Proceedings of the 2023 International Conference on Mathematical Physics and Computational Simulation
DOI: 10.54254/2753-8818/28/20230397

Research and prospects of encryption mechanism for quantum communication

Qingyang Guo

Jinan University, 855 Xingye Avenue East, Nancun Town, Panyu District, Guangzhou City, Guangdong Province, China

guoqingyang@189.cn

Abstract. With the continuous advancement of quantum communication technology, the public's interest in quantum mechanics and quantum communication has been steadily increasing. However, due to the general level of knowledge and misleading popular science videos on the internet, there are significant misconceptions regarding the understanding of quantum mechanics and quantum communication technology. This study aims to enhance readers' understanding of this field by providing an accessible introduction to the fundamentals of quantum mechanics and quantum communication. This paper starts by elaborating on the basic concepts of quantum mechanics, such as wave function, eigenvalues and eigenfunctions of observables, and the superposition of eigenstates. Then, taking polarization of light as an example, the fundamental principles of quantum mechanics are explained. Subsequently, through the examples of the BB84 and B92 protocols, the working principles of quantum communication and its advantage of being secure against eavesdropping are explained. Finally, an overview of the current status and technological challenges faced by quantum communication technology is provided. It is our expectation that readers, after reading this paper, will enhance their understanding of the theoretical foundations of quantum mechanics and quantum communication, thereby avoiding being misled by erroneous information from the internet and real-life sources.

Keywords: quantum mechanics, polarization of light, quantum communication, BB84 protocol, B92 protocol.

1. Introduction

In today's rapidly advancing technology, the development of quantum communication technology has attracted widespread attention and research [1]. Quantum mechanics, as the foundational theory in this field, provides a new perspective for understanding and utilizing the microscopic world with its unique theoretical structure and predictive capabilities [2]. However, despite the increasing importance of quantum communication technology, there remains significant confusion among the general public regarding this field. This is mainly due to two reasons: first, the theoretical foundations of quantum mechanics and quantum communication technology are relatively complex and require a certain level of expertise to comprehend; second, the internet is filled with numerous misleading popular science videos that oversimplify or misunderstand the true meanings of quantum mechanics and quantum communication technology, leading to public misconceptions [3].

To address this issue, this paper aims to introduce the fundamentals of quantum mechanics and

DOI: 10.54254/2753-8818/28/20230397

quantum communication to the readers in an accessible manner, thereby improving the public's understanding of this field. We will start with the basic knowledge of quantum mechanics, introducing concepts such as wave function, eigenvalues and eigenfunctions of observables, and the superposition of eigenstates. Then, we will use the polarization of light as an example to explain the fundamental principles of quantum mechanics in detail. Next, through the examples of the BB84 and B92 protocols, we will demonstrate the working principles of quantum communication and its inherent advantage of being secure against eavesdropping. Finally, we will present an overview of the current status of quantum communication technology and the technological challenges it faces.

The paper is divided into six sections. Section 2 primarily discusses relevant knowledge of quantum mechanics and corrects misconceptions widely spread on the internet. This section covers topics such as wave functions, eigenvalues and eigenfunctions of observables in quantum mechanics, as well as the meaning and role of observation in quantum mechanics. Section 3 provides a detailed introduction to the phenomenon of light polarization and its explanation in the context of quantum mechanics. Subsequently, Section 4 uses the popular science examples of the BB84 and B92 protocols to explain the secure nature of quantum communication technology. Section 5 explains the current status of quantum communication technology development and the challenges faced by researchers. Finally, Section 6 summarizes the entire paper, discusses its limitations, and suggests future research directions.

2. Knowledge of quantum mechanics

In the process of studying quantum communication technology, understanding the basic concepts and principles of quantum mechanics is crucial for comprehending and explaining related optical phenomena. Therefore, a grasp and in-depth understanding of quantum mechanics knowledge become essential elements in understanding quantum communication technology. By studying concepts such as wave functions, measurements, superposition principles, and eigenvalues in quantum mechanics, the theoretical foundations behind quantum communication technology can be revealed, providing strong support for the research and application of quantum communication technology [4].

2.1. Wave functions

In quantum mechanics, the wave function φ(x) is commonly used to describe the probability of a particle appearing at a position x in one-dimensional coordinates. The probability of the particle appearing at x is given by:

$$P(x) = |\varphi(x)|^2 = \varphi^*(x)\varphi(x) \tag{1}$$

where $\varphi^*(x)$ is the complex conjugate of φ(x). The wave function is obtained by solving the Schrödinger equation:

$$(-\frac{\hbar^2}{2\mu}\frac{d^2}{dx^2} + V(x))\varphi(x,t) = i\hbar\frac{d}{dt}\varphi(x,t) \tag{2}$$

where ħ is the reduced Planck's constant, V(x) is the potential field in which the particle exists.

Wave functions of other continuous observables can also be expressed in a similar form. For example, the momentum wave function (φ(p)) represents the probability of observing a value p for momentum:

$$P(p) = |\varphi(p)|^2 = \varphi^*(p)\varphi(p) \tag{3}$$

2.2. State vectors

Each physical state can be represented by a vector $|\varphi\rangle$ in the Hilbert space. These vectors, also known as ket vectors, represent the physical states in the Hilbert space [5]. State vectors have different forms in different representations, such as in the coordinate representation:

$$\varphi(x) = \langle x|\varphi\rangle \tag{4}$$

where the bra vector represents the choice of the coordinate representation.

DOI: 10.54254/2753-8818/28/20230397

2.3. Physical quantities

A physical quantity refers to the attribute or property that describes a physical phenomenon in physics and can be quantitatively described using physical measurements.

(1) Representation of Physical Quantities with Operators

In quantum mechanics, physical quantities are represented by operators. For example, the momentum operator in the position representation is given by:

$$\hat{p} = -i\hbar\frac{d}{dx} \tag{5}$$

and the Hamiltonian operator is:

$$\hat{H} = i\hbar\frac{d}{dt} \tag{6}$$

For discrete physical quantities, the corresponding operators are usually in matrix form. For instance, the x-component of angular momentum, $\hat{L}_x$, in the $\hat{L}_z$ representation is:

$$\hat{L}_x = \frac{\hbar}{\sqrt{2}}\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \tag{7}$$

(2) Properties of Physical Quantity Operators

All physical quantity operators are Hermitian operators. For a physical quantity operator A, it always satisfies:

$$\langle\varphi_m|\hat{A}|\varphi_n\rangle = \langle\varphi_n|\hat{A}^*|\varphi_m\rangle \tag{8}$$

The form of physical quantities varies in different representations. For example, the momentum operator p in the position representation is:

$$p = -i\hbar\frac{d}{dx} \tag{9}$$

but in the momentum representation, it is represented as:

$$\hat{p} = p \tag{10}$$

This applies to discrete physical quantities as well. The form of $\hat{L}_x$ in the $\hat{L}_x$ representation is:

$$\hat{L}x = \hbar\begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \tag{11}$$

which is different from its form in the $\hat{L}_z$ representation.

(3) Eigenvalues and Eigenstate Vectors of Physical Quantities

For a physical quantity operator A, if there exists a number a and a state vector |u> that satisfy:

$$\hat{A}|u\rangle = a|u\rangle \tag{12}$$

then a and u are considered as the eigenvalues and corresponding eigenstates of $\hat{A}$.

Each distinct eigenstate is orthogonal and normalized. For the same physical quantity, their eigenfunctions satisfy:

$$\langle u_m|u_n\rangle = \delta_{mn} \tag{13}$$

They are also complete, meaning that for any arbitrary state vector, it can be expressed as:

$$|\varphi\rangle = \sum c_n|u_n\rangle \tag{14}$$

Each eigenvalue of the physical quantity $\widehat{\mathrm{A}}$ represents a possible value of that quantity.

2.4. Superposition of eigenstates

Suppose the particle is in the state |φ> corresponding to a physical quantity $\widehat{\mathrm{A}}$, then it can be expressed as:

DOI: 10.54254/2753-8818/28/20230397

$$|\varphi\rangle = \sum c_n |u_n\rangle \tag{15}$$

The probability of measuring the physical quantity A and obtaining the eigenvalue an is $|c_n|^2$.

2.5. Description of particle states

If two physical quantities A and B commute, i.e., $[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A} = 0$, then they have the same set of eigenfunctions. A and B can be simultaneously used to describe the state of the particle. In the case of the hydrogen atom, the Hamiltonian (H), the square of angular momentum ($\hat{L}^2$), the z-component of angular momentum ($\hat{L}_z$), and the spin state of the particle commute and jointly describe the state of the electron.

If two physical quantities do not commute, then their values cannot be simultaneously measured accurately. Let $\widehat{A}$ and $\widehat{B}$ have eigenvalues and eigenfunctions ($|a_1\rangle$, $|a_2\rangle$, ...) and ($|b_1\rangle$, $|b_2\rangle$, ...), respectively. After measuring A, the wave function collapses to one of its eigenstates, i.e.,

$$|u_{Ai}\rangle = \sum c_{1n} |u_{Bn}\rangle \tag{16}$$

where the measurement result is ai. If the physical quantity B is then measured, and the result is b_j (with the probability $|c_{1j}|^2$), the wave function collapses to the state u_{Bj}, i.e.,

$$|u_{Bj}\rangle = \sum c_{2n} |u_{An}> \tag{17}$$

If A is measured again, the probability of obtaining a_i is $|c_{2i}|^2$, not 1. Therefore, A and B cannot be simultaneously measured accurately.

The position x and momentum p do not commute, so x and p cannot be simultaneously measured accurately.

3. Relevant optical knowledge

In the field of quantum communication, the polarization phenomenon of light plays a crucial role. Polarization describes the direction and shape of the electric field oscillation of a light wave during propagation. The polarization properties of light can be understood within the framework of quantum mechanics, where photons (light quanta) can be represented as quantum states with specific polarization states [6].

In 1809, the French physicist Étienne-Louis Malus proposed Malus' law, which describes the variation of light intensity after linearly polarized light passes through a polarizer. Through his research, a deeper understanding of the polarization phenomenon of light was achieved, laying the foundation for subsequent studies in optics, quantum communication, and other fields.

3.1. Malus' law

Malus' law states that when linearly polarized light passes through a polarizer, the relationship between the transmitted light intensity and the incident light intensity depends on the angle between the transmission axis of the polarizer and the polarization direction of the incident light. Specifically, the relationship between the transmitted light intensity I and the incident light intensity I_0 is given by:

$$I = I_0(cos\theta)^2 \tag{18}$$

where θ is the angle between the direction of vibration of the incident light and the polarization direction of the polarizer.

3.2. Quantum mechanical interpretation of malus' law

3.2.1. Eigenvalues of states. Assuming that the state corresponding to the polarization direction that can pass through the polarizer with 100% probability is:

$$\varphi_1 = (1,0)^* \tag{19}$$

DOI: 10.54254/2753-8818/28/20230397

And the state corresponding to the polarization direction that cannot pass through the polarizer with 100% probability is:

$$\varphi_2 = (0,1)^* \tag{20}$$

This indicates that the light in the φ state is perpendicular to the polarization direction of the polarizer. φ and φ are the only two eigenstates of the event of light passing through the polarizer. Any polarization state of light passing through the polarizer will collapse to one of these two eigenstates with a certain probability.

3.2.2. State of light. Suppose the angle between the direction of vibration of the incident light and the polarization direction of the polarizer is θ. Then the polarization state of light is given by:

$$\varphi = (cos\theta, sin\theta)^* \tag{21}$$

That is:

$$\varphi = cos\theta(1,0)^* + sin\theta(0,1)^* \tag{22}$$

3.2.3. Probability of light transmission. Based on relevant quantum mechanics knowledge, the probability of a photon passing through is given by:

$$P_1 = |\varphi_1{}^*\varphi|^2 = (cos\theta)^2 \tag{23}$$

Therefore, the intensity of the transmitted light after a beam of linearly polarized light with intensity I0 passes through the polarizer is:

$$I = I_0 P_1 = I_0(cos\theta)^2 \tag{24}$$

Similarly, the probability of a photon not being transmitted is:

$$P_2 = |\varphi_2{}^*\varphi|^2 = (sin\theta)^2 \tag{25}$$

3.3. Polarized light in quantum communication

In quantum communication, horizontal-vertical basis vectors and diagonal basis vectors are commonly chosen. The polarization directions of horizontal and diagonal directions are two commuting physical quantities, and therefore, they cannot be simultaneously measured.

The eigenstates on the horizontal-vertical basis vectors are:

$$\varphi_{11} = |\rightarrow\rangle \tag{26}$$

This indicates that when measuring the φ state on the horizontal-vertical basis vectors, a photon can only yield the φ state.

$$\varphi_{12} = |\uparrow\rangle \tag{27}$$

This indicates that when measuring the φ state on the horizontal-vertical basis vectors, a photon can only yield the φ state.

The eigenstates on the diagonal basis vectors are:

$$\varphi_{21} = |\nearrow\rangle \tag{28}$$

This indicates that when measuring the φ state on the diagonal basis vectors, a photon can only yield the φ state.

$$\varphi_{22} = |\searrow\rangle \tag{29}$$

This indicates that when measuring the φ state on the diagonal basis vectors, a photon can only yield the φ state.

Among them:

$$\varphi_{11} = |\rightarrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle + \frac{1}{\sqrt{2}}|\searrow\rangle \tag{30}$$

This indicates that when measuring the φ_{11} state on the diagonal basis vectors, a photon has a $\frac{1}{2}$

DOI: 10.54254/2753-8818/28/20230397

probability of yielding the φ_{21} state and a $\frac{1}{2}$ probability of yielding the φ_{22} state.

$$\varphi_{12} = |\uparrow\rangle = \frac{1}{\sqrt{2}}|\nearrow\rangle - \frac{1}{\sqrt{2}}|\searrow\rangle \tag{31}$$

This indicates that when measuring the φ_{12} state on the diagonal basis vectors, a photon has a $\frac{1}{2}$ probability of yielding the φ_{21} state and a $\frac{1}{2}$ probability of yielding the φ_{22} state.

$$\varphi_{21} = |\nearrow\rangle = \frac{1}{\sqrt{2}}|\rightarrow\rangle + \frac{1}{\sqrt{2}}|\uparrow\rangle \tag{32}$$

This indicates that when measuring the φ_{21} state on the diagonal basis vectors, a photon has a $\frac{1}{2}$ probability of yielding the φ_{11} state and a $\frac{1}{2}$ probability of yielding the φ_{12} state.

$$\varphi_{22} = |\searrow\rangle = \frac{1}{\sqrt{2}}|\rightarrow\rangle - \frac{1}{\sqrt{2}}|\uparrow\rangle \tag{33}$$

This indicates that when measuring the φ_{22} state on the diagonal basis vectors, a photon has a $\frac{1}{2}$ probability of yielding the φ_{11} state and a $\frac{1}{2}$ probability of yielding the φ_{12} state.

4. Quantum communication and its unconditional security

The unconditional security of quantum communication primarily stems from the fundamental principles and characteristics of quantum mechanics. Typically, photons play a crucial role as information carriers in quantum communication, and their states are governed by the laws of quantum mechanics. Firstly, the principle of quantum superposition states that during the measurement process, a quantum system collapses from a superposition of multiple eigenstates to a specific eigenstate. This means that an eavesdropper cannot simultaneously measure multiple states. Secondly, the quantum no-cloning theorem elucidates the impossibility of perfectly replicating an unknown quantum state. Therefore, any attempt by an eavesdropper to copy transmitted quantum bits (such as photons) will result in imperfect copies and introduce disturbances [7]. Moreover, the perturbation caused by measurements in quantum mechanics implies that eavesdroppers unavoidably introduce disturbances when attempting to steal information. The communicating parties can detect such disturbances by comparing partial information, thereby revealing eavesdropping attempts. Finally, quantum entanglement reveals that entangled quantum bits exhibit strong correlations, and any intervention by an eavesdropper will disrupt the entanglement, which can be detected by the communicating parties. In summary, although practical implementations may be subject to technological and equipment limitations, quantum communication still provides a theoretically highly secure means of ensuring information security [8].

4.1. Replicating the state of sent photons

According to the no-cloning principle, let's consider if we want to replicate the state |φ>. What we desire is $|\varphi\rangle|X\rangle = |\varphi\rangle|\varphi\rangle$.

For the eigenstates |φ1> and |φ2>, we have:

$$|\varphi_1\rangle|X\rangle = |\varphi_1\rangle|\varphi_1\rangle \tag{34}$$

$$|\varphi_2\rangle|X\rangle = |\varphi_2\rangle|\varphi_2\rangle \tag{35}$$

Therefore, eigenstates can be replicated.

For the superposition state |φ> = a|φ1> + b|φ2>, we have:

$$|\varphi\rangle|X\rangle = a|\varphi_1\rangle|\varphi_1\rangle + b|\varphi_2\rangle|\varphi_2\rangle \tag{36}$$

But what we desire is:

$$|\varphi\rangle|\varphi\rangle = (a|\varphi_1\rangle + b|\varphi_2\rangle)(a|\varphi_1\rangle + b|\varphi_2\rangle) \tag{37}$$

Therefore, superposition states cannot be replicated.

DOI: 10.54254/2753-8818/28/20230397

4.2. BB84 Protocol

The BB84 protocol, as a quantum key distribution (QKD) protocol, aims to securely distribute cryptographic keys between two remote parties for encrypted communication. This protocol was first proposed by Charles Bennett and Gilles Brassard in 1984. In the implementation of the protocol, the sender and receiver jointly generate a series of random quantum bits, represented by photons with two different polarization states. The sender sends these photons to the receiver, who randomly selects a set of bases to measure the polarization states of the photons. After the measurements are performed, the receiver informs the sender about the bases chosen. Both parties then compare the chosen bases and only retain the corresponding bits when the bases match. By filtering the retained bit string, both parties obtain a shared key for encrypted communication. Since quantum bit strings are unclonable, an eavesdropper cannot perfectly replicate the bit string, and their presence would introduce disturbances during the communication process. Therefore, the BB84 protocol provides high security for key distribution, as even if an eavesdropper successfully intercepts part of the communication, the sender and receiver can detect and correct for the interference.

4.2.1. Protocol steps with no eavesdropper.

(1) The sender randomly generates binary sequences s_A and m_A.

(2) Based on $s_A(\mathrm{n})$ and $m_A(\mathrm{n})$, the sender adjusts the state of the nth photon and sends it.

Table 1. Correspondence between s_A, m_A, and photon states.

s_A	m_A	Photon State
0	0	→
1	0	↑
0	1	↗
1	1	↘

(3) The receiver randomly generates the sequence m_B.

Table 2. Correspondence between m_B and measurement bases.

m_B	Measurement Basis
0	→, ↑
1	↗, ↘

(4) As shown in Table 3, the receiver measures the nth photon based on $m_B(\mathrm{n})$ and obtains the corresponding s_B.

Table 3. Measurement results and s_B with probabilities for different photon states and m_B.

Photon State	m_B	Measurement Result	s_B
→	0(P=1/2)	→(P=1/2)	0(P=1/2)
	1(P=1/2)	P(↗)=P(↘)=1/4	P(0)=P(1)=1/4
↑	0(P=1/2)	↑(P=1/2)	1(P=1/2)
	1(P=1/2)	P(↗)=P(↘)=1/4	P(0)=P(1)=1/4
↗	0(P=1/2)	↗(P=1/2)	0(P=1/2)
	1(P=1/2)	P(→)=P(↑)=1/4	P(0)=P(1)=1/4
↘	0(P=1/2)	↘(P=1/2)	1(P=1/2)
	1(P=1/2)	P(→)=P(↑)=1/4	P(0)=P(1)=1/4

(5) The sender and receiver publicly announce m_A and m_B. When $m_A(\mathrm{n}) = m_B(\mathrm{n})$, it is guaranteed that $s_A(\mathrm{n}) = s_B(\mathrm{n})$, and thus $s_A(\mathrm{n})$ is selected as the key.

4.2.2. Protocol steps with an eavesdropper.

(1) The sender randomly generates binary sequences s_A and m_A.

(2) Based on $s_A(\mathrm{n})$ and $m_A(\mathrm{n})$, the sender adjusts the state of the nth photon and sends it.

(3).The eavesdropper selects measurement bases m_E (assuming the correspondence is the same as

DOI: 10.54254/2753-8818/28/20230397

m_A and m_B) and measures the photons. When m_E(n) is not equal to m_A(n), the state of the photon changes.

(4) The receiver randomly generates the sequence m_B.

(5) The receiver measures the nth photon based on m(n), considering the observed state of the photon by the eavesdropper, and obtains the corresponding s_B.

Table 4. Changes in the state of the photon after being observed by the eavesdropper and measured by the receiver, along with their probabilities.

Initial State	m_E	State After Eavesdropping	m_B	Measured State
→	0(P=1/2)	→(P=1/2)	0(P=1/4)	→(P=1/4)
			1(P=1/4)	P(↗)=P(↘)=1/8
	1(P=1/2)	↗(P=1/4)	0(P=1/8)	P(→)=P(↑)=1/16
			1(P=1/8)	↗(P=1/8)
		↘(P=1/4)	0(P=1/8)	P(→)=P(↑)=1/16
			1(P=1/8)	↘(P=1/8)
↑	0(P=1/2)	↑(P=1/2)	0(P=1/4)	↑(P=1/4)
			1(P=1/4)	P(↗)=P(↘)=1/8
	1(P=1/2)	↗(P=1/4)	0(P=1/8)	P(→)=P(↑)=1/16
			1(P=1/8)	↗(P=1/8)
		↘(P=1/4)	0(P=1/8)	P(→)=P(↑)=1/16
			1(P=1/8)	↘(P=1/8)
↗	0(P=1/2)	→(P=1/4)	0(P=1/8)	→(P=1/8)
			1(P=1/8)	P(↗)=P(↘)=1/16
		↑(P=1/4)	0(P=1/8)	↑(P=1/8)
			1(P=1/8)	P(↗)=P(↘)=1/16
	1(P=1/2)	↗(P=1/2)	0(P=1/4)	P(→)=P(↑)=1/8
			1(P=1/4)	↗(P=1/4)
↘	0(P=1/2)	→(P=1/4)	0(P=1/8)	→(P=1/8)
			1(P=1/8)	P(↗)=P(↘)=1/16
		↑(P=1/4)	0(P=1/8)	↑(P=1/8)
			1(P=1/8)	P(↗)=P(↘)=1/16
	1(P=1/2)	↘(P=1/2)	0(P=1/4)	P(→)=P(↑)=1/8
			1(P=1/4)	↘(P=1/4)

(6) The sender and receiver publicly announce m_A and m_B. If m_A(n) = m_B(n), then s_A(n) and s_B(n) are selected as the key.

(7) As seen from the table, due to the presence of the eavesdropper, s_A(n) is not equal to s_B(n). Therefore, the keys obtained by the sender and the eavesdropper are different, indicating the presence of an eavesdropper. Furthermore, according to the table, the error rate of the BB84 protocol is 25% when no eavesdropper is present, while it increases to 37.5% in the presence of an eavesdropper.

4.3. B92 protocol

The B92 protocol, proposed by Charles Bennett as a modified quantum key distribution protocol, differs from the BB84 protocol. The uniqueness of the B92 protocol lies in its ability to achieve quantum key distribution using only two non-orthogonal quantum states. This simplified approach not only reduces the resources required to implement the protocol but also improves communication efficiency while maintaining high security. By using only two non-orthogonal quantum states, the B92 protocol theoretically achieves a similar level of security as the BB84 protocol, providing a more concise and practical method for key distribution in the field of quantum communication.

DOI: 10.54254/2753-8818/28/20230397

4.3.1. B92 protocol without an eavesdropper. In the absence of an eavesdropper, the communication process of the B92 protocol can be summarized in the following steps:

(1)The sender randomly generates a binary sequence s_A and adjusts the state of the nth photon based on s_A(n). Table 4 shows the corresponding photon states for different binary sequences s_A.

Table 5. Photon states corresponding to different s_A values.

s_A	Photon State
0	→
1	↗

(2) The receiver randomly selects a measurement basis for measurement, as shown in Table 5.

Table 6. Measurement results and their interpretation and probabilities for different photon states and measurement bases.

Photon State	Measurement Basis	Measurement Result	Interpretation	Probability
→	→, ↑	→	Uncertain	P=1/2
	↗, ↘	↗		P=1/4
		↘	Can only be →	P=1/4
↗	→, ↑	↑	Can only be ↗	P=1/4
	↗, ↘	→	Uncertain	P=1/4
		↗		P=1/2

(3) The receiver measures the nth photon sent by the sender using the measurement basis m_B(n) and obtains the corresponding s_B.

(4) The receiver notifies the sender, through a classical channel, about the positions where they obtained definite measurement results without revealing the chosen measurement bases.

(5) Both parties retain the positions with definite measurement results as the shared key.

In the absence of an eavesdropper, the communicating parties can successfully complete the quantum key distribution process and obtain the same shared key. Upon receiving the key, both parties can use it for encrypted communication to ensure the secure transmission of information.

It is worth noting that due to the nature of quantum communication protocols, even in the absence of an eavesdropper, the generated keys by both parties may have some errors. To ensure the correctness of the key, error correction strategies such as error detection and correction codes can be employed by both parties to rectify possible errors and enhance the accuracy and reliability of key distribution.

4.3.2. B92 protocol with an eavesdropper. In the presence of an eavesdropper, the communication process of the B92 protocol can be divided into the following steps:

(1) The sender randomly generates a binary sequence s and adjusts the state of the nth photon based on s(n).

(2) The receiver randomly selects a measurement basis for measurement.

(3) The eavesdropper chooses a measurement basis m_E (assuming it is the same as the receiver's measurement basis) and measures the photons. If m_E(n) differs from the measurement basis chosen by the receiver, the quantum state of the photon will change.

(4) The receiver randomly generates a binary sequence m_B.

(5) The receiver measures the nth photon observed by the eavesdropper based on m_B(n) and obtains the corresponding s_b.

(6) The receiver notifies the sender, through a classical channel, about the positions where they obtained definite measurement results without revealing the chosen measurement bases.

(7) Both parties retain the positions with definite measurement results as the shared key.

DOI: 10.54254/2753-8818/28/20230397

Due to the intervention of the eavesdropper, the keys obtained by the communicating parties may differ. Therefore, the parties can detect the presence of an eavesdropper by comparing parts of the key. Once an eavesdropper is detected, the communication process can be terminated, and a new round of quantum key distribution can be initiated.

It is important to note that in the presence of an eavesdropper, the error rate of the B92 protocol may increase. The eavesdropper's measurement process may perturb the quantum state of the photons, leading to incorrect results obtained by the receiver in subsequent measurements. The communicating parties can analyze changes in the error rate to more accurately determine potential eavesdropping behavior and take appropriate security measures.

5. Development and challenges of quantum communication

5.1. Development of quantum communication technology

5.1.1. International developments. Quantum communication technology has made significant progress worldwide since the 1980s. In 1984, Charles Bennett and Gilles Brassard proposed the BB84 protocol as the first quantum communication scheme. Since then, researchers have achieved a series of important breakthroughs in quantum key distribution, quantum teleportation, and quantum entanglement, among other areas.

In 2005, European scientists successfully conducted quantum key distribution experiments over distances of more than 100 kilometers, further validating the feasibility of quantum communication technology in practical scenarios. In 2013, the United States planned to adopt segmented quantum key distribution technology to provide quantum-level security for communication between data centers of internet giants. The implementation of this plan indicates that quantum communication technology is gradually moving towards commercial applications.

5.1.2. Developments in China. Since the early 21st century, China has made a series of significant breakthroughs in quantum communication. In 2008, a research group led by Professor Pan Jianwei successfully demonstrated the experimental realization of a quantum repeater, achieving entanglement swapping with storage and readout capabilities, and realizing quantum entanglement through 300 meters of optical fiber. This experiment laid a solid foundation for long-distance quantum communication.

In 2012, Pan Jianwei and other scientists achieved free-space quantum teleportation and entanglement distribution over distances of hundreds of kilometers, taking the application of quantum communication technology to a new level. In 2021, a Chinese research team achieved satellite-to-ground quantum key distribution across a distance of 4,600 kilometers, once again setting a world record. This breakthrough demonstrates China's leading position in the field of quantum communication technology. In 2023, quantum remote surgery was successfully performed in Shandong, showcasing the potential application value of quantum communication technology. The widespread application of quantum communication technology will bring revolutionary changes to fields such as healthcare, military, and finance.

5.2. Current challenges

5.2.1. Inability to guarantee security. Although quantum communication is theoretically considered to be inherently secure, in practical applications, the confidentiality of the communication process is not entirely reliable. This is mainly because the devices currently used in quantum communication do not operate under ideal conditions, making it difficult to fully guarantee communication security. In practical operations, there may be potential security risks that impact the confidentiality of quantum communication to some extent.

5.2.2. High cost of popularization. Due to the high precision requirements of quantum communication

DOI: 10.54254/2753-8818/28/20230397

devices, the manufacturing cost is relatively high, resulting in increased costs for the popularization of quantum communication technology. Currently, quantum communication technology is still in the experimental research stage, and related devices have not been mass-produced, which undoubtedly increases the difficulty of promotion and popularization.

5.2.3. Low technological level. The development and promotion of quantum communication technology require high levels of technical support. Quantum communication involves multiple interdisciplinary fields, and interdisciplinary cooperation and research are key to achieving technological breakthroughs. However, the current limitations in technological level pose challenges in the translation from theory to practical applications and from laboratory research to widespread adoption. To overcome these challenges, it is necessary to strengthen cooperation and communication in multiple interdisciplinary fields, enhance the overall technological level, and achieve the widespread application of quantum communication technology.

6. Conclusion

This paper first expounded on the core concepts in quantum mechanics, including observables, state vectors, and eigenstates, and analyzed their properties. By explaining the phenomenon of polarization of light, the theoretical foundation closely related to quantum communication was introduced. Based on this foundation, this paper provided a detailed introduction to two representative quantum communication protocols: the BB84 protocol and the B92 protocol, and elucidated the advantages of quantum communication technology in terms of security and efficiency.

Finally, this paper comprehensively analyzed the current status of quantum communication technology and the challenges it faces. Specifically, the limitations in current technological level, the high cost of device promotion, and the difficulty in ensuring communication security have constrained the development and popularization of quantum communication technology. To overcome these challenges, future research directions need to strengthen cooperation and communication in interdisciplinary fields, continuously improve the technological level, and thus achieve breakthroughs and advancements of quantum communication technology in a broader range of application areas.

References

[1] J. S. Sidhu *et al.*, "Advances in space quantum communications," *IET Quantum Communication,* vol. 2, no. 4, pp. 182-217, 2021.
[2] G. Vallone *et al.*, "Experimental satellite quantum communications," *Physical Review Letters,* vol. 115, no. 4, p. 040502, 2015.
[3] S. Imre, "Quantum communications: Explained for communication engineers," *IEEE Communications Magazine,* vol. 51, no. 8, pp. 28-35, 2013.
[4] A. Manzalini, "Quantum communications in future networks and services," *Quantum Reports,* vol. 2, no. 1, pp. 221-232, 2020.
[5] T. Chapuran *et al.*, "Optical networking for quantum key distribution and quantum communications," *New Journal of Physics,* vol. 11, no. 10, p. 105001, 2009.
[6] I. B. Djordjevic, *Quantum Communication, Quantum Networks, and Quantum Sensing*. Academic Press, 2022.
[7] S. Pirandola, "Limits and security of free-space quantum communications," *Physical Review Research,* vol. 3, no. 1, p. 013279, 2021.
[8] H.-K. Lo, "Classical-communication cost in distributed quantum-information processing: a generalization of quantum-communication complexity," *Physical Review A,* vol. 62, no. 1, p. 012313, 2000.