.

With the reliability of blockchains, a novel cloud computing architecture was proposed to solve the scalability of IoT devices, which is a challenging scientific problem. This architecture enhanced the reliability, security, and scalability of IoT devices on the cloud by combining blockchains and post-quantum cryptography. Dhar et al. (2024) focused on the security of media stored on IoT devices, where hash functions of blockchains were used to augment the overall security posture whilst QKD of quantum cryptography facilitated secure key exchange between involved parties to encrypt and decrypt data by harnessing the principles of quantum mechanics.

5 Discussion and future work

The support of quantum cryptography for IoT security also has certain limitations, mainly in academic and engineering aspects. The encryption and decryption algorithms of quantum cryptography do not always make sense, and it still has its own life cycle. At present, it has not been found that attackers can successfully decipher the encrypted information they intercepted with brute force to extract the passwords or the plaintext. However, it does not rule out that in the future, if a technologically large enough quantum computer is invented or a classical cracking algorithm is discovered, quantum cryptography will also become quite limited. The confidentiality of an encrypted message may have a very limited life, while the time required to break it is drastically reduced. In the future, how to develop a quantum cryptography encryption and decryption algorithm that prevents cracking by quantum computers with brute force will become a future development trend. As for IoT security, taking into account both efficiency and security will continue to be favored.

There are several variations of the quantum cryptographic protocol, including BB84. Still, the main problem in the physical implementation of these protocols is the maximum distance that can be traveled by the photons. Photons are essentially light particles, which can easily be distorted by environmental or natural calamities. As a matter of fact, the photons need to travel a very long distance in cases where the IoT networks are wide and stretch across many countries or cities. Quantum computing has a limitation in terms of its consideration. Additionally, quantum devices are currently very bulky and expensive, which can not be afforded by every organization or individual. The existing quantum key distribution (QKD) protocol is designed to work with only 2 devices. This is not possible in actual IoT systems which connect hundreds of devices together to communicate. These engineering problems will be applied and implemented after the study of quantum cryptography transitions from mathematics to physics.

The integration of quantum cryptography into IoT ecosystems represents a transformative leap in securing the interconnected world of the future. However, achieving a quantum-ready IoT landscape requires addressing several interdisciplinary challenges, including cost reduction, interoperability enhancement, and policy alignment, which form the potential research directions. On the one hand, security in both theory and practice still needs to be enforced continuously. The enforcement should be done from the low level to the application level. The essence is to guarantee that the hardware is reliable, with correct and trusted instructions executed when receiving those from higher levels. Subsequently, the trusted execution environment (TEE) should be designed to be resistant to modification Van Schaik et al. (2024). As mentioned in Sect. 4, some IoT devices often face malicious software. Thus, in the software aspect,

the execution environments should be clear, transparent, and secure. More mature and universal malware detection frameworks like GooseBt Yang et al. (2023) can be designed to guarantee the execution environments. Afterward, implement the mature quantum cryptography schemes to be resistant to attacks including quantum attacks. Under the protection of these schemes proved by mathematics, IoT devices can handle queries in secure environments.

On the other hand, we will focus on the performance. The high cost of quantum hardware, such as single-photon detectors and quantum key distribution (QKD) systems, remains a significant barrier to widespread IoT adoption. Recent advancements in chip-scale quantum components, such as silicon photonic quantum random number generators (QRNGs), offer promising pathways to lower deployment costs. For instance, China's "Quantum New Infrastructure" initiative Kania (2021, 2018) has already demonstrated the feasibility of integrating quantum technologies into existing IoT frameworks at a reduced cost.

6 Conclusion

A basic aspect of quantum cryptography is a quantum key distribution QKD, which is discussed above. The best feature in the QKD is the capability of the channel to detect the presence of an eavesdropper in the architecture of the system, which is in sharp contrast to classical algorithms for cryptography. It has been concluded that quantum computing and quantum cryptography have developed very efficiently. Many mature algorithms are an advanced version of the (QKD), like the coherent one-way (COW) QKD, which aims at amending the drawbacks of the original quantum key distribution algorithm. However, whether they are in their advanced version, to a certain extent, the quantum cryptographic algorithms fix the loopholes that cannot be solved by classical methods in the IoT. Intrusion detection is real-time. The eavesdropping problem can also be solved perfectly. It is possible to make them become a reality in commercial systems with further improvement. This literature review provides solutions for IoT security problems with quantum cryptography techniques when questioning their feasibility. If the IoT device consumption and long-distance travel security problems are resolved by quantum cryptography in the future, we can have more mature and successful IoT systems with quantum cryptography applied for security.

Acknowledgements Thanks to Prof. Tingting Song, for providing fundamental knowledge of quantum cryptography. Thanks to the editors and the anonymous reviewers for their insightful comments, which improved the quality of this paper.

Author contributions Y.Y. designed this study, investigated, and wrote the first version manuscript. Y.L. rearranged the gathered references, constructed the paper structure, and edited the manuscript. J.X. reaccomplished the experiments, gathered the experimental results, and drew the figures. Z.Z. supervised the study, directed the writing, and revised the manuscript. All authors reviewed the manuscript.

Funding There is no funding.

Declarations

Conflict of interest The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Ahmad, R., Alsmadi, I.: Machine learning approaches to iot security: a systematic literature review. Internet Things **14**, 100365, 1–42 (2021)

Al-Garadi, M.A., Mohamed, A., Al-Ali, A.K., Du, X., Ali, I., Guizani, M.: A survey of machine and deep learning methods for internet of things (iot) security. IEEE Commun. Surv. Tutor. **22**(3), 1646–1685 (2020)

Aman, M.N., Basheer, M.H., Sikdar, B.: Two-factor authentication for iot with location information. IEEE Internet Things J. **6**(2), 3335–3351 (2018)

Amanullah, M.A., Habeeb, R.A.A., Nasaruddin, F.H., Gani, A., Ahmed, E., Nainar, A.S.M., Akim, N.M., Imran, M.: Deep learning and big data technologies for iot security. Comput. Commun. **151**, 495–517 (2020)

Arnon-Friedman, R., Dupuis, F., Fawzi, O., Renner, R., Vidick, T.: Practical device-independent quantum cryptography via entropy accumulation. Nat. Commun. **9**(1), 1–11 (2018)

Arseni, Ş.C., Miţoi, M., Vulpe, A.: Pass-iot: A platform for studying security, privacy and trust in iot. In: 2016 International conference on communications (COMM). pp. 261–266. IEEE (2016)

Ataullah, M., Chauhan, N.: Exploring security and privacy enhancement technologies in the internet of things: a comprehensive review. Secur. Priv. **7**(6), e448 (2024)

Atlam, H.F., Wills, G.B.: Iot security, privacy, safety and ethics. In: Digital twin technologies and smart cities, pp. 123–149. Springer (2020)

Aversano, L., Bernardi, M.L., Cimitile, M., Pecori, R.: A systematic review on deep learning approaches for iot security. Comput. Sci. Rev. **40**, 100389 (2021)

Balygin, K., Klimov, A., Bobrov, I., Kravtsov, K., Kulik, S., Molotkov, S.: Inherent security of phase coding quantum key distribution systems against detector blinding attacks. Laser Phys. Lett. **15**(9), 095203 (2018)

Bartlett, S.D., Sanders, B.C., Braunstein, S.L., Nemoto, K.: Efficient classical simulation of continuous variable quantum information processes. Phys. Rev. Lett. **88**(9), 097904 (2002)

Belin, A., Lewkowycz, A., Sárosi, G.: The boundary dual of the bulk symplectic form. Phys. Lett. B **789**, 71–75 (2019)

Benenti, G., Casati, G., Rossini, D., Strini, G.: Principles of quantum computation and information: a comprehensive textbook. World Scientific, Singapore (2019)

Bennett, C.H., Brassard, G., Breidbart, S., Wiesner, S.: Quantum cryptography, or unforgeable subway tokens. In: Advances in Cryptology. pp. 267–275. Springer (1983)

Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing[J]. Theor. Comput. Sci. **560**, 7–11 (2014)

Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental quantum cryptography. J. Cryptol. **5**(1), 3–28 (1992)

Bennett, C.H., Brassard, G., Ekert, A.K.: Quantum cryptography. Sci. Am. **267**(4), 50–57 (1992)

Bhatia, V., Ramkumar, K.: An efficient quantum computing technique for cracking rsa using shor's algorithm. In: 2020 IEEE 5th international conference on computing communication and automation (ICCCA). pp. 89–94. IEEE (2020)

Bhatt, A.P., Sharma, A.: Quantum cryptography for internet of things security. J. Electron. Sci. Technol. **17**(3), 213–220 (2019)

Borregaard, J., Sørensen, A.S., Lodahl, P.: Quantum networks with deterministic spin-photon interfaces. Adv. Quantum Technol. **2**(5–6), 1800091 (2019)

Brassard, G.: Brief history of quantum cryptography: A personal perspective. In: IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005. pp. 19–23. IEEE (2005)

Brown, P., Fawzi, H., Fawzi, O.: Device-independent lower bounds on the conditional von neumann entropy. Quantum 2024, **8**, 1445 (2024)

Busch, P., Heinonen, T., Lahti, P.: Heisenberg's uncertainty principle. Phys. Rep. **452**(6), 155–176 (2007)
Cao, Y., Li, Y.H., Yang, K.X., Jiang, Y.F., Li, S.L., Hu, X.L., Abulizi, M., Li, C.L., Zhang, W., Sun, Q.C., et al.: Long-distance free-space measurement-device-independent quantum key distribution. Phys. Rev. Lett. **125**(26), 260503 (2020)
Chawla, D., Mehra, P.S.: A roadmap from classical cryptography to post-quantum resistant cryptography for 5g-enabled iot: Challenges, opportunities and solutions. Internet of Things p. 100950 (2023)
Chen, Y., Wu, A., Yang, Y., Xin, X., & Song, C.: Efficient verifiable cloud-assisted psi cardinality for privacy-preserving contact tracing. IEEE Transactions on Cloud Computing. **12**(1), 251–263 (2024)
Cherbal, S., Zier, A., Hebal, S., Louail, L., Annane, B.: Security in internet of things: a review on approaches based on blockchain, machine learning, cryptography, and quantum computing. J. Supercomput. **80**(3), 3738–3816 (2024)
Chernega, V.N., Man'ko, O.V., Man'ko, V.I.: Entangled qubit states and linear entropy in the probability representation of quantum mechanics. Entropy **24**(4), 527 (2022)
Clements, W.R., Renema, J.J., Eckstein, A., Valido, A.A., Lita, A., Gerrits, T., Nam, S.W., Kolthammer, W.S., Huh, J., Walmsley, I.A.: Approximating vibronic spectroscopy with imperfect quantum optics. J. Phys. B: Atomic, Mol. Opt. Phys. **51**(24), 245503 (2018)
Coles, P.J., Berta, M., Tomamichel, M., Wehner, S.: Entropic uncertainty relations and their applications. Rev. Mod. Phys. **89**(1), 015002 (2017)
Costin, A., Zaddach, J.: Iot malware: comprehensive survey, analysis framework and case studies. BlackHat USA **1**(1), 1–9 (2018)
Curty, M., Lo, H.K.: Foiling covert channels and malicious classical post-processing units in quantum key distribution. npj Quantum Inf. **5**(1), 1–11 (2019)
Dai, H.N., Zheng, Z., Zhang, Y.: Blockchain for internet of things: a survey. IEEE Internet Things J. **6**(5), 8076–8094 (2019)
de Curtò, J., de Zarzà, I., Cano, J.C., Calafate, C.T.: Enhancing communication security in drones using qrng in frequency hopping spread spectrum. Future Internet **16**(11), 412 (2024)
de Lima Marquezino, F., Portugal, R., Lavor, C.: Shor's algorithm for integer factorization. In: A primer on quantum computing, pp. 57–77. Springer (2019)
Deng, F.G., Li, X.H., Zhou, H.Y., Zhang, Z.J.: Improving the security of multiparty quantum secret sharing against trojan horse attack. Phys. Rev. A **72**(4), 044302 (2005)
Deogirikar, J., Vidhate, A.: Security attacks in iot: A survey. In: 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC). pp. 32–37. IEEE (2017)
Dhar, S., Khare, A., Dwivedi, A.D., Singh, R.: Securing iot devices: a novel approach using blockchain and quantum cryptography. Internet Things **25**, 101019 (2024)
Donno, M.D., Dragoni, N., Giaretta, A., Mazzara, M.: Antibiotic: protecting iot devices against ddos attacks. In: International Conference in Software Engineering for Defence Applications. pp. 59–72. Springer (2016)
Ekert, A., Jozsa, R.: Quantum computation and shor's factoring algorithm. Rev. Mod. Phys. **68**(3), 733 (1996)
Ellis, D., Stevenson, R., Young, R., Shields, A., Atkinson, P., Ritchie, D.: Control of fine-structure splitting of individual inas quantum dots by rapid thermal annealing. Appl. Phys. Lett. **90**(1), 011907 (2007)
Erhard, M., Krenn, M., Zeilinger, A.: Advances in high-dimensional quantum entanglement. Nat. Rev. Phys. **2**(7), 365–381 (2020)
Fang, H., Qi, A., Wang, X.: Fast authentication and progressive authorization in large-scale iot: How to leverage ai for security enhancement. IEEE Netw. **34**(3), 24–29 (2020)
Fedorov, M.: Entanglement of multiphoton states in polarization and quadrature variables. Laser Phys. **29**(12), 124006 (2019)
Feynman, R.P., et al.: Simulating physics with computers. Int. j. Theor. phys **21**(6/7) (1982)
Fischer, A.: Limiting uncertainty relations in laser-based measurements of position and velocity due to quantum shot noise. Entropy **21**(3), 264 (2019)
Fiurášek, J., Cerf, N.J.: Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. Phys. Rev. A **86**(6), 060302 (2012)
Gisin, N., Ribordy, G., Tittel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**(1), 145 (2002)
Gisin, N., Fasel, S., Kraus, B., Zbinden, H., Ribordy, G.: Trojan-horse attacks on quantum-key-distribution systems. Phys. Rev. A **73**(2), 022320 (2006)
Grosshans, F., Cerf, N.J.: Continuous-variable quantum cryptography is secure against non-gaussian attacks. Phys. Rev. Lett. **92**(4), 047905 (2004)
Haight, D.F.: Logging into a universal quantum computer: a novel way to construct the fibonacci sequence and the uni-phi-cation of mathematics and physics. Recent Adv. Math. Res. Comput. Sci. **10**, 104–120 (2022)

Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Wallden, P. Advances in quantum cryptography. Advances in optics and photonics. **12**(4), 1012–1236 (2020)
Han, D., Qi, H., Wang, S., Hou, D., Wang, C.: Adaptive stepsize forward–backward pursuit and acoustic emission-based health state assessment of high-speed train bearings. Structural Health Monitoring p. 14759217241271036 (2024)
Hassan, W.H., et al.: Current research on internet of things (iot) security: a survey. Comput. Netw. **148**, 283–294 (2019)
Hassija, V., Chamola, V., Saxena, V., Jain, D., Goyal, P., Sikdar, B.: A survey on iot security: application areas, security threats, and solution architectures. IEEE Access **7**, 82721–82743 (2019)
He, X., Htoon, H., Doorn, S., Pernice, W., Pyatkov, F., Krupke, R., Jeantet, A., Chassagneux, Y., Voisin, C.: Carbon nanotubes as emerging quantum-light sources. Nat. Mater. **17**(8), 663–670 (2018)
He, P., Bao, T., Xie, J.: High-Performance instruction-set hardware accelerator for ring-binary-LWE-based lightweight PQC. IEEE Transactions on Very Large Scale Integration (VLSI) Systems (2025)
Hietarinta, J., Mase, T., Willox, R.: Algebraic entropy computations for lattice equations: Why initial value problems do matter. J. Phys. A: Math. Theor. **52**(49), 49LT01 (2019)
Horodecki, R., Horodecki, P., Horodecki, M., Horodecki, K.: Quantum entanglement. Rev. Mod. Phys. **81**(2), 865 (2009)
Huang, J.Z., Kunz-Jacques, S., Jouguet, P., Weedbrook, C., Yin, Z.Q., Wang, S., Chen, W., Guo, G.C., Han, Z.F.: Quantum hacking on quantum key distribution using homodyne detection. Phys. Rev. A **89**(3), 032304 (2014)
Hussain, F., Hussain, R., Hassan, S.A., Hossain, E.: Machine learning in iot security: current solutions and future challenges. IEEE Commun. Surv. Tutor. **22**(3), 1686–1721 (2020)
Irshad, R.R., Hussain, S., Hussain, I., Nasir, J.A., Zeb, A., Alalayah, K.M., Alattab, A.A., Yousif, A., Alwayle, I.M.: Iot-enabled secure and scalable cloud architecture for multi-user systems: A hybrid post-quantum cryptographic and blockchain based approach towards a trustworthy cloud computing. IEEE Access. 2023, **11**, 105479–105498 (2023)
Isonguyo, C.N., Oyewumi, K.J., Oyun, O.S.: Quantum information-theoretic measures for the static screened coulomb potential. Int. J. Quantum Chem. **118**(15), e25620 (2018)
Ízdemir, F., Ídemiş Ízger, Z., et al.: Rivest-shamir-adleman algorithm. In: Partially Homomorphic Encryption, pp. 37–41. Springer (2021)
Jaeger, L.: Quantum Revolution 2.0: When Nanobots and Quantum Computers Become Part of Our Everyday Lives. The Second Quantum Revolution: From Entanglement to Quantum Computing and Other Super-Technologies. Cham: Springer International Publishing, 2019: 315–328. (2019)
Jain, N., Anisimova, E., Khan, I., Makarov, V., Marquardt, C., Leuchs, G.: Trojan-horse attacks threaten the security of practical quantum cryptography. New J. Phys. **16**(12), 123030 (2014)
Jouguet, P., Kunz-Jacques, S., Diamanti, E.: Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. Phys. Rev. A **87**(6), 062313 (2013)
Kak, S.: Quantum information and entropy. Int. J. Theor. Phys. **46**(4), 860–876 (2007)
Kania, E.B.: China's quantum quandary. Military Cyber Affairs **3**(2), 10 (2018)
Kania, E.B.: China's quest for quantum advantage-strategic and defense innovation at a new frontier. J. Strategic Stud. **44**(6), 922–952 (2021)
Kassim, M.R.M.: Iot applications in smart agriculture: Issues and challenges. In: 2020 IEEE conference on open systems (ICOS). pp. 19–24. IEEE (2020)
Kearney, J.J., Perez-Delgado, C.A.: Vulnerability of blockchain technologies to quantum attacks. Array **10**, 100065 (2021)
Khanna, A., Kaur, S.: Evolution of internet of things (iot) and its significant impact in the field of precision agriculture. Comput. Electron. Agric. **157**, 218–231 (2019)
Kim, H., Jung, H., Satriawan, A., Lee, H.: A configurable ml-kem/kyber key-encapsulation hardware accelerator architecture. Express Briefs, IEEE Transactions on Circuits and Systems II. **71**(11), 4678–4682 (2024)
Ko, R., Mickens, J.: Deadbolt: Securing iot deployments. In: Proceedings of the applied networking research workshop. pp. 50–57 (2018)
Koashi, M.: Simple security proof of quantum key distribution based on complementarity. New J. Phys. **11**(4), 045018 (2009)
Kumar, S., Tiwari, P., Zymbler, M.: Internet of things is a revolutionary approach for future technology enhancement: a review. J. Big data **6**(1), 1–21 (2019)
Kumar, A., Ottaviani, C., Gill, S.S., Buyya, R.: Securing the future internet of things with post-quantum cryptography. Secur. Priv. **5**(2), e200 (2022)
Kurte, R., Salcic, Z., Kevin, I., Wang, K.: Supporting constrained devices and networks in the decentralised internet of things. Internet Things **30**, 101496 (2025)

Li, X., Yan, F., Zuo, F., Zeng, Q., Luo, L.: Touch well before use: Intuitive and secure authentication for iot devices. In: The 25th annual international conference on mobile computing and networking. pp. 1–17 (2019)
Li, S., Xu, L.D., Zhao, S.: The internet of things: a survey. Inf. Syst. Fron. **17**(2), 243–259 (2015)
Li, S., Da Xu, L., Zhao, S.: 5g internet of things: a survey. J. Ind. Inf. Integr. **10**, 1–9 (2018)
Liu, Y., Zhao, Q., Li, M.H., Guan, J.Y., Zhang, Y., Bai, B., Zhang, W., Liu, W.Z., Wu, C., Yuan, X., et al.: Device-independent quantum random-number generation. Nature **562**(7728), 548–551 (2018)
Lo, H.K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**(23), 230504 (2005)
Ma, H., Teng, J., Hu, T., Shi, P., Wang, S.: Co-communication protocol of underwater sensor networks with quantum and acoustic communication capabilities. Wirel. Pers. Commun. **113**(1), 337–347 (2020)
Magaia, N., Fonseca, R., Muhammad, K., Segundo, A.H.F.N., Neto, A.V.L., de Albuquerque, V.H.C.: Industrial internet-of-things security enhanced with deep learning approaches for smart cities. IEEE Internet Things J. **8**(8), 6393–6405 (2020)
Makarov*, V., Hjelme, D.R.: Faked states attack on quantum cryptosystems. J. Mod. Opt. **52**(5), 691–705 (2005)
Makhshari, A., Mesbah, A.: Iot bugs and development challenges. In: 2021 IEEE/ACM 43rd international conference on software engineering (ICSE). pp. 460–472. IEEE (2021)
Malina, L., Dzurenda, P., Ricci, S., Hajny, J., Srivastava, G., Matulevičius, R., Affia, A.A.O., Laurent, M., Sultan, N.H., Tang, Q.: Post-quantum era privacy protection for intelligent infrastructures. IEEE Access **9**, 36038–36077 (2021)
Manavalan, E., Jayakrishna, K.: A review of internet of things (iot) embedded sustainable supply chain for industry 4.0 requirements. Comput. Ind. Eng. **127**, 925–953 (2019)
Marie, A., Alléaume, R.: Self-coherent phase reference sharing for continuous-variable quantum key distribution. Phys. Rev. A **95**(1), 012316 (2017)
Mohanta, B.K., Jena, D., Satapathy, U., Patnaik, S.: Survey on iot security: challenges and solution using machine learning, artificial intelligence and blockchain technology. Internet Things **11**, 100227 (2020)
Mujdei, C., Wouters, L., Karmakar, A., Beckers, A., Bermudo Mera, J.M., Verbauwhede, I.: Side-channel analysis of lattice-based post-quantum cryptography: exploiting polynomial multiplication. ACM Trans. Embed. Comput. Syst. **23**(2), 1–23 (2024)
Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system. Online: https://assets.pubpub.org/d8wct41f/31611263538139.pdf. 1–9 (2008)
Nam, Y., Su, Y., Maslov, D.: Approximate quantum fourier transform with o (n log (n)) t gates. NPJ Quantum Inf. **6**(1), 1–6 (2020)
Nauman, A., Qadri, Y.A., Amjad, M., Zikria, Y.B., Afzal, M.K., Kim, S.W.: Multimedia internet of things: a comprehensive survey. IEEE Access **8**, 8202–8250 (2020)
Nawir, M., Amir, A., Yaakob, N., Lynn, O.B.: Internet of things (iot): Taxonomy of security attacks. In: 2016 3rd international conference on electronic design (ICED). pp. 321–326. IEEE (2016)
Nichols, R., Mineh, L., Rubio, J., Matthews, J.C., Knott, P.A.: Designing quantum experiments with a genetic algorithm. Quantum Sci. Technol. **4**(4), 045012 (2019)
Niu, P.H., Zhou, Z.R., Lin, Z.S., Sheng, Y.B., Yin, L.G., Long, G.L.: Measurement-device-independent quantum communication without encryption. Sci. Bull. **63**(20), 1345–1350 (2018)
Nord, J.H., Koohang, A., Paliszkiewicz, J.: The internet of things: review and theoretical framework. Expert Syst. Appl. **133**, 97–108 (2019)
Peev, M., Pacher, C., Alléaume, R., Barreiro, C., Bouda, J., Boxleitner, W., Debuisschert, T., Diamanti, E., Dianati, M., Dynes, J., et al.: The secoqc quantum key distribution network in vienna. New J. Phys. **11**(7), 075001 (2009)
Peng, C.Z., Zhang, J., Yang, D., Gao, W.B., Ma, H.X., Yin, H., Zeng, H.P., Yang, T., Wang, X.B., Pan, J.W.: Experimental long-distance decoy-state quantum key distribution based format on polarization encoding. Phys. Rev. Lett. **98**(1), 010505 (2007)
Peng, L.C., Wu, D., Zhong, H.S., Luo, Y.H., Li, Y., Hu, Y., Jiang, X., Chen, M.C., Li, L., Liu, N.L., et al.: Cloning of quantum entanglement. Phys. Rev. Lett. **125**(21), 210502 (2020)
Pham, Q.V., Dev, K., Maddikunta, P.K.R., Gadekallu, T.R., Huynh-The, T., et al.: Fusion of federated learning and industrial internet of things: A survey. Comp. Networks 2022, **212**, 109048 (2022)
Pinheiro, P.V.P., Chaiwongkhot, P., Sajeed, S., Horn, R.T., Bourgoin, J.P., Jennewein, T., Lütkenhaus, N., Makarov, V.: Eavesdropping and countermeasures for backflash side channel in quantum cryptography. Opt. Express **26**(16), 21020–21032 (2018)
Pirandola, S., Eisert, J., Weedbrook, C., Furusawa, A., Braunstein, S.L.: Advances in quantum teleportation. Nat. Photonics **9**(10), 641–652 (2015)

Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al.: Advances in quantum cryptography. Adv. Opt. Photonics **12**(4), 1012–1236 (2020)

Politi, A., Matthews, J.C., Obrien, J.L.: Shor's quantum factoring algorithm on a photonic chip. Science **325**(5945), 1221–1221 (2009)

Qi, B., Lougovski, P., Pooser, R., Grice, W., Bobrek, M.: Generating the local oscillator "locally'' in continuous-variable quantum key distribution based on coherent detection. Phys. Rev. X **5**(4), 041009 (2015)

Qian, X.F., Alonso, M.A., Eberly, J.H.: Entanglement polygon inequality in qubit systems. New J. Phys. **20**(6), 063012 (2018)

Qin, H., Kumar, R., Alléaume, R.: Quantum hacking: saturation attack on practical continuous-variable quantum key distribution. Phys. Rev. A **94**(1), 012325 (2016)

Qin, H., Kumar, R., Makarov, V., Alléaume, R.: Homodyne-detector-blinding attack in continuous-variable quantum key distribution. Phys. Rev. A **98**(1), 012312 (2018)

Ren, S., Kumar, R., Wonfor, A., Tang, X., Penty, R., White, I.: Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise. JOSA B **36**(3), B7–B15 (2019)

Reshi, I.A., Sholla, S.: Securing iot data: fog computing, blockchain, and tailored privacy-enhancing technologies in action. Peer-to-Peer Netw. Appl. **17**(6), 3905–3933 (2024)

Robertson, H.P.: The uncertainty principle. Phys. Rev. **34**(1), 163 (1929)

Rosenberg, D., Harrington, J.W., Rice, P.R., Hiskett, P.A., Peterson, C.G., Hughes, R.J., Lita, A.E., Nam, S.W., Nordholt, J.E.: Long-distance decoy-state quantum key distribution in optical fiber. Phys. Rev. Lett. **98**(1), 010503 (2007)

Sengupta, J., Ruj, S., Bit, S.D.: A comprehensive survey on attacks, security issues and blockchain solutions for iot and iiot. J. Netw. Comput. Appl. **149**, 102481 (2020)

Shah, T., Venkatesan, S.: Authentication of iot device and iot server using secure vaults. In: 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE). pp. 819–824. IEEE (2018)

Shaller, A., Zamir, L., Nojoumian, M.: Roadmap of post-quantum cryptography standardization: side-channel attacks and countermeasures. Inf. Comput. **295**, 105112 (2023)

Sharma, A.K., Peelam, M.S., Chauasia, B.K., Chamola, V.: Qiotchain: quantum iot-blockchain fusion for advanced data protection in industry 4.0. IET Blockchain **4**(3), 252–62 (2023)

Skosana, U., Tame, M.: Demonstration of shor's factoring algorithm for n = 21 on ibm quantum processors. Sci. Rep. **11**(1), 1–12 (2021)

Smolin, J.A., Smith, G., Vargo, A.: Oversimplifying quantum factoring. Nature **499**(7457), 163–165 (2013)

Soh, D.B., Brif, C., Coles, P.J., Lütkenhaus, N., Camacho, R.M., Urayama, J., Sarovar, M.: Self-referenced continuous-variable quantum key distribution protocol. Phys. Rev. X **5**(4), 041010 (2015)

Stav, T., Faerman, A., Maguid, E., Oren, D., Kleiner, V., Hasman, E., Segev, M.: Quantum entanglement of the spin and orbital angular momentum of photons using metamaterials. Science **361**(6407), 1101–1104 (2018)

Tahsien, S.M., Karimipour, H., Spachos, P.: Machine learning based solutions for security of internet of things (iot): a survey. J. Netw. Comput. Appl. **161**, 102630 (2020)

Uprety, A., Rawat, D.B.: Reinforcement learning for iot security: a comprehensive survey. IEEE Internet Things J. **8**(11), 8693–8706 (2020)

Van Schaik, S., Seto, A., Yurek, T., Batori, A., AlBassam, B., Genkin, D., Miller, A., Ronen, E., Yarom, Y., Garman, C.: Sok: Sgx. fail: How stuff gets exposed. In: 2024 IEEE symposium on security and privacy (SP). pp. 4143–4162. IEEE (2024)

Vedral, V.: The role of relative entropy in quantum information theory. Rev. Mod. Phys. **74**(1), 197 (2002)

Wang, H., He, Y., Li, Y.H., Su, Z.E., Li, B., Huang, H.L., Ding, X., Chen, M.C., Liu, C., Qin, J., et al.: High-efficiency multiphoton boson sampling. Nat. Photonics **11**(6), 361–365 (2017)

Wang, Y., Primaatmaja, I.W., Lavie, E., Varvitsiotis, A., Lim, C.C.W.: Characterising the correlations of prepare-and-measure quantum networks. npj Quantum Inf. **5**(1), 1–6 (2019)

Wang, X., Lin, Y., Yang, Y., Xu, H., Luo, Z.: A secure physical health test data sharing scheme based on token distribution and programmable blockchains. Comput. Commun. **209**, 444–454 (2023)

Wei, K., Li, W., Tan, H., Li, Y., Min, H., Zhang, W.J., Li, H., You, L., Wang, Z., Jiang, X., et al.: High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. Phys. Rev. X **10**(3), 031030 (2020)

Wootters, W.K., Zurek, W.H.: A single quantum cannot be cloned. Nature **299**(5886), 802–803 (1982)

Wu, K.D., Theurer, T., Xiang, G.Y., Li, C.F., Guo, G.C., Plenio, M.B., Streltsov, A.: Quantum coherence and state conversion: theory and experiment. npj Quantum Inf. **6**(1), 1–9 (2020)
Xu, S., Chen, X., Guo, Y., Yang, Y., Wang, S., Yiu, S.M., Cheng, X.: Lattice-based forward secure multi-user authenticated searchable encryption for cloud storage systems. IEEE Transactions on Computers. 1–14 (2025)
Xu, S., Cao, Y., Chen, X., Guo, Y., Yang, Y., Guo, F., & Yiu, S. M. (2024, October). Post-quantum searchable encryption supporting user-authorization for outsourced data management. In Proceedings of the 33rd ACM International Conference on Information and Knowledge Management (pp. 2702–2711).
Xu, X., Ren, J., Zhu, L., Zhang, L.: Intelligent device system of urban transportation service. In: 2019 IEEE 8th joint international information technology and artificial intelligence conference (ITAIC). pp. 1729–1732. IEEE (2019)
Yang, R.Q.: Complexity for quantum field theory states and applications to thermofield double states. Phys. Rev. D **97**(6), 066004 (2018)
Yang, Y., Lin, Y., Li, Z., Zhao, L., Yao, M., Lai, Y., Li, P.: Goosebt: a programmable malware detection framework based on process, file, registry, and com monitoring. Comput. Commun. **204**, 24–32 (2023)
Yin, J., Cao, Y., Li, Y.H., Liao, S.K., Zhang, L., Ren, J.G., Cai, W.Q., Liu, W.Y., Li, B., Dai, H., et al.: Satellite-based entanglement distribution over 1200 kilometers. Science **356**(6343), 1140–1144 (2017)
Yuan, H., Cao, Y., Kamra, A., Duine, R.A., Yan, P.: Quantum magnonics: When magnon spintronics meets quantum information science. Phys. Rep. **965**, 1–74 (2022)
Zbinden, H., Bechmann-Pasquinucci, H., Gisin, N., Ribordy, G.: Quantum cryptography. Applied Physics B: Lasers & Optics **67**(6), (1998)
Zhang, G., Haw, J.Y., Cai, H., Xu, F., Assad, S., Fitzsimons, J.F., Zhou, X., Zhang, Y., Yu, S., Wu, J., et al.: An integrated silicon photonic chip platform for continuous-variable quantum key distribution. Nat. Photonics **13**, (12), 839–842 (2019)
Zhang, Y., Bian, Y., Li, Z., Yu, S., Guo, H.: Continuous-variable quantum key distribution system: Past, present, and future. Applied Physics Reviews. **11**(1), (2024)
Zhao, Y., Qi, B., Ma, X., Lo, H.K., Qian, L.: Experimental quantum key distribution with decoy states. Phys. Rev. Lett. **96**(7), 070502 (2006)
Zheng, X., Sun, S., Mukkamala, R.R., Vatrapu, R., Ordieres-Meré, J., et al.: Accelerating health data sharing: a solution based on the internet of things and distributed ledger technologies. J. Med. Internet Res. **21**(6), e13583 (2019)
Zhou, L., Sheng, Y.B., Long, G.L.: Device-independent quantum secure direct communication against collective attacks. Sci. Bull. **65**(1), 12–20 (2020)
Zhou, Z., Sheng, Y., Niu, P., Yin, L., Long, G., Hanzo, L.: Measurement-device-independent quantum secure direct communication. Sci. China Phys., Mech. Astron. **63**(3), 1–6 (2020)