sensors

MDPI

Article

Counterfactual Anonymous Quantum Teleportation in the Presence of Adversarial Attacks and Channel Noise

Saw Nang Paing, Jason William Setiawan, Shehbaz Tariq, Muhammad Talha Rahim, Kyesan Lee * and Hyundong Shin *

Department of Electronics and Information Convergence Engineering, Kyung Hee University, Yongin 17104, Korea

* Correspondence: kyesan@khu.ac.kr (K.L.); hshin@khu.ac.kr (H.S.)

Abstract: Hiding the identity of involved participants in the network, known as anonymity, is a crucial issue in some cryptographic applications such as electronic voting systems, auctions, digital signatures, and Byzantine agreements. This paper proposes a new anonymous quantum teleportation protocol based on counterfactual communication where no information-carrying particles pass through the channel. It is achieved by the distribution of a counterfactual entanglement among the participants in the network followed by the establishment of an anonymous entanglement between the sender and the receiver. Afterwards, the sender can anonymously teleport a quantum state to the receiver by utilizing the anonymous entanglement. However, the practicality of the anonymous quantum network mainly calls for two performance measures—robustness against adversarial attacks and noisy environments. Motivated by these demands, firstly, we prove the security of our proposed protocol and show that it achieves both the sender and receiver's anonymity in the presence of active adversaries and untrusted parties. Along with anonymity, we also ensure the correctness of the protocol and the privacy of the teleported qubit. Finally, we analyze the robustness of our proposed protocol under the presence of channel noise and compare its fidelity with those of the conventional protocols. The main advantage of our proposed protocol is that it can provide useful anonymous quantum resources for teleportation under noisy environment with a higher security compared to previous protocols.

Keywords: counterfactual; robustness; security; correctness; anonymity; noise-tolerance level

Citation: Nang Paing, S.; Setiawan, J.W.; Tariq, S.; Talha Rahim, M.; Lee, K.; Shin, H. Counterfactual Anonymous Quantum Teleportation in the Presence of Adversarial Attacks and Channel Noise. *Sensors* **2022**, *22*, 7587. https://doi.org/10.3390/s22197587

Academic Editor: Evangelos Kranakis

Received: 31 August 2022
Accepted: 2 October 2022
Published: 6 October 2022

1. Introduction

Quantum cryptography has brought a lot of interesting, secure communication protocols such as quantum key distribution [1], quantum secure direct communication [2], quantum secret sharing [3], quantum private comparison [4], etc., under the laws of quantum mechanics. These protocols ensure the unconditional security of the transmitted message, i.e., the content of the transmitted information is learned only by the sender and the receiver. At the same time, the irrelevant participants or adversaries get no knowledge of it. However, not all communication applications are confined only to the security of the message. Some cryptographic applications, such as electronic voting, auction, digital signature, Byzantine agreement, etc., require hiding the participants' identities to complete the task without bias. This hiding of participants' identities while accomplishing the communication task is known as anonymity. Hence, anonymity is important in securing the identity of communicating parties, just as absolute security is crucial to the confidentiality of the secret message.

The first classical anonymous protocol proposed in [5] demonstrated the unconditional tracelessness of the message sender and receiver. This protocol determines if a dinner bill is paid anonymously without disclosing any other information. Each cryptographer at the dining table secretly flips an unbiased coin with their right neighbor; hence, they can see

the coin they flipped and the coin their left neighbor flipped. The cryptographers then announce the state of the two coins, the same or different sides. If one of the cryptographers is the payer, they reveal the opposite result. After that, they compute the sum of all the announcements. If the sum equals one, one of them pays the dinner bill. Hence, this protocol enables the anonymous transmission of one bit that confirms the payment.

Later, by incorporating quantum mechanics, it was expanded to the quantum version of anonymous transmission [6]. Although this protocol used quantum resources, we could only use it for the transmission of classical messages anonymously. To address this limitation, a Greenberger–Horne–Zeilinger (GHZ) based anonymous communication protocol that allowed the transmission of quantum information was proposed in [7]. The key concept behind this idea was to distribute an anonymous entanglement between the sender and the receiver, followed by the desired communication task. In addition to the multipartite entanglement-based protocols, an entanglement relay-based quantum anonymous transmission protocol was proposed [8]. The protocol was proved privacy-preserving and could enable long-distance anonymous quantum communication. However, most of the anonymous quantum communication protocols did not take channel noise into consideration. Hence, a W-state-based quantum anonymous transmission protocol that outperformed the GHZ state-based and entanglement relay-based protocols in the presence of noise was proposed [9]. To date, various anonymous quantum communication protocols have been proposed based on single particles, Bell states, GHZ states, and W states [10–21]. In order to employ these protocols in practical network scenarios, they must be able to provide the desired communication task under the presence of adversaries and a noisy environment. However, all of these protocols have one thing in common—the particle that travels across the quantum channel to fulfill the communication task can be intercepted by adversaries, failing communication. In addition, most of these protocols do not provide a noise analysis.

To compensate for the aforementioned issues, we propose a new anonymous quantum teleportation protocol which makes use of counterfactual communication. By enabling the transmission of information without any information-carrying particle passing through the channel, counterfactual communication prevents attacks that rely on the intercepted information-carrying particle in the channel. Counterfactual communication arises from the interaction-free measurement, which infers the presence of a bomb without touching it with 25% probability [22]. With the integration of the quantum Zeno effect [23], this probability approaches unity and leads to the counterfactual transmission of the one-bit value. The gate that enables this kind of operation is called the quantum Zeno (QZ) gate. By inserting a QZ gate within another QZ gate, known as a chained quantum Zeno (CQZ) gate, the counterfactual communication of two-bit values is achieved [24]. Recently, counterfactual communication has been applied to different areas, including quantum cryptography, quantum computing, and quantum communication [25–31].

Most of the previous anonymous quantum communication protocols rely on the preshared entanglement among the participants in the network. In this work, we counterfactually distribute the entanglement among the participants and accomplish the task of anonymous quantum teleportation. In order to meet the requirements of practical quantum networks, we perform a security and noise analysis for our proposed protocol. The security of our proposed protocol is ensured by examining it under counterfactual man-in-the-middle attacks and Trojan horse attacks. For the noise analysis, we evaluate the performance of our proposed protocol in the presence of channel noise and compare it with the performance of relay-based and GHZ-based anonymous quantum communication. The rest of the paper is as follows: Section 2 describes the preliminaries followed by our proposed method. Section 3 analyzes the performance of the protocol with emphasis on its security, accuracy, privacy, and noise. Section 4 describes the application of our proposed protocol in an IoT network. Finally, Section 5 gives our conclusion.

2. Materials and Methods

2.1. Preliminaries

This section introduces the basic theorems and gates utilized in our counterfactual anonymous quantum teleportation protocol.

2.1.1. Collision Detection

Theorem 1. *The collision detection protocol allows the detection of the existence of multiple senders in one round of the protocol. The protocol starts by allowing each participant to input one bit. Let v represent the number of "1's" inputted by all participants in the network. The protocol has three possible outcomes depending on the value of v: (i) no participant wants to perform the communication task ($v = 0$), (ii) only one participant wants to perform the communication task ($v = 1$), and (iii) more than one participant wants to perform the communication task ($v \geq 2$). If all the participants in the network are honest, the protocol outputs the correct result with a probability exponentially close to 1 [13]. The correctness of the protocol does not allow any individual participant to terminate the protocol. The adversary gains no additional information even if the protocol is implemented correctly, except for them allocating random bit values rather than "0" to all conspiring participants [32]. Due to its similarity with the veto protocol [33], the presence of a single corrupt participant will lead to the outcome corresponding to (iii), regardless of the inputs of the other participants. Hence, no cheating is possible, and the protocol succeeds in detecting collisions in the presence of adversaries.*

2.1.2. Notification Protocol

Theorem 2. *The notification protocol allows any participant in the network to notify other participants of their preference. Each participant outputs a private bit that indicates whether or not they have been notified at least once. The value of the bit is correctly calculated with a probability exponentially close to 1 [14,32,33].*

2.1.3. Anonymous Broadcast of Classical Message

Theorem 3. *When a sender anonymously broadcasts their message s to n participants in the network, it must meet the following criteria [32,33]:*

1 *Every participant in the network receives the message s;*
2 *The identity of the sender remains hidden from any adversary, i.e., if the adversary has control over t participants, the probability that they can correctly guess the identity of the sender is no more than $1/(n-t)$;*
3 *Any malicious behavior against the protocol is discovered.*

2.1.4. CQZ Gate

A chained quantum Zeno (CQZ) gate [24] is used to realize the logic of counterfactual communication, which is a nested version of the quantum Zeno (QZ) gate. We can implement it using optical components such as polarizing beam splitters (PBS), switchable polarization rotator (SPR), switchable mirrors (SM), mirrors (MR), optical delays (OD), and photon detectors (D), as shown in Figure 1. The gate that takes an H(V)-polarized photon as input is called H(V)-CQZ gate, respectively. To initiate the CQZ gate, Alice inputs the photon into the gate and it gets rotated by the SPR. Here, we denote $\mathrm{SPR}^{H(V)}$ as the SPR used in the H(V)-QZ gate, and its function can be described as

$$|H(V)\rangle \rightarrow \cos\theta\,|H(V)\rangle + \sin\theta\,|V(H)\rangle\,, \tag{1}$$

$$|V(H)\rangle \rightarrow \cos\theta\,|V(H)\rangle - \sin\theta\,|H(V)\rangle\,, \tag{2}$$

respectively, where θ is the rotation angle. Let us denote $\theta_N = \pi/2N$ and $\theta_M = \pi/2M$ as the angles rotated by the SPR in the inner and outer QZ gates, respectively, where $N(M)$ represents the number of inner (outer) cycles. After the photon has been rotated by the SPR, the PBS separates it into two components; one component goes into path 0, where it gets stored for a certain period, and the other goes into the inner QZ gate via path 1. The

photon component in path 1 gets rotated by another SPR and is again separated into two parts by another PBS; one component gets stored in path 1 while the other component is transmitted into the quantum channel through path 2.

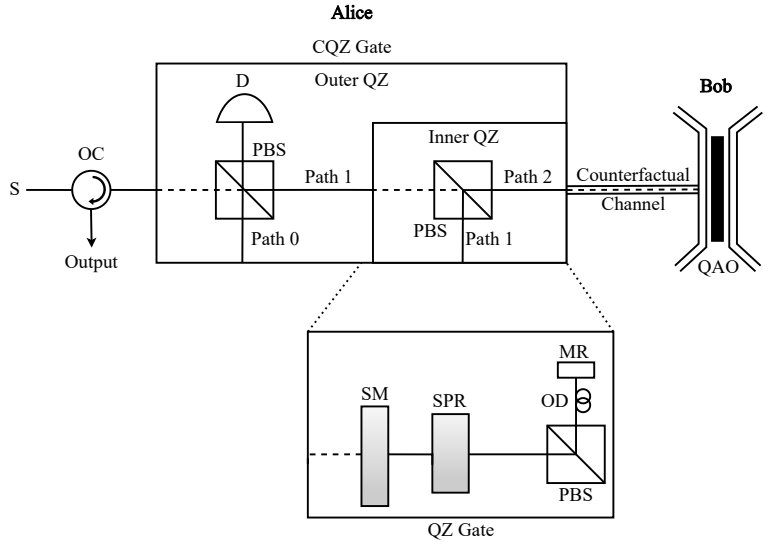

Figure 1. Chained quantum Zeno (CQZ) gate. It is a nested version of the quantum Zeno (QZ) gate where Alice inputs a source photon (S), which can be an H- or V-polarized photon. It is made up of a set of optical devices, including switchable mirrors (MR), switchable polarization rotators (SPR), polarizing beam splitters (PBS), optical delays (OD), mirrors (MR), optical circulator (OC), and detectors (D). Once the photon enters into the CQZ gate, it gets collapsed into three different paths, namely path 0, path 1, and path 2, due to the SPRs and PBSs in the outer and inner QZ gates. Only the photon component in path 2 enters into the quantum channel. Bob, who is on the other side of the quantum channel, holds a quantum absorptive object (QAO), which is a superposition of absence and presence states of absorptive object (AO). He decides whether to absorb or not that photon component by inserting or not inserting AO. For a complete CQZ gate operation, the photon experiences M cycles of the outer QZ gate where each outer cycle consists of N cycles of the inner QZ gate. The logical operation of the CQZ gate is that it retains (rotates) the polarization of the incoming source photon in the absence (presence) of AO.

Bob, on the other side of the transmission channel, decides whether to absorb or reflect the photon. If he decides to absorb the incoming photon, he inserts the absorptive object (AO) at their side of the transmission channel. Otherwise, he does nothing. If the photon component that enters the transmission channel is not absorbed by AO and reflected from Bob's side, it combines with the photon component in path 1 and goes to the start of the inner QZ gate. Otherwise, the next inner cycle starts with only the photon component in path 1. After this procedure is repeated N times in the inner QZ gate, the photon component that comes out of the inner QZ gate combines with the photon component in path 0 at the PBS of the outer QZ gate. The resulting photon after the PBS is used again for the next cycle of the outer QZ gate. In case of the absence of AO, it is discarded at detector D to ensure counterfactuality. Finally, we can describe the state of the photon after the CQZ gate with M outer and N inner cycles in the absence and presence of AO as follows:

$$Absence : |H(V)\rangle \rightarrow \cos m\theta_M |H(V)\rangle + \sin m\theta_M |V(H)\rangle \xrightarrow{m=M} |H(V)\rangle , \quad (3)$$

$$Presence : |H(V)\rangle \rightarrow \cos^{m-1}\theta_M(\cos\theta_M |H(V)\rangle + \sin\theta_M |V(H)\rangle) \xrightarrow{m=M} |V(H)\rangle . \quad (4)$$

Thus, if Bob does not insert an AO, the polarization of the photon sent by Alice remains the same with probability $\eta_1 = \cos^{2M}\theta_M$; otherwise, the photon with opposite polarization is

resulted with probability $\eta_2 = \prod_{m=1}^{M}\left(1-\sin^2(m\theta_M)\sin^2\theta_N\right)^{KN}$ [31]. These probabilities tend to 1 as N and M approach infinity.

2.2. Counterfactual GHZ State Distribution

Consider a network that consists of a server and K participants. The server prepares a quantum AO (QAO), which is the superposition of the absence and presence states of an AO, as $|C\rangle = \frac{|0\rangle_C+|1\rangle_C}{2}$. Meanwhile, each participant holds an H-polarized photon and prepares an H-CQZ gate. Here, $|0\rangle_C$ ($|1\rangle_C$) represents the absence (presence) of AO and the H(V)-polarized photon is denoted as $|0\rangle_{P_i}$ ($|1\rangle_{P_i}$) where $i \in \{1,2,...,K\}$. Using the tripartite counterfactual entanglement distribution in [34], we extend it to a multipartite case. As the server is responsible for the counterfactual GHZ state distribution, the H-CQZ gate of each participant P_i is connected to the server via the switch L as shown in Figure 2.

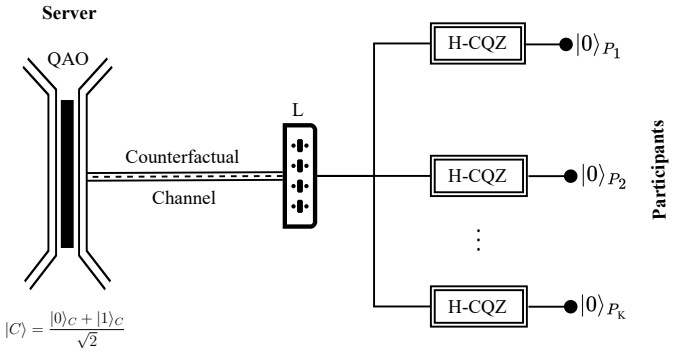

Figure 2. Counterfactual GHZ state distribution. Consider a network that consists of a server and K participants. The server holds a QAO which is in the state $|C\rangle = \frac{|0\rangle_C+|1\rangle_C}{2}$ while the K participants hold H-polarized photons denoted as $|0\rangle_{P_i}$ where $i \in \{1,2,...,K\}$. Each participant performs an H-CQZ operation upon establishing a connection with the server through the switch L. Once all the K participants have completed their respective H-CQZ operations in a consecutive manner, a $K+1$ partite GHZ state is distributed among the K participants and the server, as described in Equation (8).

To start the protocol, the server connects P_1 through the switch L and P_1 inputs their H-polarized photon $|0\rangle_{P_1}$ into the H-CQZ gate. As described in Section 2.1, the logical operation of the H-CQZ gate is that it completely rotates the polarization of the incoming photon in the presence of an AO and retains the polarization in the absence of a photon. If the photon is not lost during the operation of the CQZ gate, the initial combined state of the server and the participants becomes

$$|\psi_0\rangle = \left(\frac{|0\rangle_C + |1\rangle_C}{\sqrt{2}}\right) \otimes |0\rangle_{P_1} \otimes |0\rangle_{P_2} \otimes \ldots \otimes |0\rangle_{P_K} \tag{5}$$

and changes into

$$|\psi_1\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\eta_1}\,|00\rangle_{CP_1} + \sqrt{\eta_2}\,|11\rangle_{CP_1}\right) \otimes |0\rangle_{P_2} \otimes \ldots \otimes |0\rangle_{P_K}, \tag{6}$$

where η_1 and η_2 correspond to the success probabilities of counterfactual communication in the presence and absence of an AO, respectively. The CQZ operation between the server and P_1 establishes entanglement between them while the qubits of the other participants remain separated.

Next, the server closes its connection with P_1 and establishes a new connection with P_2. P_2 sends their photon towards their respective H-CQZ gate, which undergoes M outer

and N inner cycles of the CQZ gate. If it does not get discarded after the gate, the state $|\psi_1\rangle$ becomes

$$|\psi_2\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\eta_1^2}\,|000\rangle_{CP_1P_2} + \sqrt{\eta_2^2}\,|111\rangle_{CP_1P_2}\right) \otimes |0\rangle_{P_3} \otimes \ldots \otimes |0\rangle_{P_K}. \tag{7}$$

The entanglement gets counterfactually distributed between the server, P_1, and P_2. The success probability of the operation is $\eta_1^2/2$ in the absence of an AO and $\eta_2^2/2$ in its presence. The server repeats the same procedure with P_3 to P_N by varying the switch L. If the photon of each participant comes out of their respective CQZ gate successfully, the final state of the system becomes

$$|\psi_K\rangle = \frac{1}{\sqrt{2}}\left(\sqrt{\eta_1^K}\,|000...0\rangle_{CP_1P_2...P_N} + \sqrt{\eta_2^K}\,|111...1\rangle_{CP_1P_2...P_K}\right) \tag{8}$$

Finally, the $K+1$-partite GHZ state gets established between the server and the K participants.

To achieve perfect GHZ state distribution, we can increase the number of inner and outer cycles of the CQZ gates. In Figure 3, we plot the success probability of counterfactual GHZ state distribution for 50 parties with 2000 inner and 200 outer cycles. It can be seen from the graph that as the values of N and M approach infinity, the values of η_1^K and η_2^K tend to 1, leading to perfect counterfactual GHZ state distribution.

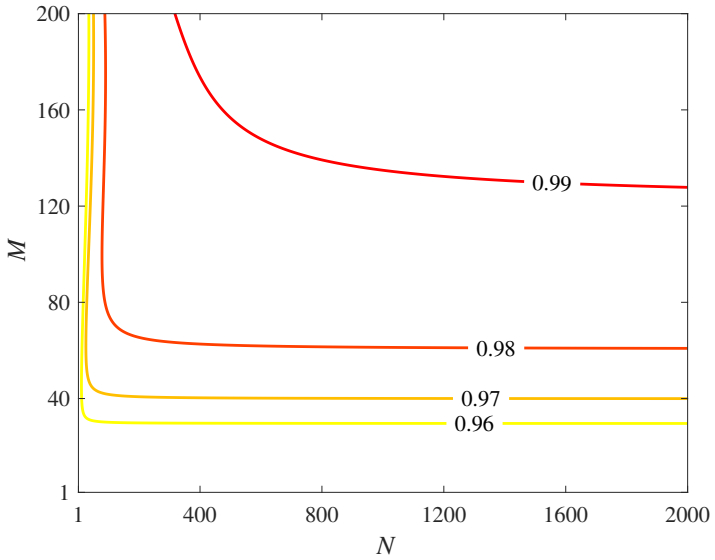

Figure 3. The success probability of counterfactual GHZ state distribution for a network of 50 participants where the CQZ gate held by each participant has $N = 2000$ and $M = 200$ of inner and outer cycles, respectively.

2.3. Counterfactual Anonymous Quantum Teleportation (CAQT)

Most quantum communication protocols rely on the preshared entanglement to carry out the communication tasks. In the absence of preshared entanglement, communication between the individual parties cannot take place. In practice, preshared entanglement is severely degraded by the decoherence mechanism, resulting in mixed entangled states instead of pure entangled states. As a result, it has a detrimental influence on the performance of communication tasks [35]. In this article, we assume that each participant holds a single qubit, and no entanglement exists between them. Suppose that a network consists of a server and K participants where a quantum channel and classical authenticated channel exist between the server and each participant. By utilizing the method described in Section 2.2, all the participants in the network counterfactually create $J + \delta_1 + \delta_2$ numbers of GHZ state among themselves.

Anonymous quantum teleportation requires anonymous entanglement between the sender and the receiver. It requires an entangled channel between the sender and the receiver while their identities remain hidden from the rest of the network. In this setup, only one participant in the network can be the sender. Since multiple senders may be active simultaneously, they need to run the collision detection protocol described in Section 2.1.1 to avoid the failure of the protocol. When all the participants in the network get an agreement on the communication of one sender, the sender uses the notification protocol defined in Section 2.1.2 to inform the receiver anonymously. Afterward, the following steps are required to achieve the anonymous entanglement between the sender and receiver, as illustrated by the circuit diagram in Figure 4.

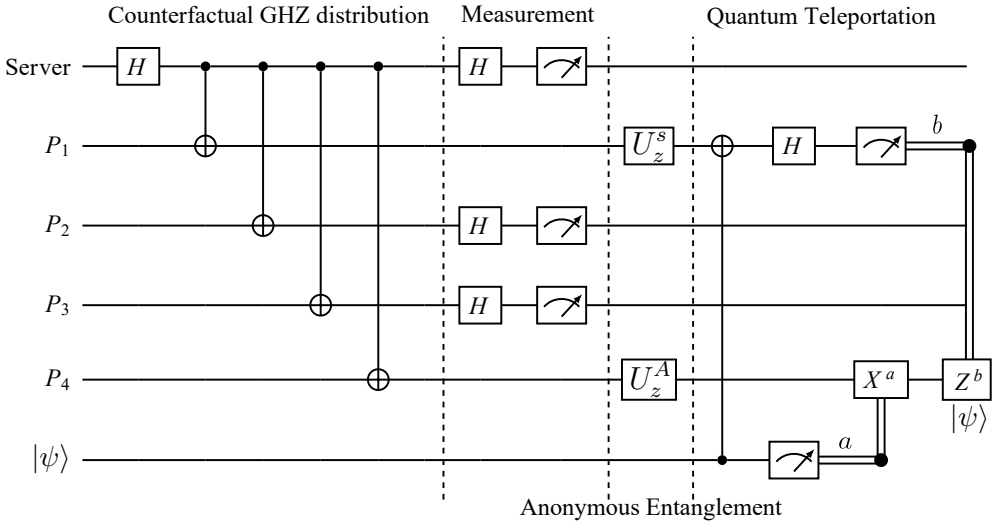

Figure 4. Circuit diagram of counterfactual anonymous quantum teleportation for a network consisting of a server and four participants (P_1, P_2, P_3 and P_4). Here, we consider P_1 as the anonymous sender and P_4 as the anonymous receiver. P_1 anonymously wants to send the message $|\psi\rangle$ to their preferred receiver P_4 through the counterfactually distributed GHZ state. After the counterfactual GHZ state distribution, all participants except the sender and receiver measure their respective qubits in the $\mathcal{X}$ basis and announce the results through the classical channel while the sender and the receiver announce the random classical bit. Then, the sender performs U_z^s on their qubit, where s denotes the random classical bit created by the server. On the other hand, the receiver performs U_z^A on their qubit, where A represents the XOR value of the classical announcements of all the other participants except him. Once the anonymous entanglement is established between the sender and the receiver, they perform quantum teleportation in an anonymous manner based on that resource.

Step 1: For the anonymous entanglement to be reliable, it is necessary to check the security of the counterfactually distributed GHZ states. Different partite GHZ states collapse into other states when measured using a different basis. Thus, the server randomly chooses δ_1 numbers of GHZ states and instructs the participants to measure their corresponding qubits using random basis $\{\mathcal{X}, \mathcal{Z}\}$ and announce their results. The server then determines whether or not the measurement results fall into the right form of $K+1$ GHZ basis. If the results are correct, the rest of the $J+\delta_2$ numbers of GHZ states are employed to establish the anonymous entanglement.

Step 2: For the remaining $J+\delta_2$ number of GHZ states, apart from the sender and receiver, every participant, including the server, measures their corresponding qubits in the $\mathcal{X}$ basis and stores the results as $\left\{m_i^j\right\}$ where i corresponds to the ith participant, j corresponds to the jth GHZ state and $j \in \{1, 2, ..., J\}$.

Step 3: The sender randomly creates a string $s = \left\{s^1, s^2, ..., s^J\right\}$ and applies $U_z = |0\rangle\langle 0| - |1\rangle\langle 1|$ on their qubits if $s^j = 1$.

Step 4: The receiver also randomly creates a string $r = \left\{r^1, r^2, ..., r^J\right\}$.

Step 5: Using the anonymous broadcasting protocol described in Section 2.1.3, all the participants announce their classical message string through the broadcast channel. Then, the one who gets a notification, the receiver, calculates the XOR of all the broadcast classical message as follows:

$$A^j = r^j \oplus \left(\bigoplus_{i=11}^{K+1} m_i^j \right) \tag{9}$$

If $A^j = 1$, they perform U_z on their qubit and the entanglement of the form $|\psi^+\rangle = |00\rangle + |11\rangle/\sqrt{2}$ has been anonymously distributed between the sender and receiver.

Step 6: To verify the created anonymous entanglement, for each round of anonymous entanglement creation, the sender randomly decides whether to use it for security checking or anonymous teleportation. In the case of security checking, the sender measures their qubit in $\mathcal{X}$ basis. Then, the server announces the measurement basis and sends the bit value 1 to the receiver via the classical broadcast channel, indicating that they are performing security checking. On the other hand, if the sender wishes to perform anonymous teleportation, they do not measure their qubit. Instead, they announce the random measurement basis and sends the bit 0 to the receiver via the classical broadcast channel. The receiver has to check the bit received from the classical broadcast channel before performing any measurement on their qubit. If it is 1, they measure their qubit using the announced basis. Otherwise, they do nothing on their qubit.

Step 7: Step 2 to 6 is run for $J + \delta_2$ times. If δ_2 rounds of anonymous entanglement is chosen for security checking, the sender performs the quantum teleportation protocol on the remaining J numbers of anonymous entangled pairs.

3. Results and Discussion

3.1. Performance Analysis of CAQT in the Presence of Adversaries

In this section, firstly, we prove the correctness of our proposed protocol. Then, we analyze the security of the GHZ state that is counterfactually distributed among the participants, since it is the main step of our proposed protocol. Afterward, we prove the anonymity of the sender and receiver and the privacy of the teleported qubit in the presence of adversaries.

3.1.1. Correctness of CAQT

Suppose that all the participants in the network are honest, and the perfect counterfactual entanglement gets established among them by using multiple numbers of N and M for each CQZ gate. Then, $\eta_1^K = \eta_2^K \approx 1$ and the state $|\psi_K\rangle$ becomes

$$|\psi_K\rangle \approx \frac{1}{\sqrt{2}} \Big(|000...0\rangle_{CP_1P_2...P_K} + |111...1\rangle_{CP_1P_2...P_K} \Big). \tag{10}$$

When all the participants in the network except the sender and receiver have performed $\mathcal{X}$ basis measurement on the shared counterfactual GHZ state in step 1, the state $|\psi_K\rangle$ transforms to

$$\begin{aligned} |\psi_K\rangle &\rightarrow I_S \otimes I_R \otimes \mathcal{X}^{\otimes K-2} \left(\frac{1}{\sqrt{2}} (|000...0\rangle_{CP_1P_2...P_K} + |111...1\rangle_{CP_1P_2...P_K}) \right) \\ &= \frac{1}{\sqrt{2}} \Big(|00\rangle_{SR} + (-1)^l |11\rangle_{SR} \Big) \otimes \left(\bigotimes_{i=1, i\neq S,R}^{K+1} |x\rangle \right), \end{aligned} \tag{11}$$

where S (R) represents the sender (receiver), $l = \bigoplus_{i=1, i\neq S,R}^{K+1} |x|$, $x \in \{+, -\}$ and $+(-)$ denotes the value $0(1)$.

In the above Equation (11) , if there is an odd number of $|-\rangle$ results in the $\mathcal{X}$ basis measurement, i.e., $l = 1$, the entanglement shared between the sender and the receiver

is $|\phi^-\rangle_{SR} = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$. Otherwise, they share the desired entanglement of the form $|\phi^+\rangle_{SR} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Thus, the receiver must apply $\mathcal{U}_z$ on their qubit if $l = 1$ to get the desired shared entanglement. The result A calculated by the receiver in step 4 of our proposed protocol will agree with the value of l. The argument will be true regardless of the sender broadcasting 0 or 1. Hence, our protocol can provide the correct anonymous entanglement between the sender and the receiver.

3.1.2. Security of Counterfactual GHZ State

The reliability of the anonymous entanglement in our proposed protocol depends on the counterfactual GHZ state. Thus, it is necessary to evaluate whether the adversaries become anonymously entangled with the valid $K+1$ counterfactual GHZ state. In the counterfactual context, the adversary (Eve) is accessible only to the quantum channel between the two end parties. Since only the H photon component, which carries no information, passes through the quantum channel in the H-CQZ gate, no information is available to Eve from the quantum channel [36]. Therefore, Eve cannot apply conventional attack strategies to get the quantum and classical side information. She must set up the counterfactual setting and attempt to perform possible attacks such as man-in-the-middle and Trojan horse attacks. We prove in the following that our proposed protocol is robust against the attacks introduced by Eve.

Man-in-the-middle (MITM) attack: This is the most common attack in most communication scenarios where Eve impersonates Alice for Bob and vice versa. To perform a MITM attack and mimic the setting of our proposed protocol, Eve pretends to be the server and prepares a QAO for the K participants. On the other hand, she also prepares K CQZ setups and acts as the K participants for the server. In case Eve can correctly guess the detection time window of the server and the path length between the server and the participants, the composite state after Eve's attack becomes

$$\begin{aligned} |\chi\rangle_{mitm} =& \frac{1}{\sqrt{2}}\left(\sqrt{\eta_1^K}\,|000...0\rangle_{CE_1E_2...E_K} + \sqrt{\eta_2^K}\,|111...1\rangle_{CE_1E_2...E_K}\right)\otimes \\ & \frac{1}{\sqrt{2}}\left(\sqrt{\eta_1^K}\,|000...0\rangle_{E_SP_1P_2...P_K} + \sqrt{\eta_2^K}\,|111...1\rangle_{E_SP_1P_2...P_K}\right), \end{aligned} \tag{12}$$

where E_S denotes Eve who pretends to be the server for the legitimate participants and E_k denotes Eve who pretends to be the kth participant for the legitimate server where $k \in \{1, 2, ..., K\}$. From (12), we can see that the correlation between the actual server and the participants gets destroyed by Eve. The $K+1$ partite GHZ state may collapse into 2^K possible states when measured in the $\mathcal{X}$ basis. When the actual server and K participants measure their respective qubits in the presence of Eve in step 1 of our protocol, it results in two collapsed states. One originates from the $K+1$ partite GHZ state shared among the legitimate server C and E_k participants, while the other originates from the $K+1$ partite GHZ state shared between E_S and the legitimate K participants. The announced measurement result of the server comes from the former collapsed GHZ state while the results from the legitimate participants come from the latter collapsed GHZ state. This causes the measurement results of the server and the legitimate participants to fall into one of the 2^K+1 possible result sets. However, the actual results must be one of 2^K possible result sets. On that account, the probability that the measurement results of the server and the legitimate participants fall into the valid GHZ basis is $1/2$. Thus, we can indicate the probability of the existence of Eve in the channel by $\gamma_{mitm} = \frac{1}{2}$.

Trojan horse (TH) attack: To avoid being detected by the server, Eve builds a CQZ setup and exposes a ghost photon to the server to append her qubit to the GHZ state. A ghost photon here means that the chance of an eavesdropping photon appearing in the channel approaches zero due to the continuous measurement of the server during the CQZ operation [37]. This ghost photon can assist Eve in determining the presence or absence of an AO at the server from the detector click of their CQZ setting. However, a successful TH

attack requires the eavesdropping photon to complete the operation within the access time window of the apparatus of the server. By varying the access time window, the server can discover the existence of Eve. If Eve is lucky enough, we can describe the resulting GHZ state after the attack as

$$|\chi\rangle_{th} = \frac{1}{\sqrt{2}}\left(\sqrt{\eta_1^{K+1}}\,|000...00\rangle_{CP_1P_2...P_KE} + \sqrt{\eta_2^{K+1}}\,|111...11\rangle_{CP_1P_2...P_KE}\right), \tag{13}$$

where E denotes the qubit of Eve. We consider only one adversary in (13), which may change as the number of adversaries (N_E) increases. By tracing out Eve's qubit, the density matrix of the legitimate system is

$$\begin{aligned}\rho_{GHZ} = Tr_E(|\chi\rangle_{th}\langle\chi|_{th}) &= \sum_{i=1}^{K+1} p_i \rho_C \otimes \rho_{P_1} \otimes \rho_{P_2} \otimes \ldots \otimes \rho_{P_K} \\ &\neq |\psi_K\rangle\langle\psi_K|,\end{aligned} \tag{14}$$

where p_i is the probability distribution. From (14), we can see that the tracing out of Eve's system causes the legitimate system to collapse into a mixed state different from the expected shared GHZ state. In the presence of Eve, there are 2^{K+E} possible measurement results for the server and the K participants. Regardless of the number of Eve, only 2^{K+E-1} results will fall under the correct GHZ basis. Thus, when the server and the K participants perform security checking on the counterfactual GHZ state distribution in step 1, the probability that Eve cannot hide her presence is $\gamma_{th} = \frac{1}{2}$.

3.1.3. Anonymity of CAQT

For anonymity, we consider two cases:

(i) Anonymity of the sender;
(ii) Anonymity of the receiver.

For the first case, we can identify the probability of a certain participant being the sender as in ref [7]

$$\text{Prob}[S = s] = \frac{1}{n-t}, \tag{15}$$

where S is the random variable identifying a sender and t is the number of corrupted participants. The global state between all participants is (8), with is symmetrically distributed between each participant. Similarly, the operations performed on the global state, i.e., measurements, are purely local. No party knows the operations performed by the other. The resultant state after a local operation is independent of the participant's identity, which makes each participant equally likely to be the sender. Thus, the identity of the sender remains anonymous. We can adopt a similar reasoning for the second case.

An important observation is that any malicious participant can only alter the global state without identifying the identity of the sender and receiver. Similarly, even if the malicious participants collude, the malicious participants are unable to correctly identify the sender and receiver as long as the condition $t \leq K-2$ gets fulfilled. This point is of great significance in our protocol as it shows that the resultant state created using counterfactual communication can guarantee anonymity.

3.1.4. Privacy of Teleported Qubit

Although the main goal of anonymous communication is to protect the anonymity of the sender and receiver, it is also needed to assure the privacy of the transmitted quantum message. Once the security of the counterfactual GHZ state distribution is guaranteed, no external adversaries can get involved in the anonymous communication. Only two types of internal adversaries—semiactive adversaries and active adversaries—can lead to security flaws. We define a semiactive adversary as the one who follows the protocol but announces

the wrong result rather than the correct one, and an active adversary as the one who does not follow the protocol and announces random results.

In the case of semiactive adversaries, an even number of adversaries still leads to the correct form of anonymous entanglement because their announcements of wrong measurement results cancel each other out and do not affect the anonymous entanglement phase. However, the server can detect an odd number of semiactive adversaries causing an invalid anonymous entanglement in step 6 of the protocol. Regardless of whether or not the correct anonymous entanglement gets established, the adversaries will not be able to extract the anonymous teleported quantum message. This limitation is due to the following two reasons: (i) the identity of the sender and the receiver is hidden from the adversaries, and (ii) only the notified receiver can correctly extract the two classical messages required for teleportation from the broadcast messages.

In the case of active adversaries, they attempt to entangle their qubits with the anonymous entanglement by not measuring their qubits in the $\mathcal{X}$ basis and broadcasting random results. If they are lucky enough and the random results are correct, they pass the security checking phase in step 6. Consequently, we can express the shared entanglement between the sender, receiver, and an active adversary as

$$|\Phi\rangle = \frac{1}{\sqrt{2}} |000\rangle_{srq} + |111\rangle_{srq} . \tag{16}$$

where s, r, and q denotes the qubits of the sender, receiver, and active adversary, respectively. If $|\psi\rangle_a = \alpha |0\rangle_a + \beta |1\rangle_a$ is the quantum message the sender wants to teleport, the state after the Bell basis measurement of the sender becomes

$$\begin{aligned} |\Phi\rangle_{BM} = |\phi^+\rangle_{as} \left(\alpha |00\rangle_{rq} + \beta |11\rangle_{rq}\right) + |\phi^-\rangle_{as} \left(\alpha |00\rangle_{rq} - \beta |11\rangle_{rq}\right) \\ + |\psi^+\rangle_{as} \left(\alpha |11\rangle_{rq} + \beta |00\rangle_{rq}\right) + |\psi^-\rangle_{as} \left(\alpha |11\rangle_{rq} - \beta |00\rangle_{rq}\right) . \end{aligned} \tag{17}$$

Still, the knowledge of adversaries is limited to the two classical messages required for teleportation. However, the receiver also cannot get the correct teleported qubit. Apart from disturbing the protocol, the adversaries cannot obtain any useful information from this attack. Hence, it is evident that the privacy of the teleported quantum message remains preserved in the presence of adversaries.

3.2. Performance Analysis of CAQT under Channel Noise

The most significant hurdle in any communication task is the presence of noise in the channel, which deteriorates the performance of communication. In this section, we investigate the impact of quantum noise in counterfactual anonymous quantum teleportation. We compare its performance with conventional anonymous quantum teleportation protocols achieved through GHZ states [7] and entanglement relays [8]. In conventional quantum communication, the qubit that passes through the quantum channel gets subjected to quantum-noise-induced alterations. Contrary to the conventional scenario, in counterfactual quantum communication, noise affects only the fraction of the qubit in path 2 that travels through the transmission channel, as shown in Figure 1.

The entanglement shared between the two end nodes lies at the heart of the quantum teleportation process. In our proposed protocol, the anonymous entanglement between the sender and receiver mainly relies on the counterfactual GHZ state distribution. Under the

noisy quantum framework, the GHZ state shared among the participants is encompassed within the noise operator described by

$$\begin{aligned}\tilde{\mathcal{U}} =& |1\rangle_C \langle 1|_C{}^{\otimes K} \otimes \left(\otimes_{i=1}^{K} I_{P_i}\right) \otimes I_{path}{}^{\otimes K} \\ &+ |0\rangle_C \langle 0|_C{}^{\otimes K} \otimes \left(\otimes_{i=1}^{K} I_{P_i}\right) \otimes \left(|0\rangle_{path} \langle 0|_{path} + |1\rangle_{path} \langle 1|_{path}\right)^{\otimes K} \\ &+ |0\rangle_C \langle 0|_C{}^{\otimes K} \otimes \wedge_{P_1} \otimes \wedge_{P_2} \otimes \ldots \otimes \wedge_{P_K} \otimes |2\rangle_{path} \langle 2|_{path}{}^{\otimes K},\end{aligned} \tag{18}$$

where I_{P_i} is a two-dimensional identity operator, I_{path} is a three-dimensional identity operator, and $\wedge_{P_i}$ is the quantum noise operator encountered by the qubit of participant P_i [36]. From the noise operator, we observe that the noise affects only the photon component that comes out of the CQZ gate and enters the transmission channel via path 2. The density operator of the noisy counterfactual GHZ state can be described as

$$\widetilde{\rho_{GHZ}} = \tilde{\mathcal{U}} U_{CQZ}{}^{\otimes K} |\psi_0\rangle \langle\psi_0| U_{CQZ}^{\dagger}{}^{\otimes K} \tilde{\mathcal{U}}^{\dagger}, \tag{19}$$

where U_{CQZ} denotes the operation of the CQZ gate.

We can obtain the anonymous entangled state shared between S and R after step 4 by tracing out all participants in the network except S and R as follows:

$$\zeta_{SR} = \frac{1}{\kappa} Tr_{K-1}\left[\widetilde{\rho_{GHZ}} \left(\mathcal{I}_{SR} \otimes |+\rangle \langle +|_{K-1}\right)\right] \tag{20}$$

where κ is the normalization factor and $|+\rangle \langle +|_{K-1}$ is the projection onto the $|+\rangle$ state of $K-1$ participants. Note that, for the ideal noiseless channel, the anonymous entanglement shared between the S and R is $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. In the following sections, we compare the performance of the anonymous entanglement established using our CAQT protocol and conventional AQT protocols under different types of quantum noise. Here, we considered three types of quantum noise: dephasing noise, bit-flip noise, and depolarizing noise. To analyze the performance of noisy AQT protocols, the fidelity was employed as a metric to quantify the closeness between the ideal anonymous entanglement and the noisy anonymous entanglement.

3.2.1. Comparison with Conventional AQT Protocols under Dephasing Noise

Dephasing is a process in which a qubit loses its phase information after traveling through a transmission channel. The action of the dephasing channel can be described as follows:

$$\rho \rightarrow (1-p)\rho + pZ\rho Z, \tag{21}$$

where ρ is the density operator of the initial quantum state, Z is the Pauli Z operator, and $0 \leq p \leq 1$ is a noise parameter.

In Figure 5, we compare our proposed protocol with the conventional GHZ-based and relay-based AQT protocols under the dephasing noise. In the conventional AQT protocols, the entanglement was preshared using ideal channel. For the consistency with our reasoning, we assumed that the entanglement was preshared among the participants under noise and there were $N = K+1$ participants in the network. For the GHZ-based AQT, the density operator of the initial resource can be written as $\widetilde{\sigma_{GHZ}} = \wedge^{\otimes N} |GHZ\rangle \langle GHZ|_N$. Without loss of generality, the anonymous entanglement Φ_{SR} arising from this preshared entanglement is described as

$$\Phi_{SR} = \frac{1}{\mathcal{N}} Tr_{N-2}\left[\widetilde{\sigma_{GHZ}} \left(\mathcal{I}_{SR} \otimes |+\rangle \langle +|_{N-2}\right)\right], \tag{22}$$

where $\mathcal{N}$ is the normalization factor. The main difference between the conventional GHZ-based AQT and our proposed protocol is the distribution of the GHZ state. Since coun-

terfactual communication is robust against dephasing noise [36], it allows a GHZ state distribution employing this property to remain unaffected by it as well. The fidelity of these protocols is plotted as a function of noise for $N = 4$ and $N = 8$ participants in Figure 5. We can see that the fidelity of the anonymous entanglement in our proposed protocol, $F_{AE}(\zeta_{SR}) = Tr[\zeta_{SR} |\phi^+\rangle \langle\phi^+|_{SR}]$, is almost equal to one regardless of the number of participants. On the other hand, for the conventional GHZ-based AQT, one can observe the parabolic behavior of the fidelity of the anonymous entanglement, $F_{AE}(\Phi_{SR}) = Tr[\Phi_{SR} |\phi^+\rangle \langle\phi^+|_{SR}]$.

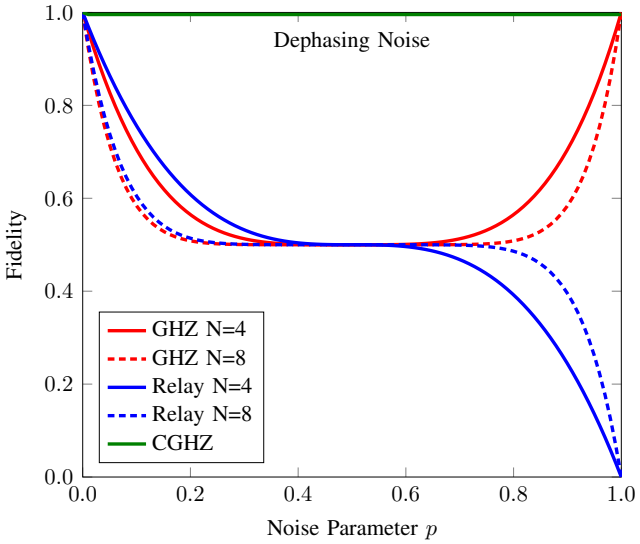

Figure 5. Fidelity of the anonymous entanglement of CAQT compared to those of conventional GHZ-state-based AQT and relay-based AQT under dephasing noise. Here, the dotted (solid) line denotes the fidelity of anonymous entanglement when the number of participants N is 4 (8). The fidelity values of the anonymous entanglement of conventional GHZ-state-based AQT (GHZ), relay-based AQT (Relay), and our counterfactual GHZ-state-based AQT (CGHZ) are represented by the red, blue, and green lines, respectively. The fidelity of our proposed protocol is the same for both $N = 4$ and $N = 8$.

In the relay-based AQT, each participant in the network holds a Bell pair. They perform entanglement swapping in a consecutive order to create entanglement between the first and last participants. Meanwhile, the sender and the receiver locally perform a CNOT operation on their target ancillary qubits before entanglement swapping with their next participant. Finally, a four-partite entanglement is formed between the sender, the receiver, and the first and last participants. When the first and last participants measure their qubit in the $\mathcal{X}$ basis, the anonymous entanglement is established between the sender and receiver. However, quantum noise affects each entanglement swapping between any two consecutive participants. Although this protocol enables long-distance communication, the quantum noise experienced in each entanglement swapping pair reduces the fidelity of the anonymous entanglement, $F_{AE}(\Psi_{SR}) = Tr[\Psi_{SR} |\phi^+\rangle \langle\phi^+|_{SR}]$. It is evident from the plot that in the presence of dephasing noise, $F_{AE}(\Psi_{SR})$ decreases remarkably as the distance, i.e., the number of participants, increases under the noise parameter $p \leq 0.5$. Beyond that noise level, $F_{AE}(\Psi_{SR})$ slightly increases as the number of participants increases. By contrast, our proposed protocol allows anonymous communication over remote participants with high fidelity, even in a large network with many participants. Hence, our proposed protocol outperforms the conventional AQT protocols in the presence of dephasing noise.

3.2.2. Comparison with Conventional AQT Protocols under Bit-Flip Noise

Bit-flip noise flips the computational state of the qubit from $|0\rangle$ to $|1\rangle$ and vice versa. Given a bit-flip channel, it applies the identity operator with some probability $1 - p$ and a bit-flip Pauli X operator with probability p on the incoming qubit. We can represent the generic model for the bit-flip channel as follows:

$$\rho \rightarrow (1 - p)\rho + pX\rho X. \tag{23}$$

In Figure 6, we plot the fidelity values of the anonymous entanglement in our proposed protocol and the conventional AQT protocols under the bit-flip noise for $N = 4$ and $N = 8$. Within a noise range from 0 to 0.5, we can see that relay-based AQT performs better than the other two protocols. However, its performance degrades linearly with the noise beyond that range, whereas the GHZ-based AQT yields the best performance.

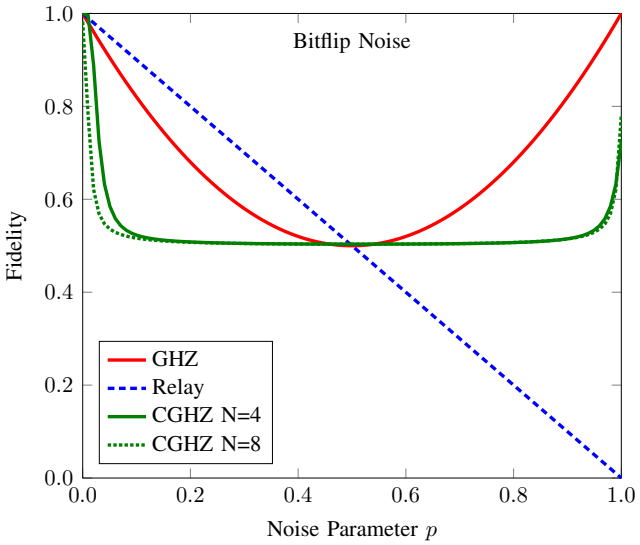

Figure 6. Fidelity of the anonymous entanglement of CAQT compared to those of conventional GHZ-based AQT and relay-based AQT under bit-flip noise. Here, the dotted (solid) line denotes the fidelity of anonymous entanglement when the number of participants N is 4 (8). The fidelity values of the anonymous entanglement of conventional GHZ-state-based AQT (GHZ), relay-based AQT (Relay), and our counterfactual GHZ-state-based AQT (CGHZ) are represented by the red, blue, and green lines, respectively. The conventional AQT protocols yield the same fidelity graph for both $N = 4$ and $N = 8$.

Although our proposed protocol is not the best option to choose in an environment with bit-flip noise, it can provide a fidelity greater than 0.5 for any noise level. It has been known that if the fidelity of an entanglement resource is greater than 0.5, it is considered a useful resource for quantum teleportation [9,38]. Hence, our proposed protocol is applicable for the anonymous transmission of a quantum message with the advantage of no information-carrying particle passing through the channel.

3.2.3. Comparison with Conventional AQT Protocols under Depolarizing Noise

The depolarizing channel is the worst-case scenario among all the noise scenarios as it induces the combined effect of the dephasing and bit-flip channels. When the entangled state interacts with the environment under a depolarizing noise, it severely affects the entanglement feature of quantum states. Generally, it maps the pure input state to the mixed output state as follows:

$$\rho \rightarrow (1 - p)\rho + p\pi, \tag{24}$$

where $\pi = I/2$ is the maximally mixed state.

As shown in Figure 7, the fidelity of conventional protocols decreases as the number of participants and noise level increases. These protocols can support useful anonymous entanglement resources for teleportation only under a very low number of participants and noise levels. On the other hand, the fidelity $F_{AE}(\zeta_{SR})$ of our proposed protocol reaches the saturation point at about 0.5 as the number of participants and noise level increases. Hence, in a large network with high noise levels, the performance of our proposed protocol surpasses that of conventional protocols and can provide useful resources for quantum teleportation.

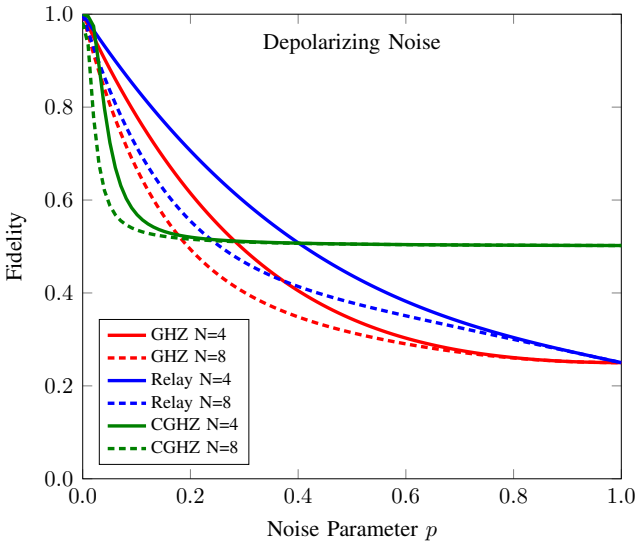

Figure 7. Fidelity of anonymous entanglement of CAQT compared to those of conventional GHZ-based AQT and relay-based AQT under depolarizing noise. Here, the dotted (solid) line denotes the fidelity of anonymous entanglement when the number of participants N is 4 (8). The fidelity values of the anonymous entanglement of conventional GHZ-state-based AQT (GHZ), relay-based AQT (Relay), and our counterfactual GHZ-state-based AQT (CGHZ) are represented by the red, blue, and green lines, respectively.

To get a better inside on the behavior of the conventional AQT protocols and our proposed protocol, we provide a summary of comparison results in Table 1.

Table 1. Performance comparison of AQT protocols under three different types of channel noise.

Protocols		**GHZ-Based AQT**	**Relay-Based AQT**	**Counterfactual GHZ-Based AQT**
Initial Resources		**Preshared GHZ State**	**Bell States**	**Single Photons**
Fidelity	Dephasing Noise	Parabolic curve	Nonlinear decrease	Not affected
	Bit-flip noise	Parabolic curve	Linear decrease	High-order parabolic curve
	Depolarizing noise	High-order exponential decrease	Exponential decrease	Saturated at 0.5
Useful quantum resource	Dephasing Noise	Can provide	Cannot provide at $p > 0.5$	Can provide
	Bit-flip noise	Can provide	Cannot provide at $p > 0.5$	Can provide
	Depolarizing noise	Cannot provide at $p > 0.5$	Cannot provide at $p > 0.5$	Can provide

4. Application of CAQT in IoT Network

Secure IoT device communication is crucial for the reliable exchange of data in internet-enabled financial transactions, social communications, digitally signed documents, the transmission of medical data, or military communications [39,40]. Such applications require disparate network nodes performing computing, sensing, and data routing to collaborate and exchange huge quantities of data, which causes serious concerns for data security [39]. Attacks on privacy can reveal sensitive information such as the user identity and real-time user location data to malicious entities. The constraint on computational resources and power on individual nodes render postquantum cryptographic schemes ineffective [40].

Anonymous communication can offer information-theoretic anonymity for internode communication which is one of the requirements in IoT networks. Quantum-enabled solutions such as quantum anonymous transmission protocols can be fundamental to establishing security frameworks to support centralized and decentralized architectures for heterogeneous IoT applications in the long term. However, various environmental factors such as noise and loss due to faulty nodes, device reliability, and communication length may doom such protocols to be inefficient in real-world scenarios [41,42]. Our protocol, supported by the evidence provided above, outperformed the previously proposed protocols when channel noise and adversarial attacks were considered. Hence, it could support a plethora of application scenarios for single and multiple involved parties including anonymous wireless sensing networks, reliable social communication platforms, and telemedicine.

5. Conclusions

We presented an anonymous quantum teleportation protocol employing a counterfactual GHZ state distribution. We supplemented the protocol with a proof of its correctness and a comprehensive security analysis against potential attacks such as man-in-the-middle attacks and Trojan horse attacks, proving its robustness to malicious attacks. We demonstrated that it was simple to identify the presence of eavesdroppers in the quantum channel. Since the primary objective of anonymous communication is to protect the identities of the sender and the receiver, our proposed protocol met this criterion as long as the number of malicious participants was less than $K - 2$. In addition, our protocol also preserved the privacy of the teleported qubit in the presence of adversaries. We further showed that our proposed protocol outperformed conventional GHZ-based AQT and relay-based AQT in the presence of dephasing noise and depolarizing noise. Although our proposed protocol did not offer the best performance under a bit-flip noise, it could provide useful quantum resources for anonymity. Thus, it is applicable in practical quantum communication scenarios.

Author Contributions: Conceptualization, S.N.P.; methodology, S.N.P., J.W.S., M.T.R. and S.T.; software, S.N.P. and J.W.S.; validation, S.N.P., J.W.S., M.T.R. and S.T.; formal analysis, S.N.P., J.W.S., M.T.R., S.T. and K.L.; investigation, S.N.P., J.W.S., M.T.R. and S.T.; resources, S.N.P., J.W.S., M.T.R., S.T. and K.L.; data curation, S.N.P. and J.W.S.; writing—original draft preparation, S.N.P. and M.T.R.; writing—review and editing, S.N.P., J.W.S., M.T.R. and S.T.; visualization, S.N.P., J.W.S., M.T.R. and S.T.; supervision, H.S. and K.L.; project administration, H.S. and K.L.; funding acquisition, H.S. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korea government (MSIT) (nos. 2019R1A2C2007037 and 2022R1A4A3033401) and by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2021-0-02046) supervised by the IITP (Institute for Information & Communications Technology Planning & Evaluation). This research is partially funded by the BK21 FOUR program of National Research Foundation of Korea.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

GHZ	Greenberger–Horne–Zeilinger
QZ	Quantum Zeno
CQZ	Chained quantum Zeno
PBS	Polarizing beam splitter
SM	Switchable mirror
MR	Mirror
OD	Optical delay
OC	Optical circulator
D	Detector
AO	Absorptive object
QAO	Quantum absorptive object
AQT	Anonymous quantum teleportation
CAQT	Counterfactual anonymous quantum teleportation

References

1. Bennett, C.H.; Brassard, G.; Ekert, A.K. Quantum Cryptography. *Sci. Am.* **1992**, *267*, 50–57. [CrossRef]
2. Deng, F.G.; Long, G.L.; Liu, X.S. Two-step Quantum Direct Communication Protocol using the Einstein–Podolsky-Rosen Pair Block. *Phys. Rev. A* **2003**, *68*, 042317. [CrossRef]
3. Gottesman, D. Theory of Quantum Secret Sharing. *Phys. Rev. A* **2000**, *61*, 042311. [CrossRef]
4. Zhou, N.R.; Xu, Q.D.; Du, N.S.; Gong, L.H. Semi-Quantum Private Comparison Protocol of Size Relation with D-Dimensional Bell States. *Quantum Inf. Process.* **2021**, *20*, 1–15. [CrossRef]
5. Chaum, D. The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. *J. Cryptol.* **1988**, *1*, 65–75. [CrossRef]
6. Boykin, P.O. *Information Security and Quantum Mechanics: Security of Quantum Protocols*; University of California: Los Angeles, CA, USA, 2002.
7. Christandl, M.; Wehner, S. Quantum Anonymous Transmissions. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Chennai, India, 4–8 December 2005; Springer: Berlin/Heidelberg, Germany, 2005; pp. 217–235.
8. Yang, W.; Huang, L.; Song, F. Privacy Preserving Quantum Anonymous Transmission via Entanglement Relay. *Sci. Rep.* **2016**, *6*, 1–8. [CrossRef]
9. Lipinska, V.; Murta, G.; Wehner, S. Anonymous Transmission in a Noisy Quantum Network using the W State. *Phys. Rev. A* **2018**, *98*, 052320. [CrossRef]
10. Li, Y.; Yu, C.; Wang, Q.; Liu, J. Quantum Communication for Sender Anonymity Based on Single-Particle with Collective Detection. *Phys. Scr.* **2021**, *96*, 125118. [CrossRef]
11. Brassard, G.; Broadbent, A.; Fitzsimons, J.; Gambs, S.; Tapp, A. Anonymous Quantum Communication. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2–6 December 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 460–473.
12. Chen, Z.; Lou, X.; Guo, Y. A Cooperative Quantum Anonymous Transmission with Hybrid Entanglement Swapping. *Int. J. Theor. Phys.* **2013**, *52*, 3141–3149. [CrossRef]
13. Khan, A.; Khalid, U.; ur Rehman, J.; Lee, K.; Shin, H. Quantum Anonymous Collision Detection for Quantum Networks. *EPJ Quantum Technol.* **2021**, *8*, 27. [CrossRef]
14. Khan, A.; ur Rehman, J.; Shin, H. Quantum Anonymous Notification for Network-Based Applications. *Quantum Inf. Process.* **2021**, *20*, 397. [CrossRef]
15. Khan, A.; Khalid, U.; ur Rehman, J.; Shin, H. Quantum Anonymous Private Information Retrieval for Distributed Networks. *IEEE Trans. Commun.* **2022**, *70*, 4026–4037. [CrossRef]
16. Gong, B.; Gao, F.; Cui, W. Anonymous Communication Protocol over Quantum Networks. *Quantum Inf. Process.* **2022**, *21*, 1–12. [CrossRef]
17. Huang, Z.; Joshi, S.K.; Akta, D.; Lupo, C.; Quintavalle, A.Q.; Venkatachalam, N.; Wengerowsky, S.; Neumann, S.P.; Liu, B.; Kling, B.; et al. Experimental Implementation of Secure Anonymous Protocols on an Eight-User Quantum Key Distribution Network. *Npj Quantum Inf.* **2022**, *8*, 1–7.

18. Mishra, S.; Thapliyal, K.; Parakh, A.; Pathak, A. Quantum Anonymous Veto: A Set of New Protocols. *EPJ Quantum Technol.* **2022**, *9*, 14. [CrossRef]
19. Wang, Y.; Li, X.; Han, Y.; Zhang, K. Practical Anonymous Entanglement with Noisy Measurement. *Quantum Inf. Process.* **2022**, *21*, 1–17. [CrossRef]
20. Yang, Y.G.; Cao, G.D.; Huang, R.C.; Gao, S.; Zhou, Y.H.; Shi, W.M.; Xu, G.B. Multiparty Anonymous Quantum Communication without Multipartite Entanglement. *Quantum Inf. Process.* **2022**, *21*, 1–21. [CrossRef]
21. Thalacker, C.; Hahn, F.; de Jong, J.; Pappa, A.; Barz, S. Anonymous and Secret Communication in Quantum Networks. *New J. Phys.* **2021**, *23*, 083026. [CrossRef]
22. Elitzur, A.C.; Vaidman, L. Quantum Mechanical Interaction-free Measurements. *Found. Phys.* **1993**, *23*, 987–997. [CrossRef]
23. Itano, W.M.; Heinzen, D.J.; Bollinger, J.J.; Wineland, D. Quantum Zeno effect. *Phys. Rev. A* **1990**, *41*, 2295. [CrossRef]
24. Salih, H.; Li, Z.H.; Al-Amri, M.; Zubairy, M.S. Protocol for direct counterfactual quantum communication. *Phys. Rev. Lett.* **2013**, *110*, 170502. [CrossRef]
25. Noh, T.G. Counterfactual Quantum Cryptography. *Phys. Rev. Lett.* **2009**, *103*, 230501. [CrossRef]
26. Salih, H.; Hance, J.R.; McCutcheon, W.; Rudolph, T.; Rarity, J. Deterministic Teleportation and Universal Computation without Particle Exchange. *arXiv* **2020**, arXiv:2009.05564.
27. Salih, H. Protocol for Counterfactually Transporting an Unknown Qubit. *Front. Phys.* **2016**, *3*, 94. [CrossRef]
28. Shenoy, A.; Srikanth, R.; Srinivas, T. Counterfactual Quantum Certificate Authorization. *Phys. Rev. A* **2014**, *89*, 052307. [CrossRef]
29. Hosten, O.; Rakher, M.T.; Barreiro, J.T.; Peters, N.A.; Kwiat, P.G. Counterfactual Quantum Computation through Quantum Interrogation. *Nature* **2006**, *439*, 949–952. [CrossRef]
30. Zaman, F.; Shin, H.; Win, M.Z. Counterfactual Concealed Telecomputation. *arXiv* **2020**, arXiv:2012.04948.
31. Zaman, F.; Shin, H.; Win, M.Z. Counterfactual Full-Duplex Communication. *arXiv* **2019**, arXiv:1910.03200.
32. Wang, T.Y.; Wen, Q.Y.; Zhu, F.C. Economical Quantum Anonymous Transmissions. *J. Phys. B: At. Mol. Opt. Phys.* **2010**, *43*, 245501. [CrossRef]
33. Broadbent, A.; Tapp, A. Information-Theoretic Security without an Honest Majority. In Proceedings of the International Conference on the Theory and Application of Cryptology and Information Security, Kuching, Malaysia, 2–6 December 2007; Springer: Berlin/Heidelberg, Germany, 2007; pp. 410–426.
34. Chen, Y.; Gu, X.; Jiang, D.; Xie, L.; Chen, L. Tripartite Counterfactual Entanglement Distribution. *Opt. Express* **2015**, *23*, 21193–21203. [CrossRef]
35. Kim, Y.S.; Lee, J.C.; Kwon, O.; Kim, Y.H. Protecting Entanglement from Decoherence using Weak Measurement and Quantum Measurement Reversal. *Nat. Phys.* **2012**, *8*, 117–120. [CrossRef]
36. Ullah, M.A.; Paing, S.N.; Shin, H. Noise-Robust Quantum Teleportation with Counterfactual Communication. *IEEE Access* **2022**, *10*, 61484–61493. [CrossRef]
37. Li, Z.H.; Wang, L.; Xu, J.; Yang, Y.; Al-Amri, M.; Zubairy, M.S. Counterfactual Trojan Horse Attack. *Phys. Rev. A* **2020**, *101*, 022336. [CrossRef]
38. Yang, Y.G.; Liu, X.X.; Gao, S.; Zhou, Y.H.; Shi, W.M.; Li, J.; Li, D. Towards Practical Anonymous Quantum Communication: A Measurement-Device-Independent Approach. *Phys. Rev. A* **2021**, *104*, 052415. [CrossRef]
39. Khan, M.A.; Salah, K. IoT Security: Review, Blockchain Solutions, and Open Challenges. *Future Gener. Comput. Syst.* **2018**, *82*, 395–411. [CrossRef]
40. Fernández-Caramés, T.M. From Pre-Quantum to Post-Quantum IoT Security: A Survey on Quantum-Resistant Cryptosystems for the Internet of Things. *IEEE Internet Things J.* **2020**, *7*, 6457–6480. [CrossRef]
41. Liao, C.T.; Bahrani, S.; da Silva, F.F.; Kashefi, E. Benchmarking of Quantum Protocols. *Sci. Rep.* **2022**, *12*, 1–13. [CrossRef] [PubMed]
42. Alvarez, D.; Kim, Y. Survey of the Development of Quantum Cryptography and Its Applications. In Proceedings of the IEEE 11th Annual Computing and Communication Workshop and Conference, Las Vegas, NV, USA, 27–30 January 2021; pp. 1074–1080.