Utilizing Quantum Circuits to Simulate and Learn Quantum Internet Core Mechanisms

Jehn-Ruey Jiang
Department of Computer Science and Information Engineering
National Central University
Taoyuan, Taiwan
jrjiang@csie.ncu.edu.tw

***Abstract*—The quantum internet connects quantum-information-processing nodes (e.g., quantum computers) through quantum communication channels (e.g., optical fibers) to send, compute, and receive information encoded in quantum states. It has features the current Internet cannot provide such as unhackable communications and distributed quantum computing. In this article, quantum circuits are presented to simulate core quantum internet mechanisms, including quantum entanglement, quantum teleportation, entanglement swapping used in quantum repeaters, and quantum key distribution, to facilitate the learning of the core mechanisms. By observing the simulation results of the quantum circuits, readers can readily comprehend how the quantum internet achieves unhackable information transmission with unconditional security and how it enables large-scale distributed quantum computing and quantum cloud computing by coupling several quantum computers located worldwide.**

Keywords—quantum internet, quantum entanglement, quantum teleportation, entanglement swapping, quantum repeaters, quantum key distribution, quantum cloud computing

I. INTRODUCTION

The Internet, based on TCP/IP and other protocols, connects people, machines, and services worldwide, and has become indispensable for our lives. People rely heavily on the Internet for various aspects of their lives, including work, education, shopping, travel, leisure, entertainment, and social activities. Since the predecessor of the Internet, ARPANET, began operating in October 1969 [1], the Internet has been operating for more than fifty years, continuously evolving and expanding to support larger-scale connections. However, this also brings numerous cybersecurity concerns. For example, hackers can exploit the Internet to launch network attacks with ease, aiming to extort money, steal confidential or private data, hijack funds from bank accounts, or fraudulently acquire improper goods or benefits using stolen credit card information.

The emergence of quantum computers poses an even greater concern for Internet security. Quantum computers operate in a fundamentally different way from classical computers currently in use. Classical computers such as the IBM Summit supercomputer perform computations on bits, whereas quantum computers, such as Google Sycamore and IBM Q, utilize quantum bits, or qubits, for computation [2]. Qubits can exist in a special state called superposition, allowing them to simultaneously represent both 0 and 1 states and undergo operations. When n qubits are in superposition, they represent and undergo operations on all 2^n states simultaneously, whereas n bits only represent and undergo operations on one of the 2^n states at a time. Consequently, the computing power of quantum computers scales exponentially with the number of qubits. When compared with classical computers, quantum computers thus exhibit exponential speedup in computation. Quantum computers have shown quantum supremacy [3] as they perform computations that classical computers cannot complete within a finite amount of time. This advancement in the computing power of quantum computers introduces new challenges and implications for Internet security.

Numerous quantum algorithms have been proposed for quantum computers to solve intractable problems effectively. For example, Shor's algorithm [4] executes certain steps on a quantum computer to factor large integers in polynomial time complexity. This provides an exponential speedup compared to the fastest classical algorithm, the general number field sieve (GNFS), for factoring large integers. Shor's algorithm thus can break the RSA public-key cryptosystem that is based on large integer factorization. Since many mechanisms in the current Internet rely on RSA or related cryptosystems to maintain network security, the security of the Internet is highly vulnerable due to the emergence of quantum computers.

In response to the security threats posed by quantum computers to the Internet, researchers have proposed post-quantum cryptography (PQC) [5] and quantum cryptography (QC) [6] as potential countermeasures against the threats. PQC focuses on developing cryptosystems that run on classical computers using mathematical principles that differ from those of existing systems while ensuring security against attacks posed by quantum algorithms.

PQC examples include lattice-based cryptosystems, such as CRYSTALS-Kyber, CRYSTALS-Dilithium, FALCON, and hash-based cryptosystems, such as SPHINCS+, recommended by the National Institute of Standards and Technology (NIST) [7]. On the other hand, QC exploits quantum mechanical properties to perform cryptographic tasks. The best-known example of QC is the quantum key distribution (QKD) protocol [8] for exchanging keys. The BB84 protocol [9] is the first QKD protocol that achieves information-theoretic security or unconditional security based on one-time pad (OTP) keys [10]. The protocol uses the quantum communication channel to transmit qubit states that encode the keys and employs the classical channel to transmit control messages. If the attacker attempts to read or copy the qubit quantum states, the state will be changed due to the uncertainty property and the no-cloning theorem. This can be used to detect eavesdropping to prevent key compromises.

For the Internet, optical fibers are used to establish communication channels for transmitting data. Since a photon can be used to represent a qubit, we can leverage optical fiber connections to establish quantum channels for transmitting qubit quantum states and build the quantum internet. Furthermore, quantum channels can be established through laser links connected to free-space satellites. To distinguish

them from the quantum channels in the quantum internet, the channels established in the current Internet are called classical channels. In optical communication, classical channels use light pulses to transmit data, where each pulse contains billions of photons representing bit 1, and the absence of photon pulses during a certain period represents bit 0. Quantum channels, on the other hand, use an individual photon to transmit a qubit state. For example, the vertical polarization of a photon is used to represent qubit 1, and the horizontal polarization to represent qubit 0. Other orthogonal states of photons can also be used to represent 0 and 1, such as 45- and -45-degree polarization. Besides transmitting qubit quantum states through quantum channels directly, the quantum teleportation mechanism based on the quantum entanglement phenomenon can transmit qubit quantum states through quantum channels and classical channels altogether. Later, we will elaborate quantum entanglement and quantum teleportation and show quantum circuits simulating them for readers to learn their concepts.

As mentioned earlier, quantum channels in the quantum internet differ from classical channels in the current Internet. Classical channels transmit data of bits using light pulses containing billions of photons, resulting in long transmission distances and low error rates. However, quantum channels transmit qubits of quantum states using the polarization of a single photon. Thus, quantum channels are prone to decay and have short transmission distances and high error rates. To overcome the limitations of quantum channels, a series of quantum repeaters [11] can be deployed to extend the distance of quantum channels. Quantum repeaters were initially proposed by Briegel et al. [12]. Unlike traditional repeaters in classical channels that can replicate and resend signals, quantum repeaters require mechanisms such as entanglement generation, entanglement purification, quantum memory, and entanglement swapping to operate effectively due to the uncertainty principle and the no-cloning theorem.

In this article, the overall architecture and fundamental knowledge of the quantum internet are introduced. Then, core mechanisms in the quantum internet such as quantum entanglement, quantum teleportation, entanglement swapping, and quantum key distribution are explained. Quantum circuits simulating the core mechanisms of the quantum internet are designed and executed on IBM quantum simulators and real IBM Q quantum computers. By showcasing the design of quantum circuits and their simulation or execution results, the core mechanisms of the quantum internet can be understood.

The remainder of this article is organized as follows. Section II explains the basic concepts and knowledge of the quantum internet. Section III further elaborates on the core mechanisms in the quantum internet and simulates them with quantum circuits. Finally, Section IV concludes and summarizes the entire paper.

II. Preliminaries of Quantum Internet

The construction of the quantum internet is one of the main objectives of the “European Union's Quantum Technologies Flagship” program [13]. It aims to achieve highly secure data transmission, including classical bit data and qubit states. This project was announced in May 2016 and launched in October 2018. It is a 10-year program with a total investment of approximately € 1 billion. In July 2020, the U.S. Department of Energy (DOE) released a "Quantum Internet Blueprint" project [14] to construct a nationwide quantum internet in 10 years. Critical research areas of the project include securing quantum protocols on existing fiber optic channels, transmitting entangled quantum information between network nodes, building and integrating quantum network devices such as quantum repeaters and switches, developing routing techniques, and error-correction techniques for qubit transmission over the Internet. In 2017, China established the Beijing-Shanghai backbone, a quantum encryption communication backbone that spans approximately 2,000 km through 32 quantum repeaters. It also connects this backbone to the Micius quantum satellite [15] through laser links using two ground stations, resulting in a 4600-kilometer quantum channel. Additionally, the Micius quantum satellite also serves as a quantum repeater to form a 7,600-kilometer quantum channel between China and Austria.

As mentioned in Ref. [16], the vision of the quantum internet is to co-exist with the current Internet and achieve quantum communications between any two points on Earth, connecting quantum processors and enabling communication and computational capabilities that cannot be achieved by classical computers. In addition to transmitting quantum states to enhance data transmission security, the quantum internet can connect multiple quantum computers to achieve distributed quantum computing (DQC). Since current quantum computers are in the noisy intermediate-scale quantum (NISQ) era [17], they have a limited number of qubits and are subject to noise. Therefore, fault-tolerant techniques are needed to improve the fidelity of qubits with redundant qubits. The quantum internet can connect multiple quantum computers to pool qubits together for achieving massively scalable DQC with qubit entanglement.

The quantum teleportation mechanism sends the state of a qubit of a sending node to a receiving node via a quantum channel and a classical channel, as long as a pair of entangled qubits exists between the two nodes. Thus, the first step in quantum teleportation is to generate a pair of entangled qubits, and then distribute one of the qubits to the sending node and the other qubit to the receiving node. There are various ways to generate entangled qubit pairs. For example, the spontaneous parametric down-conversion (SPDC) technique generates an entangled qubit pair or a photon pair by directing laser light into a specially designed nonlinear birefringent crystal as shown in Fig. 1. One photon of the pair is delivered to the sending node, Alice, whereas the other is delivered to the receiving node, Bob, enabling the process of quantum teleportation. The details of the quantum teleportation mechanism will be described later in the following section.

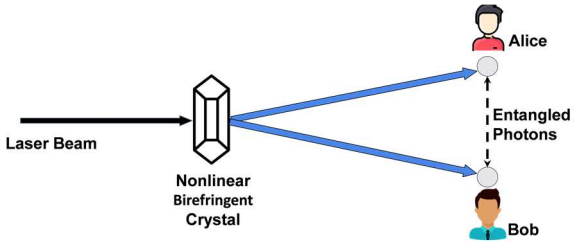


Fig. 1. Illustration of entangled qubit pair (or photon pair) generation.

The quantum internet utilizes both quantum channels and classical channels to form a global network, connecting quantum computers and classical computers. Figure 2 illustrates the physical architecture of the quantum internet [18], which includes various network end nodes (e.g., classical computers and quantum computers), intermediate network

devices (e.g., classical repeaters/switches and quantum repeaters/switches), free-space satellites, and ground stations for connecting to satellites. Quantum channels are established using fiber optics or ground station-satellite laser links to transmit qubit states. The transmission distance between the ground station and the satellite can reach 1,200 km. However, because the intensity of photons in the optical fiber decays significantly with the transmission distance, the optical fiber needs a quantum repeater to extend the transmission range for every distance of about one hundred or several tens of kilometers.

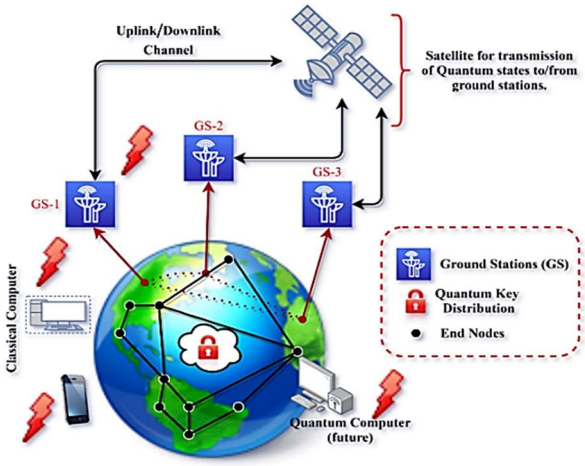


Fig. 2. Quantum Internet physical architecture [18].

The quantum repeater plays an important role in the quantum internet. The heart of a quantum repeater is the process of entanglement swapping. Initially, pairs of entangled particles (or qubits) are created and qubits are distributed to network nodes. Then, through the interaction of these qubits, entanglement is "swapped" from one qubit to another, and two qubits become entangled even though they are not initially directly entangled. For example, a pair of entangled qubits is initially created, and qubits are distributed to an end node, Alice, and an intermediate node, Robert. At the same time, another pair of entangled qubits is created and qubits are distributed to another end node, Bob, and the intermediate node Robert. Afterward, the intermediate node Robert performs entanglement swapping on the pair of its two qubits for exchanging their entanglement relationships. Consequently, the qubit of the Alice node and the qubit of the Bob node become entangled, even though they are not initially directly entangled. In the above-mentioned example, the intermediate node Robert is a quantum repeater. In practice, the satellite can be the quantum repeater of two ground stations spanning large distances. When an intermediate node has more than one pair of qubits to be chosen for performing entanglement swapping, the node is called a quantum switch.

There is another example of using quantum repeaters to extend the range of maintaining (or transmitting) entangled qubits. In the quantum internet scenario of Fig. 3, there are three quantum repeaters between the two end nodes Alice and Bob spaced at distance D. The two nodes and the three repeaters are connected by four segments of quantum channels, each with a length of D/4. Each quantum repeater prepares two pairs of entangled qubits. One of the qubits of repeater-1 is entangled with Alice's qubit, whereas the other is entangled with a qubit of repeater-2. Similarly, one of the qubits of repeater-2 is entangled with repeater-1's qubit, whereas the other is entangled with repeater-3's qubit. Finally, one of the qubits of repeater-3 is entangled with repeater-2's qubit, whereas the other is entangled with Bob's qubit. Then, entanglement swapping is performed on repeater-1, entangling Alice's qubit with the left qubit of repeater-2. Entanglement swapping is performed at repeater-3, entangling Bob's qubit with the right qubit of repeater-2. Finally, entanglement swapping is performed at repeater-2 between the left and right qubits, entangling Alice's and Bob's qubits, even though Alice and Bob are not directly connected and their qubits are not entangled previously.

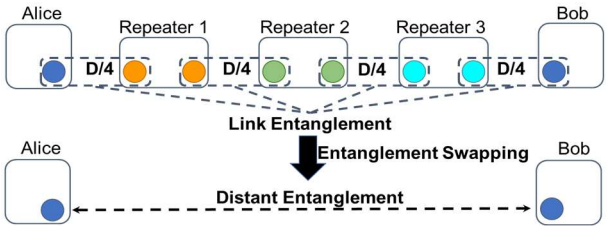


Fig. 3. Illustration of quantum repeater operations using entanglement swapping.

As stated earlier, the quantum teleportation mechanism allows for the transmission of qubit states by using the quantum channel and the classical channel, as long as quantum entanglement exists between qubits of the sending node and the receiving node. Since classical repeaters/switches are employed to extend the transmission range of the classical channel, and quantum repeaters/switches extend the range of quantum entanglement, it is possible to transmit qubit states between any two end nodes of the quantum internet. Thus, based on QKD protocols [8] such as the BB84 protocol [9], secret keys can be exchanged between two quantum internet end nodes without revealing any information on the keys. If the exchanged keys are OTP keys [10], and their lengths are greater than or equal to the length of the ciphertext, then the ciphertext can achieve unbreakable information-theoretic security or perfect security [19].

III. Quantum Circuits to Simulate Quantum Internet Core Mechanisms

Quantum circuits are designed to simulate the quantum internet core mechanisms, including quantum entanglement, quantum teleportation, the quantum repeater, and the BB84 QKD protocol. The core mechanisms are elaborated one by one in the following subsections, along with demonstrations of the quantum circuits simulating them.

A. Quantum Entanglement

Quantum entanglement is crucial in quantum mechanics. Coined by Erwin Schrödinger and famously referred to as "spooky action at a distance" by Albert Einstein, it is a physical phenomenon observed between quantum entities (or particles) where their properties are integrated into a unified one. Therefore, when the quantum state of one entity changes, regardless of the distance between the entangled quantum entities, the quantum states of the other entities change instantaneously. For example, in the case of two entangled photons with opposite polarizations, if one photon is observed or measured to collapse into a vertical polarization, the other photon will instantaneously collapse into a horizontal polarization.

A Bell state or an Einstein-Podolsky-Rosen (EPR) pair is a quantum entangled state between two qubits. Figure 4 shows the quantum circuit corresponding to the Bell state of two

entangled qubits, which is constructed with a Hadamard (H) gate and a controlled-not (CNOT or CX) gate. Figure 5(a) depicts the measurement histogram of exexuting the Bell-state quantum circuit on a quantum computer simulator provided by the IBM Quantum Lab service [20]. The two qubit states are either '00' or '11', and their associated probabilities are both close to 50%, which coincides with the condition that the two qubits are entangled. In the Dirac notation, this quantum circuit corresponds to the entanglement state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$.

Figure 5(b) shows the measuremt histogram of executing the Bell-state quantum circuit on a real IBM quantum computer (ibm_oslo) provided by the IBM Quantum Lab service. Similar to Fig. 5(a), the probabilities of obtaining the measurement outcomes '00' and '11' for the two qubits are also close to 50%. However, due to the inherent noise in real quantum computers, which affects the qubit fidelity, the histogram also exhibits small probabilities of the measurement outcomes '01' and '10'.

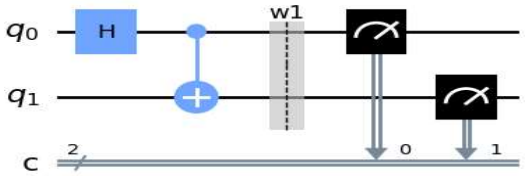
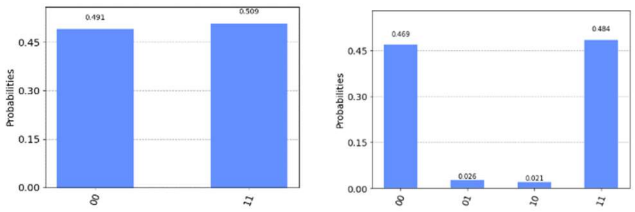


Fig. 4. Quantum circuit for the Bell entangled state qubit pairing.



(a) (b)

Fig. 5. Measurement histograms of executing the entangled Bell-state quantum circuit on (a) a quantum computer simulator and (b) a real quantum computer.

B. *Quantum Teleportation*

The entangled qubits in the Bell state serve as the basis for quantum teleportation, allowing two distant nodes, Alice and Bob, to send and receive the quantum state of a qubit through classical communication. The realization of quantum teleportation is explained using the two-qubit entanglement state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$.

Assuming that the sending node Alice and the receiving node Bob either possess one of the two qubits q_a and q_b in the entangled Bell state $|q_a, q_b\rangle = |\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Alice's qubit and Bob's qubit are denoted as q_a and q_b. Suppose that Alice wants to transmit the state of the qubit q_s to Bob's qubit q_b. This can be achieved through the quantum teleportation circuit depicted in Fig. 6. Note that the qubit q_s is initialized to be of the quantum state $\begin{pmatrix} \frac{1}{3}+\frac{2}{3}i \\ \frac{\sqrt{3}}{3}+\frac{1}{3}i \end{pmatrix}$, so the probability density of the qubit state is $\begin{pmatrix} \left|\frac{1}{3}+\frac{2}{3}i\right|^2 \\ \left|\frac{\sqrt{3}}{3}+\frac{1}{3}i\right|^2 \end{pmatrix} = \begin{pmatrix} \frac{5}{9} \\ \frac{4}{9} \end{pmatrix} = \begin{pmatrix} 0.\bar{5} \\ 0.\bar{4} \end{pmatrix}$. This verifies the measurement result of Bob's qubit q_b coincides with the probability density of Alice's qubit q_s.

The part of the quantum circuit before the first barrier is to establish the Bell entanglement state $|\Phi^+\rangle$ of q_a and q_b. The part of the quantum circuit after the first barrier is for Alice to teleport the state of q_s to Bob's qubit q_b, as described below.

Alice first applies a controlled-not (CNOT) gate, with q_s as the control qubit and q_a as the target qubit. She then applies a Hadamard (H) gate to q_s. Finally, she measures q_s and q_a and sends the measurement results to Bob through a classical communication channel. Upon receiving the measurement results, Bob can complete the quantum teleportation process based on the following four scenarios:

Scenario 1: If the measurement results of q_s and q_a are both $|0\rangle$, then q_b already holds the state of q_s. Thus, no gate is applied to q_b.

Scenario 2: If the measurement result of q_s is $|0\rangle$ and the measurement result of q_a is $|1\rangle$, then an X gate is applied to q_b to restore the state of q_s on q_b.

Scenario 3: If the measurement result of q_s is $|1\rangle$ and the measurement result of q_a is $|0\rangle$, then a Z gate is applied to q_b to restore the state of q_s on q_b.

Scenario 4: If the measurement results of both q_s and q_a are $|1\rangle$, then a Z gate and an X gate are applied to q_b to restore the state of q_s on q_b.

Figure 7(a) shows the histogram of the measurement results of qubit q_b when the quantum circuit is executed on a quantum computer simulator. As shown in Fig. 7(a), the histogram shows q_b is '1' with a probability of around $0.\bar{5}$, and '0', $0.\bar{4}$, which complies with the probability density of q_s. Figure 7(b) shows the histogram of the measurement results of qubit q_b when the quantum circuit is executed on a real IBM quantum computer (ibm_manila). As shown in Fig. 7(b), the histogram of the measurement results of qubit q_b also shows q_b is '1' with a probability of around $0.\bar{5}$, and '0', $0.\bar{4}$. This also complies with the probability density of q_s.

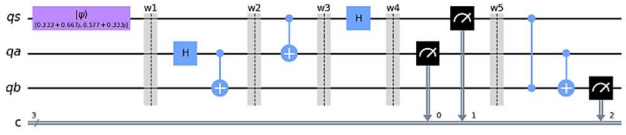
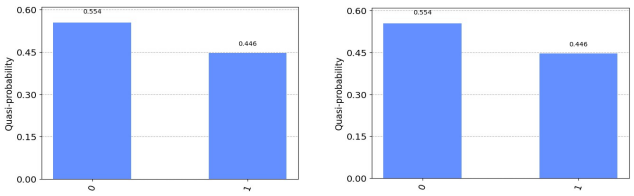


Fig. 6. Quantum circuit realizing quantum teleportation.



(a) (b)

Fig. 7. Measurement histograms of qubit q_b after executing the quantum circuit realizing quantum teleportation on (a) a quantum simulator and (b) a real quantum computer.

C. *Quantum Repeater*

A quantum repeater/switch [11] is used to extend the distance of a quantum channel. As mentioned earlier, a quantum repeater/switch relies on mechanisms such as

entanglement generation, entanglement purification, quantum memory, and entanglement swapping to achieve its functionality. The core mechanism of entanglement swapping and explanations for the corresponding quantum circuit and its execution results are as follows.

Assuming that two end nodes in the quantum internet, Alice and Bob, are too far apart to generate entanglement between their qubits via a directly linked quantum channel. However, there is an intermediate node named Sue between Alice and Bob. Sue and Alice share pairs of entangled qubits, and Sue and Bob share pairs of entangled qubits. In such a scenario, entanglement swapping is performed by Sue to establish entanglement between Alice's qubit and Bob's. The procedure is described as follows.

Node Sue generates a pair of entangled qubits. One qubit is possessed by Sue, and the other, by Alice. Similarly, Sue generates another pair of entangled qubits, and she owns one qubit, while Bob owns the other. Then, Sue performs the entanglement swapping to make Alice's qubit and Bob's qubit entangled even though Alice and Bob have no direct quantum channel connection and their qubits are initially unrelated.

Figures 8 and 9 depict the quantum circuits related to entanglement and their execution results on the IBM quantum computer simulator. Before the first barrier line in the quantum circuit, Alice's and Bob's qubits become entangled with Sue's first qubit and second qubit, respectively. After the second barrier line, Sue performs entanglement swapping by using one CNOT gate, one H gate, one measurement-controlled Z gate, and one measurement-controlled X gate. There are no direct operations between Alice's and Bob's qubits in the quantum circuit, yet entanglement is generated between Alice's and Bob's qubits. The execution results are shown in Fig. 9, where Alice and Bob's qubits are measured as either '00' or '11' with approximately equal probabilities around 50%. This coincides with the probability distribution of the Bell-state $|\Phi^+\rangle$.

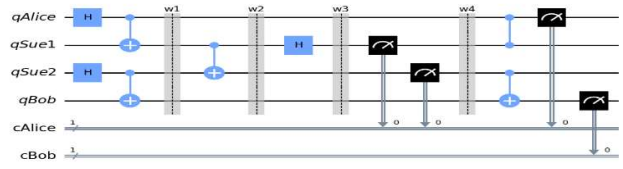


Fig. 8. Quantum circuit simulating the entanglement swapping.

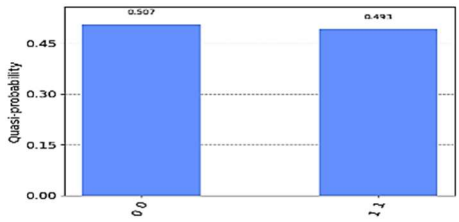


Fig. 9. Measurement histogram of executing the quantum circuit simulating the entanglement swapping.

D. BB84 Protocol

The BB84 protocol [9], proposed by Bennett and Brassard in 1984, is a well-known quantum key distribution (QKD) protocol [8] and is considered to be the first protocol in quantum cryptography. It is used to transmit OTP keys [10] between a sender and a receiver. As long as the key length is greater than or equal to the length of the plain text, it achieves information-theoretic security, unconditional security, or provable security [19]. That is to say, the ciphertext completely reveals no information about the plaintext, ensuring perfect security even when the attacker has unrestricted capabilities.

In the BB84 protocol, a quantum channel is used to transmit quantum states and a classical channel is used to transmit the measurement results and control messages of the quantum states. The basic concept of this protocol is to use two different quantum state bases to transmit and measure quantum states. For example, if the quantum channel is implemented with an optical fiber or a quantum satellite laser link to transmit photons, then one basis can be the rectilinear basis with vertical polarization and horizontal polarization of photons. The other basis can be the diagonal basis with 45-degree and -45-degree (or 135-degree) polarization of photons. The sender and the receiver randomly choose one basis for each transmission and measurement of the quantum states. For instance, the sender can choose the rectilinear basis to transmit a bit 0 through vertical polarization and a bit 1 through horizontal polarization. Meanwhile, the receiver can choose the diagonal basis and interpret a measurement result of 45-degree polarization as bit 0, and conversely, a measurement result of -45-degree polarization as bit 1.

In the BB84 protocol, since the sender and receiver both randomly choose bases, there is approximately a 50% probability for both nodes to select the same basis. In such a case, the two nodes can correctly exchange qubit information, meaning that the qubit information of the receiver matches with the sender's. The matched information can be used later to form an OTP key. Additionally, even when the sender and receiver choose different bases, there is still approximately a 50% probability that the received qubit information of the receiver matches with the sender's. Therefore, there is an overall 75% probability that the sender and the receiver have the same qubit information. This is verified by the measurement results of executing a relevant quantum circuit, as shown in Fig. 10.

Figure 10 is the quantum circuit related to the BB84 protocol, illustrating the four cases in which the sender Alice and the receiver Bob use the same or different bases to transmit the qubit 0. Figure 11 shows the execution results of the quantum circuit on an IBM quantum computer simulator. In the quantum circuit, the rectilinear basis is represented by +Z for 0 and -Z for 1 on the Bloch sphere, whereas the diagonal basis is represented by +X for 0 and -X for 1. Basis transformation is conducted on the quantum circuit by using the H gate. In practice, the state before the first barrier line in the quantum circuit represents Alice's representation of the qubit 0. The first two qubits, q_0 and q_1, are represented in the ±Z basis, whereas the last two qubits, q_2 and q_3, are represented in the ±X basis. Since the IBM quantum computer cannot change the measurement basis and its default measurement basis is the ±Z basis, an H gate is applied before measuring the qubits in the ±Z basis measurement, which is equivalent to performing an ±X basis measurement. The part between the first and second barrier lines in the quantum circuit indicates Bob's choice of measurement basis. Qubits q_0 and q_2 are measured on the ±Z basis, whereas qubits q_1 and q_3 are measured on the ±X basis. The results show that qubits q_0 and q_3 are both measured as '0' with a 100% probability, whereas qubits q_1 and q_2 have a 50% probability of being measured as '0' correctly (Fig. 11). Therefore, the overall probability of correctly measuring the qubit as '0' is 75%.

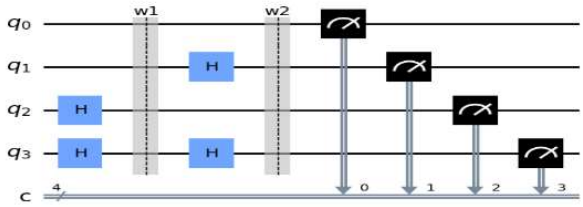


Fig. 10. Quantum circuit related to BB84 protocol to simulate sender and receiver using and not using the same basis.

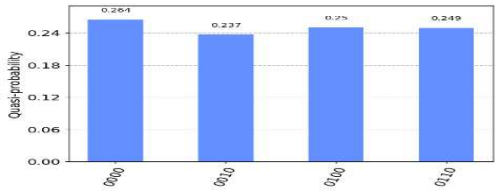


Fig. 11. Measurement histogram of executing quantum circuit related to BB84 protocol to simulate sender and receiver using and not using the same basis.

Generally, when Alice and Bob use the same basis to represent and measure qubits, the qubits can be received correctly with a 100% probability. Therefore, Alice and Bob can use these qubits to build a secret key, such as an OTP key. However, because there might be an eavesdropper Eve in both the classical and the quantum channels, it is necessary to use a portion of these correctly received qubits to detect any potential eavesdropper.

During the execution of the BB84 protocol, an eavesdropper cannot copy qubits due to the no-cloning theorem. If the eavesdropper tries to intercept qubits by measuring them, then the qubit state collapses into one state of the quantum measurement basis. Thus, the eavesdropper needs to guess the basis adopted by the sender to resend every intercepted qubit. Assuming that Alice and Bob adopt the same basis for sending and receiving qubits. Eve has a 50% probability of guessing correctly about the basis used by Alice, so Bob cannot detect the presence of Eve in such a case of correct guessing. On the contrary, Eve has a 50% probability of guessing incorrectly about the basis used by Alice. For such a case of incorrect guessing, Bob has still a 50% probability of receiving the same qubit information as Alice, leading to a 50% probability of not detecting the qubit interception. Therefore, Alice and Bob have a 25% probability of not detecting the presence of Eve for a single qubit under the condition that Alice and Bob adopt the same basis. The BB84 protocol relies on this to detect possible qubit interception to ensure the protocol's security. However, due to the space limitation, readers are referred to [9] for the details of the BB84 protocol.

IV. Conclusion

The evolution from the Internet to the quantum internet is overviewed, including the current status and prospects of quantum internet development worldwide. Quantum circuit simulations are presented to illustrate quantum internet core mechanisms, including quantum entanglement, quantum teleportation, entanglement swapping used in the quantum repeater, and quantum key distribution. By observing the simulation results of the quantum circuits, quantum internet core mechanisms can be understood to gain further insights into how the quantum internet achieves unbreakable, unconditional secure data transmission between two end nodes that are far apart. The quantum internet is still developing but with challenges and difficulties. Related research directions require in-depth investigation and exploration. The main research directions are (1) designing more efficient quantum key distribution protocols, (2) establishing novel methods for entanglement generation, entanglement purification, entanglement distribution, quantum memory, and entanglement swapping, (3) devising routing mechanisms to select appropriate intermediate quantum repeaters/switches to form efficient and high-quality end-to-end quantum channel in quantum internet, and (4) connecting quantum computers located worldwide to perform large-scale distributed quantum computing and quantum cloud computing.

References

[1] B. Stewart, Internet History – One Page Summary, https://www.livinginternet.com/i/ii_summary.htm, accessed on Jan. 10, 2024.

[2] J.-R. Jiang and C.-W. Chu, "Classifying and benchmarking quantum annealing algorithms based on quadratic unconstrained binary optimization for solving NP-hard problems," IEEE Access, vol. 11, pp. 104165-104178, 2023.

[3] F. Arute, et al., "Quantum supremacy using a programmable superconducting processor," Nature, 574, 505–510, 2019.

[4] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring." In Proc. of the IEEE 35th annual symp. on foundations of computer science, pp. 124–134, 1994.

[5] E. Zeydan, et al., "Recent advances in post-quantum cryptography for networks: A survey," In Proc. of the IEEE 7th Int'l Conf. on Mobile and Secure Services (MobiSecServ), pp. 1–8, 2022.

[6] A. Kumar, and S. Garhwal, "State-of-the-art survey of quantum cryptography," Archives of Computational Methods in Engineering, 28, 3831–3868, 2021.

[7] T. Hasija, et al., "A survey on NIST selected third round candidates for post quantum cryptography," In Proc. of 7th Int'l Conf. on Comm. and Electronics Systems (ICCES), pp. 737–743, 2022.

[8] K. K. Choure, et al., "Recent advancement in high speed and secure quantum key distribution: A review," In Proc. of 2022 Optical and Wireless Technologies (OWT 2022), pp. 259–267, 2022.

[9] C. H. Bennett, and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," In Proc. of IEEE Int'l Conf. on Computers, Systems and Signal Processing, pp. 175–179, 1984.

[10] F. Miller, Telegraphic code to insure privacy and secrecy in the transmission of telegrams, CM Cornwell, 1882.

[11] P. S. Yan, et al., "A survey on advances of quantum repeater," Europhysics Letters, 136, 14001, 2021.

[12] H. J. Briegel, et al., "Quantum repeaters: the role of imperfect local operations in quantum communication," Physical Review Letters, 81(26), 5932, 1988.

[13] Quantum Flagship, https://golden.com/wiki/Quantum-Flagship-DB8PKDY, accessed on Jan. 10, 2024.

[14] Launch to the future: quantum internet, https://www.energy.gov/articles/us-department-energy, accessed on Jan. 10, 2024.

[15] S. K. Liao, et al., "Satellite-to-ground quantum key distribution," Nature, 549, 43–47, 2017.

[16] S. Wehner, et al., "Quantum internet: A vision for the road ahead," Science, 362, eaam9288, 2018.

[17] J. Preskill, "Quantum computing in the NISQ era and beyond," Quantum, 2, 79, 2018.

[18] A. Singh, et al., "Quantum internet—applications, functionalities, enabling technologies, challenges, and research directions," IEEE Communications Surveys & Tutorials, 23, 2218–2247, 2021.

[19] C. E. Shannon, "Communication theory of secrecy systems," The Bell System Technical Journal, 28, 656–715, 1949.

[20] IBM Quantum Lab, https://quantum-computing.ibm.com/lab, accessed on Jan. 10, 2024.