sensors

MDPI

Article

Quantum Multi-User Broadcast Protocol for the "Platform as a Service" Model

Peng Shi, Nachuan Li, Shumei Wang, Zhi Liu, Mengran Ren and Hongyang Ma *

Quantum Physics Laboratory, School of Science, Qingdao University of Technology, Qingdao 266520, China; shipeng@qut.edu.cn (P.S.); tigerdbrick1998@gmail.com (N.L.); shumeiwang@aliyun.com (S.W.); liuzhi001336@163.com (Z.L.); mengran_ren09@163.com (M.R.)

* Correspondence: hongyang_ma@aliyun.com

Received: 24 October 2019; Accepted: 28 November 2019; Published: 29 November 2019

Abstract: Quantum Cloud Computing is the technology which has the capability to shape the future of computing. In "Platform as a Service (PaaS)" type of cloud computing, the development environment is delivered as a service. In this paper, a multi-user broadcast protocol in network is developed with the mode of one master and N slaves together with a sequence of single photons. It can be applied to a multi-node network, in which a single photon sequence can be sent to all the slave nodes simultaneously. In broadcast communication networks, these single photons encode classical information directly through noisy quantum communication channels. The results show that this protocol can realize the secret key generation and sharing of multiple nodes. The protocol we propose is also proved to be unconditionally secure in theory, which indicates its feasibility in theoretical application.

Keywords: Quantum Cloud Platform; phase-covariant cloning; Quantum Cloning Machine; multi-user broadcast; Platform as a Service

1. Introduction

The interest in quantum cloud computing (see [1]) has really taken off in the past few years, but, in the future, quantum computers will be quite expensive in nature and will not be available to every one. To solve this problem, a basic idea of cloud computing, which migrates the processing power from customer's computer to remote Internet servers, is put forward. One of the service models on quantum cloud computing, "Platform as a Service" [2] is proposed for supporting online development environment. Multi-user broadcast, similar to multicast, can be used on cloud platform to communicate between router and users.

Multicast has many applications such as access to business information dissemination, distributed databases, distance teleconferencing, and network learning. Multi-user broadcast protocol can increase quantum network efficiency and conserve its resources. A sender, Alice, wants to send some confidential information to receivers, Bob brothers. They must multicast communicating messages, on the basis of high enough confidentiality and legitimacy of information. As an applied system, its safety is very important.

A simple communication mode is one to one, such as the BB84 protocol [3]. Multiparty communication [4–6] has drawn much attention. Matsumoto [7] proposed a quantum-key-distribution protocol that could enable three parties to agree at once on a shared common random bit string in the presence of an eavesdropper without the use of entanglement, which might not be directly applied to the one-to-many multicast communication. Yan [8] proposed a quantum secret sharing protocol between multiparty m members in Group 1 and multiparty n members in Group 2 using a sequence of single photons. Another extension of the theory of various Quantum Cloning Machines (QCM)

protocols [9–14] has been designed and their applications and implementations have been studied, both theoretically and experimentally. The research of quantum cloning and deep application are continuously developing. In our research, we use optimal one to M phase-covariant QCM to implement multi-user broadcast protocol. Theoretically, these QCM, which provide the most dangerous and efficient attack for the BB84 protocol, can be used to multicast message in an optimal fidelity.

The rest of this paper is organized as follows. We show a summary of relevant results concerning multicast addresses and quantum cloning in Section 2. In Section 3, we present multi-user broadcast protocol based on quantum cloning. In Section 4, we analyze optimal fidelity, throughput efficiency and security. Finally, we present our conclusions.

2. Overview

2.1. Multicast Addresses

There are one source and a group of destinations in multicast communication protocol. Figure 1 shows the simple multicast communication network, which depicts a set of quantum network nodes. The node of quantum network is a source sub of quantum data that must be delivered to a group G_1 of quantum network nodes, F_1, F_2, ..., F_i, ..., F_M, respectively. There is more than one quantum network node, but the group does not contain all possible quantum network nodes. This relationship is one to many.

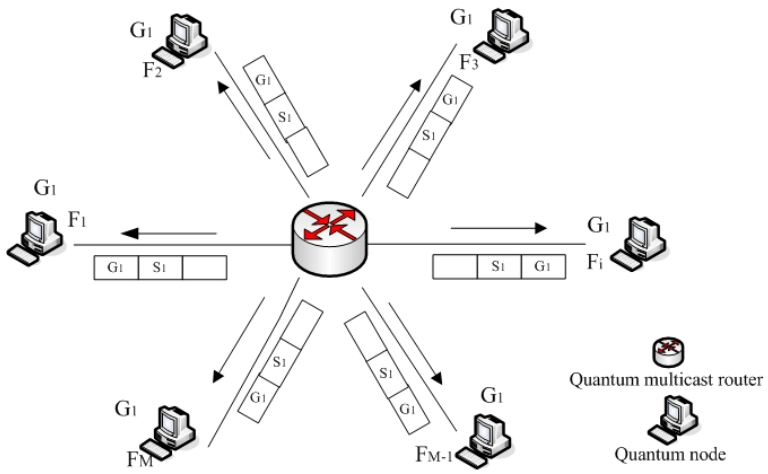

Figure 1. The simple multicast communication network.

The multicast address is a destination address for a group of quantum network nodes that have joined a multicast group, which is a great help to classical communication of quantum network communication protocol. A packet that uses a multicast address as a destination can reach all members of the group unless there are some filtering restrictions by the quantum network node. It only discusses the multicast addresses in the network layer, in particular the multicast addresses used in the $IPv4$ protocol. Multicast addresses for $IPv6$ can hardly even be touched. In TCP/IP protocol suites, Class D IP addresses are used as multicast addresses. The range of Class D addresses is 224.0.0.0–239.255.255.255, include 28 variable bits, 2^{28} (more than 268 million) multicast groups. Quantum network nodes may be permanent or transient. The former refers to the fact that the group has a permanently assigned address, rather than that members are permanently assigned to the group. The latter refers to the groups which do not have a permanent assignment to unreserved address.

2.2. Phase-Covariant Quantum Cloning

The no-cloning theorem [15] states that it is impossible to build a quantum copying machine that would perfectly copy arbitrary quantum states. However, we can try to clone a quantum state

approximately with the optimal fidelity, or instead, we can try to clone it perfectly with the largest probability. Thus, various quantum cloning machines have been designed for different quantum information protocols. Some well-known quantum cloning machines include universal quantum cloning machine, phase-covariant cloning machine, the asymmetric quantum cloning machine, and the probabilistic quantum cloning machine. For instance, a cloning machine that achieves equal fidelity for every state is called a universal quantum cloning machine ($UQCM$). This problem is equivalent to distributing information to different receivers, and it is natural to require the performance is the same for every input state, since we do not have any specific information about the input state ahead. According to no-cloning theorem, it is expected that the original input state will be destroyed and become as one of the output copies. Because of the different types of copies, there are symmetric and asymmetric $UQCMs$. In the past years, much progress has been made in studying quantum cloning machines and their applications and implementations, both theoretically and experimentally. More details about quantum cloning are proposed in [16–18].

Here, we mainly discuss the phase-covariant quantum cloning, which has developed on the basis of universal quantum cloning and can produce equally good copies for all input states that lie on the equator of the Bloch sphere. The quantum state

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle), \tag{1}$$

where $\varphi \in [0, 2\pi)$ is an arbitrary phase parameter, is often used as the input qubit of the phase-covariant QCM. For instance, the optimal $1 \to 2$ phase-covariant cloning transformation takes the form [19]

$$\begin{aligned} |0\rangle_A|0\rangle_B|0\rangle_C &\to \sqrt{\frac{1}{2}}\left(|0\rangle_B|00\rangle_{AC} + |1\rangle_B|\chi\rangle_{AC}\right) = |\phi_0\rangle_{ABC}, \\ |1\rangle_A|0\rangle_B|0\rangle_C &\to \sqrt{\frac{1}{2}}\left(|1\rangle_B|11\rangle_{AC} + |0\rangle_B|\chi\rangle_{AC}\right) = |\phi_1\rangle_{ABC}, \end{aligned} \tag{2}$$

where $|\chi\rangle = 1/\sqrt{2}(|10\rangle + |01\rangle)$, A is the initial state of the cloning machine, B is an ancilla state of the system, and C is the blank state. The optimal fidelity of phase-covariant QCM is $F = 1/2 + 1/\sqrt{8} \approx 0.85$, which is higher than the fidelity ($F \approx 0.83$) of $UQCM$.

Then, considering the optimal $1 \to M$ phase-covariant QCM, one of the cloning transformations is

$$|\psi\rangle \otimes \left(|R\rangle^{\otimes M-1}\right) \otimes |M\rangle \overset{U_{1,M}}{\to} |\psi\rangle^{\otimes M} \otimes |M(\psi)\rangle, \tag{3}$$

where $|\psi\rangle$ is the state of Hilbert space H, $|R\rangle$ is a blank state, and $|M\rangle$ is the state of auxiliary system (ancilla). The $U_{1,M}$ is described by the following unitary operator[20]:

$$\begin{aligned} |\phi_0\rangle_{AC} &= U_{1,M}|0\rangle \otimes |R\rangle = \sum_{j=0}^{M-1} \alpha_j |(M-j)0, j1\rangle \otimes |R_j\rangle, \\ |\phi_1\rangle_{AC} &= U_{1,M}|1\rangle \otimes |R\rangle = \sum_{j=0}^{M-1} \alpha_{M-1-j} |(M-1-j)0, (j+1)1\rangle \otimes |R_j\rangle, \end{aligned} \tag{4}$$

in which $\alpha_j = \sqrt{2(M-j)/M(M+1)}$, $|R\rangle$ is the initial state of the copy machine and the $M-1$ blank copies, and $|R_j\rangle \equiv |(M-1-j)0, 1j\rangle$ are orthogonal normalized internal states of the QCM. With the help of an ancilla qubit, the optimal fidelity of $1 \to M$ phase-covariant QCM for equatorial qubits takes the form[18]

$$F_{1,M} = \begin{cases} 1/2 + \sqrt{M(M+2)}/4M, & M \text{ is even}, \\ 1/2 + (M+1)/4M, & M \text{ is odd}, \end{cases} \tag{5}$$

which is the decreasing function for M and is better than the fidelity of $UQCM$ via numerical computation.

3. Multi-User Broadcast Protocol Based on *QCM*

3.1. Neighbor Quantum Node Discovery Process

The quantum multicast router starts to discover its neighbors with probe packet messages, which contain the important informations: a list of addresses for neighbors from which the originating router has received probe packet messages, a generation ID used to detect changes in status of neighbors, and so on. After receiving the probe packet messages, the quantum multicast router records the address of the original router and the interface of received messages.

3.2. Neighbor Quantum Node Pruning Process

Probe packet messages are also used as keepalives when a neighbor has been discovered, and then the neighbor node send messages to the quantum multicast router within strict time intervals. If the quantum multicast router does not receive messages from this node after several probes within a specified period of time, the neighbor node will be declared dead. We call this step a neighbor quantum node pruning process, and this node is considered undependable at this time. For example, the pruning process of neighbor node F_{M-1} is shown in Figure 2. The quantum multicast router must store the states of all nodes after each pruning process. If necessary, nodes and the router need to repeatedly send and receive messages in this process as many times as possible to complete the pruning process of quantum nodes.

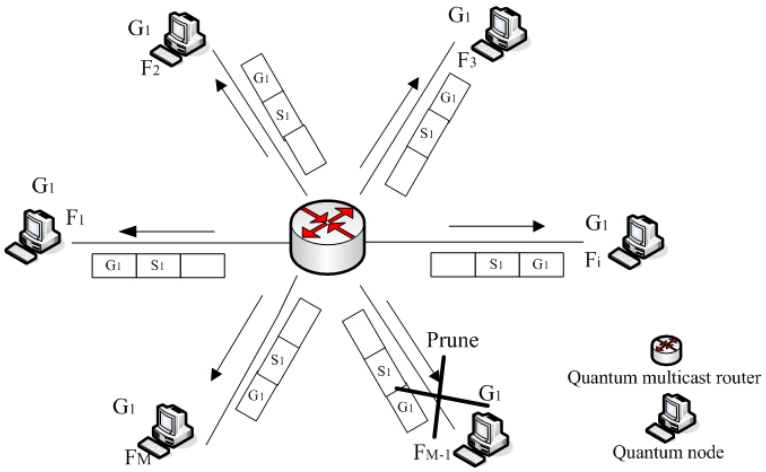

Figure 2. Pruning process of an undependable neighbor quantum node.

3.3. Group Routing Tables Building Process

The quantum multicast router needs to collect members' information and share it with other multicast routers, and then construct group routing table containing group members' information. The graph of quantum nodes and links is called tree, so the quantum multicast router can be regarded as the root node. All other nodes $F_i (i = 1, 2, \cdots, M)$ can only be reached from the root node through a single path. Multicast communication means that a sender sends messages to a group of recipients who are members of the same group. Since a copy of the message is sent by the sender and then copied and forwarded by the router, each multicast router needs to know the list of groups.

The group routing tables carry four core data: the quantum nodes identity, the list of links, a sequence number, and the age. The quantum nodes identity and the list of links are needed to make the quantum topology. The sequence number distinguishes new routing tables from old ones. The age prevents old routing tables from remaining in the domain for a long time. When the topology of a domain changes, any quantum nodes in the domain are quickly notified by the router to update their topology.

3.4. Multicast Date Packet Communication on Quantum Cloning Process

We apply the phase-covariant cloning machine to multicast communication (in Figure 3). For each input single photons, we use a unitary transformation matrix A to prepare the input state on the equator of the Bloch sphere:

$$A = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & e^{-i\varphi} \\ e^{i\varphi} & -1 \end{pmatrix}. \tag{6}$$

The quantum multicast router encodes these strings as a block of $(4n + \delta)$, and sends $|\Psi_0\rangle = \sum_{i=0}^{4n+\delta} |\psi_i\rangle$ to $F_i (i = 1, 2, \cdots, M)$ by quantum cloning via the quantum communication channel. For simplicity, we assume that the quantum channel is noiseless. The quantum multicast router transmits $|\Psi_0\rangle$ through quantum channel to construct QCM.

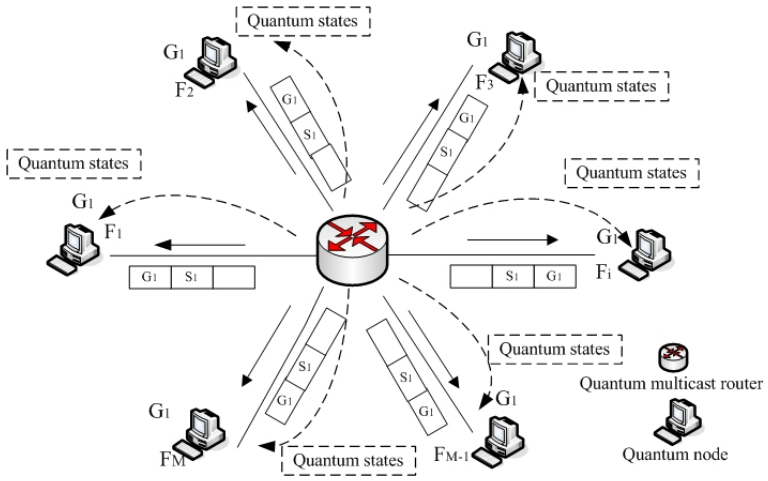

Figure 3. Multicast quantum cloning process.

The quantum multicast router acts on an input state $|\psi\rangle$ as follows:

$$\begin{aligned} \sum_{i=0}^{4n+\delta} U_{1,M} |\psi_i\rangle \otimes |R\rangle &= \sum_{i=0}^{4n+\delta} \sum_{j=0}^{M-1} \alpha_{M-1-j} |(M-1-j)\psi_i, (j+1)\psi_i^{\perp}\rangle \otimes |R_j(\psi_i)\rangle \\ &= \sum_{i=0}^{4n+\delta} \sum_{j=0}^{M-1} \alpha_{M-1-j} |(M-1-j)\psi_i, (j+1)\psi_i^{\perp}\rangle \otimes |(M-1-j)\psi_i^*, (j+1)(\psi_i^*)^{\perp}\rangle, \end{aligned} \tag{7}$$

where $|R_j(\psi_i)\rangle$ represents the internal state of QCM with $|R_j(\psi_i)\rangle \perp |R_k(\psi_i)\rangle$ for all $j \neq k$, and the equatorial qubits take the forms

$$\begin{aligned} |\psi_i\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle), \\ |\psi_i^*\rangle &= \frac{1}{\sqrt{2}}(|0\rangle + e^{-i\varphi}|1\rangle), \\ \left|\psi_i^{\perp}\right\rangle &= \frac{1}{\sqrt{2}}(e^{-i\varphi}|0\rangle - |1\rangle), \\ \left|(\psi_i^*)^{\perp}\right\rangle &= \frac{1}{\sqrt{2}}(e^{i\varphi}|0\rangle - |1\rangle). \end{aligned} \tag{8}$$

Quantum correlation is the key concept for the quantum computation, quantum processing, and quantum information. Entanglement is a special case of quantum correlation. It is a property of correlations between two or more quantum systems. This nonlocal nature of entanglement has also been identified as an essential resource for many novel tasks. The preparation of entangled states in different physical systems has been widely studied and constitutes an essential step in many quantum

information processing and transmission tasks [21–23]. For Alice and M Bob brothers, we assume that they all share a multi-particle entangled state $|\Omega\rangle$, and a choice of $|\Omega\rangle$ with these properties in the following M-qubit state:

$$|\Omega\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |\phi_0\rangle_{AC} + |1\rangle \otimes |\phi_1\rangle_{AC}), \tag{9}$$

where $|\phi_0\rangle_{AC}$ and $|\phi_1\rangle_{AC}$ are the optimal cloning states given by Equation (4), and $|\Omega\rangle$ turns into

$$|\Omega\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle \sum_{j=0}^{M-1} \alpha_j |(M-j)0, j1\rangle \otimes |(M-1-j)0, j1\rangle + |1\rangle \sum_{j=0}^{M-1} \alpha_j |j0, (M-j)1\rangle \otimes |j0, (M-1-j)1\rangle). \tag{10}$$

The tenser product of $|\Omega\rangle$ with the equator qubits $|\Psi_0\rangle$ held by the $(2M + 4n + \delta + 1)$-qubit state of Alice. Alice performs a joint measurement of the system $|\Psi_0\rangle \otimes |\Omega\rangle$ by using Bell measurement [24], where the four Bell states are defined as usual as the following

$$\begin{aligned} |\phi_\pm\rangle &= \frac{1}{\sqrt{2}}\left(|00\rangle \pm |11\rangle\right), \\ |\psi_\pm\rangle &= \frac{1}{\sqrt{2}}\left(|01\rangle \pm |10\rangle\right). \end{aligned} \tag{11}$$

Once one of the Bell states is obtained, we can recover the correct state by exploiting the symmetries of states $|\phi_0\rangle_{AC}$ and $|\phi_1\rangle_{AC}$ under the unitary transformation. Consider three Pauli matrices; the unitary transformation can be expressed as

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{12}$$

The quantum multicast router measures Bell state of A, and the router and each nodes can transmit qubit BC in the following four forms as $\sum_{i=0}^{4n+\delta}(|0\rangle \pm e^{i\varphi}|1\rangle)/\sqrt{2}$ or $\sum_{i=0}^{4n+\delta}(|1\rangle \pm e^{i\varphi}|0\rangle)/\sqrt{2}$. When $\sum_{i=0}^{4n+\delta}(|1\rangle \pm e^{i\varphi}|0\rangle)/\sqrt{2}$ is obtained, the unitary transformation is $\sigma_x(\sigma_x\sigma_z)$ corresponding to the symbol "+"("−") in the equations. When $\sum_{i=0}^{4n+\delta}(|0\rangle \pm e^{i\varphi}|1\rangle)/\sqrt{2}$ is obtained, the unitary transformation is $\sigma_0(\sigma_z)$ corresponding to the symbol "+"("−"). After these operations, the secret key is transmitted to the server, and the quantum multicast router and each node releases part of the quantum information. If the test is correct, the communication station (STA) is a legitimate user. Otherwise, there must be illegal eavesdroppers, which we discuss in the next section. In this process, quantum multicast router transmits classical information through Ethernet addresses. The main problem below is to change the three right-most bytes of the multicast IP address to hexadecimal. If the left-most number is greater than or equal to 8, subtract 8 from the left-most number. After the system gets the result, add the result to the starting Ethernet multicast address. Thus, the multicast date packet communication on quantum cloning process has completed successfully.

3.5. Selective Repeating Process

In this protocol model, the multicast router node acts as a key management system and authenticates the communication users in communication. The multicast router manages the security key for the communication users and authenticates the identity of users by arbitrating the quantum signature using the shared quantum state [25]. In the process of communication, the multicast router node conducts authentication occasionally to prevent the user from being attacked.

Ideally, we assume that each photon emission is perfect. If the information transmission fails due to channel loss or eavesdropping, the multicast router will return a negative acknowledgment (NAK) to the nodes. After receiving the NAK, the node will start the selective repeating process, thus ensuring the security and reliability of the communication. The strings are transmitted continuously as a block of $(4n + \delta)$, the quantum multicast router resends (or repeats) only those codewords that are

negatively acknowledged. Since the strings must be delivered to the user in correct order, a buffer must be provided at the receiver to store the error-free qubits of received qubits after error detection. When the first negatively acknowledged strings are successfully received, the receiver releases the error-free qubits in consecutive order until the next erroneously received qubits are encountered. Sufficient qubits receiver buffers must be provided, otherwise the qubits buffers may overflow and quantum data may be lost.

4. Analysis

4.1. Analysis of Quantum Bit Error Rate and Secure Key Rate

The Quantum Bit Error Rate ($QBER$) is defined as the number of wrong bits to the total number of received bits and is normally in the order of a few percent. In the following, we use it expressed as a function of rates:

$$QBER \approx \frac{R_{error}}{R_{sift}}, \tag{13}$$

where the sifted key corresponds to the cases in which Alice and Bob made compatible choices of bases, hence its rate is half that of the raw key. In a practical quantum key distribution system, e.g. the $BB84$ protocol, after attenuation and sifting, the sifted key generation rate is given by [26]

$$R_{sift} = \frac{1}{2} q \cdot f_{rep} \cdot \mu \cdot t_{link} \cdot \eta. \tag{14}$$

where the factor q ($q \leq 1$, typically 1 or $\frac{1}{2}$) must be introduced for some phase-coding setups in order to correct for noninterfering path combinations, f_{rep} is the pulse rate, μ is the mean number of photon per pulse, t_{link} is the probability of a photon to arrive at the analyzer, and η is the probability of the photon being detected.

The secure key rate in our protocol is the quantum communication rate of the whole system. This depends on the rate of key distribution when each root node communicates with its children, that is the rate of the sifted key generation.

4.2. Analysis of Optimal Fidelity

The fidelity is widely used within the quantum computation and quantum information community, and we discuss the quantum multi-user broadcast protocol for the "Platform as a Service" model. In our study, the algorithm discussed above is sufficient to complete each step of the computation with higher fidelity than $1 \rightarrow M$ phase-covariant QCM by Equation (5).

The quantum multicast router obtains measurement outcome for $|\Psi_0\rangle_{out}$, and publicly announces the results. S_1, S_2, ..., S_i, ..., $S_N (N < M)$ carry out the unitary transformation σ separately on their qubits. The final states of qubits for $S_i (i = 1, 2, \cdots, N)$ equal to the original state $|\Psi_0\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$. We now wish that the optimal phase-covariant cloning machine can be achieved. Let us see fidelity, which is found to take the form

$$F = \frac{1}{2}[1 + \eta(1, N)] = \begin{cases} 1/2 + \sqrt{N(N+2)}/4N, & N \text{ is even}, \\ 1/2 + (N+1)/4N, & N \text{ is odd}, \end{cases} \tag{15}$$

where

$$\eta(1, N) = \sum_{j=0}^{N-1} \alpha_j \alpha_{N-1-j} \frac{C_{N-1}^{j}}{\sqrt{C_N^j C_N^{j+1}}}. \tag{16}$$

4.3. Analysis of Throughput Efficiency

Next, we discuss the throughput efficiency which is defined as the ratio of the average number of information digits successfully accepted by the receiver per unit of time to the total number of digits that could be transmitted per unit of time. Suppose the simple case of the communication protocol, and the sender continuously sends codewords to the receiver and only resends those negatively acknowledged codewords. First, three probabilities are defined: P_c, P_d, and P_e, where $P_c + P_d + P_e = 1$. P_c is the probability of receiving no error message, P_d is the probability of receiving detectable error pattern, and P_e is the probability of receiving undetectable error pattern. Then, the probability of receiving vector being accepted by the receiver is $P = P_c + P_e$.

The average number of retransmissions (including original transmissions) for a codeword to be successfully received by the receiver is

$$t_{AV} = 1 \cdot P + 2 \cdot P \cdot (1 - P) + \cdots + l \cdot P \cdot (1 - P)^{l-1} + \cdots = \frac{1}{P} \tag{17}$$

Finally, the throughput of sending n codewords successfully is $T = \dfrac{n}{t_{AV}} = nP$. Thus, the throughput efficiency depends on the channel error rate only.

4.4. Analysis of Security under Typical Attack

The Security of this broadcast protocol depends on every process of communication between one source and a group of destinations. The protocol is divided into five parts as neighbor quantum node discovery process, neighbor quantum node pruning process, group routing tables building process, multicast date packet communication on quantum cloning process, and selective repeating process. Conventional data communication is used in processing classical information, and cleartext can be transferred through quantum channel. There is no information revealed. As for the vector attack, according to quantum no-cloning theorem, the attacker cannot accurately copy quantum nodes for DOS attack. If the attacker generates illegal users to prevent information transmission, it will be found in the authentication process by the key management system and the illegal communication will be terminated.

4.4.1. Attack via Direct Measurement

One can analyze the security of multicast data packet communication via direct measurement. $F_i(i = 1, 2, \cdots, M)$ receives the random $(4n + \delta)$ qubits, who measures each qubits in the basis σ_x or σ_z at random. $S_i(i = 1, 2, \cdots, N)$ receives $\varepsilon(|\Psi_0\rangle \langle\Psi_0|)$, where ε describes the quantum operation due to the combined effect of the channel and eavesdropper's (Eve) actions. $S_i(i = 1, 2, \cdots, N)$ then publicly announces this fact. For now, each of the $N + 1$ nodes has its own states described by separate density matrices. Note that, at this point, since S_0 did not reveal b, Eve has no knowledge of what basis she should have measured to eavesdrop in the communication. At best, she can only guess. If her guess were wrong, then she would have disturbed the state received by $S_i(i = 1, 2, \cdots, N)$. Moreover, whereas in reality the noise ε may be partially due to the environment in addition to Eve's eavesdropping, it does not help Eve to have complete control over the channel. Thus, Eve is entirely responsible for ε.

When the quantum multicast router first receives a multicast packet from S_1, the packet check is performed, using the routing table to verify that the packet arrived on the right interface for the packet's source. If the packet arrived on any other interface, drop it.

4.4.2. Attack via Ancilla Particle

We suppose Eve intercepts the particle sent by Alice, which will be entangled with an ancilla $|e\rangle$ prepared by Eve. The unitary transformation that is implemented on Alice's particle E does not change the state of single photons [27].

$$\begin{aligned}
E \otimes |0e\rangle &= a\,|0e_{00}\rangle + b\,|1e_01\rangle\,,\\
E \otimes |1e\rangle &= b'\,|0e_{00}\rangle + a'\,|1e_01\rangle\,,\\
E \otimes |+e\rangle &= \frac{1}{2}[|+\rangle\,(a\,|e_{00}\rangle + b\,|e_{01}\rangle + b'\,|e_{10}\rangle + a'\,|e_{11}\rangle) + |-\rangle\,(a\,|e_{00}\rangle - b\,|e_{01}\rangle + b'\,|e_{10}\rangle - a'\,|e_{11}\rangle)],\\
E \otimes |-e\rangle &= \frac{1}{2}[|+\rangle\,(a\,|e_{00}\rangle + b\,|e_{01}\rangle - b'\,|e_{10}\rangle - a'\,|e_{11}\rangle) + |-\rangle\,(a\,|e_{00}\rangle - b\,|e_{01}\rangle - b'\,|e_{10}\rangle + a'\,|e_{11}\rangle)],
\end{aligned} \tag{18}$$

where the unitary transformation E can be written as

$$E = \begin{pmatrix} a & b' \\ b & a' \end{pmatrix}, \tag{19}$$

where $|a|^2 = |a'|^2$, $|b|^2 = |b'|^2$, and $|a|^2 + |b|^2 = 1$. Thus, the probability of Eve being detected is

$$P_e = |b|^2 = 1 - |a|^2 = \left|b'\right|^2 = 1 - \left|a'\right|^2, \tag{20}$$

the eavesdropping brings a certain amount of error rate, and it must be detected.

According to the information theory, the amount of maximum accessible information in quantum system is limited by *Holevo* limit:

$$\chi(\psi) = S(\psi) - \sum_i p_i S(\psi_i), \tag{21}$$

where $S(\psi)$ is the von Neumann entropy of state ψ, $\psi = \sum_i p_i \psi_i$, and ψ_i is a state prepared in probability p_i. If communicating parties prepare states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, then the information entropy $H(p) = -\sum_i p_i log_2 p_i = 2$. Thus the von Neumann entropy of Eve [27] is $S(\psi') = 0 < H(P)$. It seems that Eve cannot obtain the complete information of photons in our protocol.

5. Conclusions

We describe a multi-user broadcast protocol in network for the one-to-many multicast communication network including the master and N slave mode using a sequence of single photons. This protocol might be useful in practice because it guarantees multicast information robustness. In the one-to-many multicast communication mode, S_0 creates $(4n + \delta)$ random bits and multicasts information to $S_i (i = 1, 2, \cdots, N)$. S_0 and S_i publicly announce the selection of the random measurement basis. There are at least $2n$ bits left, and if not, the protocol will be aborted. Meanwhile, the Calderbank–Shor–Steane (CSS) coding theory can be employed for correcting the errors introduced by the noisy communication channel. Therefore, the $N + 1$ nodes compute the related information, and finally obtains the correct key. The commercial success of quantum key distribution for the generation of a private shared secret key motivates this investigation. The protocol is also proved to be unconditionally secure in theory, which indicates its feasibility in theoretical application. For future study, it may be significant to investigate the performance of our protocol for encoding secret classical messages.

In our proposed protocol, the photon is the carrier of information. Quantum information is encoded in the flying photon bit, and the transmit power is related to the performance of the transmitter module. In practical quantum communication, the transmission distance is limited due to the imperfection of the transmitter module and the detection module, which is a general problem in all practical quantum communication systems.

This protocol mainly establishes the quantum multi-user communication model without considering channel noise. In the practical noisy channel, we can use the quantum error-correction code to correct the error generated in the transmission process. Commonly used quantum error-correction codes are Quantum Stabilizer Code (QSC) and Quantum Low-Density Party-Check Code (QLDPC) [28].

One thing to point out is that we concentrate only on closed systems where the decoherence and dissipations are neglected. It is well-known that in open quantum systems the Hamilton operator is non-Hermitian [29,30]. The dynamical behavior of open quantum systems plays a key role in many applications of quantum mechanics, such as the environment-induced decay of quantum coherence, relaxation in many-body systems, and applications in condensed matter theory, quantum transport, quantum chemistry, and quantum information. If the decoherence and dissipation of the open systems are considered, the protocol based on quantum error correction coding needs to be studied in the future in more detail.

Author Contributions: Conceptualization, H.M.; methodology, H.M. and P.S.; validation, N.L. and S.W.; investigation, S.W. and Z.L.; writing—original draft preparation, P.S. and H.M.; writing—review and editing, P.S. and N.L.; and visualization, M.R.

Funding: This work was supported by the Project of Shandong Province Higher Educational Science and Technology Program (No. J18KZ012), the National Natural Science Foundation of China (Nos. 61772295 and 11975132), and the Natural Science Foundation of Shandong Province (No. ZR2016FB09).

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Singh, H.; Sachdev, A. The Quantum way of Cloud Computing. In Proceedings of the 2014 International Conference on Reliability Optimization and Information Technology (ICROIT), Faridabad, India, 6–8 February 2014; pp. 397–400.
2. Keller, E.; Rexford, J. The "Platform as a Service" Model for Networking. In Proceedings of the 2010 Internet Network Management Workshop/Workshop on Research on Enterprise Networking (INM/WREN), San Jose, CA , USA, 27 April 2010; pp. 95–108.
3. Bennett, C.H.; Brassard, G. WITHDRAWN: Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Bangalore, India, 9–12 December 1984; p. 175.
4. Loukopoulos, K.; Browne, D.E. Secure multiparty computation with a dishonest majority via quantum means. *Phys. Rev. A* **2010**, *81*, 062336. [CrossRef]
5. Ma, H.; Chen, B.; Guo, Z.; Li, H. Development of quantum network based on multiparty quantum secret sharing. *Can. J. Phys.* **2008**, *86*, 1097–1101. [CrossRef]
6. Zhou, N.R.; Cheng, H.L.; Gong, L.H.; Li, C.S. Three-Party Quantum Network Communication Protocols Based on Quantum Teleportation. *Int. J. Theor. Phys.* **2014**, *53*, 1387–1403. [CrossRef]
7. Matsumoto, R.Multiparty quantum-key-distribution protocol without use of entanglement. *Phys. Rev. A* **2007**, *76*, 062316. [CrossRef]
8. Yan, F.L.; Gao, T. Quantum secret sharing between multiparty and multiparty without entanglement. *Phys. Rev. A* **2005**, *72*, 012304. [CrossRef]
9. Woodhead, E. Quantum cloning bound and application to quantum key distribution. *Phys. Rev. A* **2013**, *88*, 012331. [CrossRef]
10. Iblisdir, S.; Acín, A.; Cerf, N.J.; Filip, R.; Fiurášek, J.; Gisin, N. Multipartite asymmetric quantum cloning. *Phys. Rev. A* **2005**, *72*, 042328. [CrossRef]
11. Bužek, V.; Braunstein, S.L.; Hillery, M.; Bruß, D. Quantum copying: A network. *Phys. Rev. A* **1997**, *56*, 3446–3452. [CrossRef]
12. Andersen, U.L.; Josse, V.; Leuchs, G. Unconditional Quantum Cloning of Coherent States with Linear Optics. *Phys. Rev. Lett.* **2005**, *94*, 240503. [CrossRef]
13. Scarani, V.; Iblisdir, S.; Gisin, N.; Acín, A. Quantum cloning. *Rev. Mod. Phys.* **2005**, *77*, 1225–1256. [CrossRef]
14. Fang, B.L.; Song, Q.M.; Ye, L. Realization of a universal and phase-covariant quantum cloning machine in separate cavities. *Phys. Rev. A* **2011**, *83*, 042309. [CrossRef]

15. Wootters, W.K.; Zurek, W.H. A single quantum cannot be cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]
16. Fan, H.; Matsumoto, K.; Wang, X.B.; Wadati, M. Quantum cloning machines for equatorial qubits. *Phys. Rev. A* **2001**, *65*, 012304. [CrossRef]
17. Bruß, D.; Cinchetti, M.; Mauro D'Ariano, G.; Macchiavello, C. Phase-covariant quantum cloning. *Phys. Rev. A* **2000**, *62*, 012302. [CrossRef]
18. Fan, H.; Wang, Y.N.; Jing, L.; Yue, J.D.; Shi, H.D.; Zhang, Y.L.; Mu, L.Z. Quantum cloning machines and the applications. *Phys. Rep.* **2014**, *544*, 241–322. [CrossRef]
19. Fan, H.; Imai, H.; Matsumoto, K.; Wang, X.B. Phase-covariant quantum cloning of qudits. *Phys. Rev. A* **2003**, *67*, 022317. [CrossRef]
20. Gisin, N.; Massar, S. Optimal Quantum Cloning Machines. *Phys. Rev. Lett.* **1997**, *79*, 2153–2156. [CrossRef]
21. Eleuch, H. Quantum Trajectories and Autocorrelation Function in Semiconductor Microcavity. *Appl. Math. Inf. Sci.* **2009**, *3*, 185–196.
22. Mohamed, A.B.; Eleuch, H. Non-classical effects in cavity QED containing a nonlinear optical medium and a quantum well: Entanglement and non-Gaussianity. *Eur. Phys. J. D* **2015**, *69*, 191. [CrossRef]
23. Berrada, K.; Abdel-Khalek, S.; Eleuch, H.; Hassouni, Y. Beam splitting and entanglement generation: Excited coherent states. *Quantum Inf. Process.* **2013**, *12*, 69–82. [CrossRef]
24. Lütkenhaus, N.; Calsamiglia, J.; Suominen, K.A. Bell measurements for teleportation. *Phys. Rev. A* **1999**, *59*, 3295–3300. [CrossRef]
25. Zeng, G.; Keitel, C.H. Arbitrated quantum-signature scheme. *Phys. Rev. A* **2002**, *65*, 042312. [CrossRef]
26. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
27. Cao, Z.W.; Zhao, G.; Zhang, S.H.; Feng, X.Y.; Peng, J.Y. Quantum secure direct communication protocol based on the mixture of Bell state particles and single photons. *Acta Phys. Sin.* **2016**, *65*, 230301.
28. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*, 1st ed.; Cambridge University Press: Cambridge, UK, 2000.
29. Eleuch, H.; Rotter, I. Resonances in open quantum systems. *Phys. Rev. A* **2017**, *95*, 022117. [CrossRef]
30. Eleuch, H.; Rotter, I. Open quantum systems and Dicke superradiance. *Eur. Phys. J. D* **2014**, *68*, 74. [CrossRef]