Anonymous transmission in a noisy quantum network using the W state

Lipinska, Victoria; Murta, Gláucia; Wehner, Stephanie

DOI
10.1103/PhysRevA.98.052320

Publication date
2018

Document Version
Final published version

Published in
Physical Review A

Anonymous transmission in a noisy quantum network using the *W* state

Victoria Lipinska,* Gláucia Murta,† and Stephanie Wehner
QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, Netherlands

(Received 29 June 2018; published 16 November 2018)

We consider the task of anonymously transmitting a quantum message in a network. We present a protocol that accomplishes this task using the *W* state and we analyze its performance in a quantum network where some form of noise is present. We then compare the performance of our protocol with some of the existing protocols developed for the task of anonymous transmission. We show that, in many regimes, our protocol tolerates more noise and achieves higher fidelities of the transmitted quantum message than the other ones. Furthermore, we demonstrate that our protocol tolerates one nonresponsive node. We prove the security of our protocol in a semiactive adversary scenario, meaning that we consider an active adversary and a trusted source.

DOI: 10.1103/PhysRevA.98.052320

I. INTRODUCTION

In cryptographic scenarios we are often concerned with hiding the content of the messages being exchanged. However, sometimes the identity of the parties who communicate may also carry relevant information. Examples of tasks where the identities of the ones who communicate carry crucial information are voting, electronic auctions [1] or, more practically, sending a message to a secret beloved [2]. Therefore, the establishment of anonymous links in a network, where identities of connected parties remain secret, is an important primitive for both classical [3] and quantum communication.

In this paper we consider a task of anonymously transmitting a quantum message in a network. To define the task more precisely, consider a quantum network with N nodes. One of the nodes, sender S, would like to communicate a quantum state $|\psi\rangle$ to a receiver R in a way that their identities remain completely hidden throughout the protocol. In particular, for S it implies that her identity remains unknown to all the other parties, whereas for R it implies that no one except S knows her identity. The essence of the protocol is to create an entangled link between S and R by performing local operations on the other nodes of the network. Such a link is called *anonymous entanglement* (AE) [4], since the identities of the nodes holding the shares of the entangled pair is kept anonymous. After anonymous entanglement is created, S and R use it as a resource for teleporting the quantum information $|\psi\rangle$. Note that the main goal of anonymous transmission is to fully hide the identities of the sender and the receiver; it does not aim at guaranteeing the reliability of the transmitted message.

A number of protocols have been proposed to tackle this task, which was first introduced in Ref. [4]. There, the authors present a protocol which makes use of a given multipartite Greenberger-Horne-Zeilinger (GHZ) state as a quantum resource, i.e., $|\mathrm{GHZ}_N\rangle = \frac{1}{\sqrt{2}}(|0\ldots0\rangle + |1\ldots1\rangle)$. The problem was subsequently developed to consider the preparation and certification of the GHZ state [5,6]. In Ref. [6], it was first shown that the proposed protocol is information-theoretically secure against an active adversary. What is more, other protocols were proposed, which do not make use of multipartite entanglement, but utilize solely Bell pairs to create anonymous entanglement [7]. Yet, so far, it has not been discussed whether multipartite states other than the GHZ allow for anonymous transmission of a quantum state. Moreover, nothing is known about the performance of such protocols in a realistic quantum network, where one inevitably encounters different forms of noise.

Here we design a protocol for quantum anonymous transmissions which uses the W state, $|W\rangle_N = \frac{1}{\sqrt{N}}(|10\ldots0\rangle + \cdots + |0\ldots01\rangle)$. Just like other existing protocols, our protocol is based on establishing anonymous entanglement between S and R. We prove the security of our protocol in a semiactive adversary scenario, meaning that we consider an active adversary and a trusted source, as in Ref. [4]. We also show that security is preserved in the presence of noise in the network, when all the particles are subjected to the same type of noise. What is more, we compare the performance of our protocol with previously proposed protocols that use the GHZ state and Bell pairs. We quantify the performance of protocols by the fidelity of the transmitted quantum state. We find that, in many cases, our W-state based protocol tolerates more noise than the other protocols and achieves higher fidelity of the transmitted state. Additionally, we show that our protocol can tolerate one non-responsive node, e.g., if one of the qubits of a multipartite state gets lost. In contrast, the protocol using the GHZ state cannot be carried out at all in this case, since the loss of a single qubit destroys the entanglement of the state. We also address the performance of the Bell-pair based protocol, presented in Ref. [7], and we show that in the presence of noise, the performance of the protocol depends on the ordering of S and R in the network. To the best of our knowledge this is the first analysis of anonymous transmission in the presence of noise. Without such an analysis the performance of near-future

*v.lipinska@tudelft.nl
†g.murtaguimaraes@tudelft.nl

applications for quantum networks cannot be characterized [8].

The paper is organized as follows. In Sec. II, we present the protocol for anonymous transmission with the W state and discuss its correctness. In Sec. III, we provide the security definition and prove that our protocol is secure in the semiactive and passive adversary scenario. Finally, in Sec. IV we examine the behavior of our protocol in a noisy quantum network and compare it with the other existing protocols.

II. THE PROTOCOL

Our anonymous transmission protocol, Protocol 1, allows a sender S to transmit an arbitrary quantum state $|\psi\rangle$ to a receiver R in an anonymous way and uses the N-partite W state as a quantum resource.

Protocol 1: Anonymous transmission with the W state.

Goal: Transmit a quantum state $|\psi\rangle$ from the sender S to the receiver R, while keeping the identities of S and R anonymous.

1. *Collision detection.*
   Nodes run the classical collision detection protocol [9] to determine a single sender S. All nodes input 1 if they do wish to be the sender and 0 otherwise. If a single node wants to be the sender, continue.
2. *Receiver notification.*
   Nodes run the classical receiver notification protocol [9], where the receiver R is notified of her role.
3. *State distribution.*
   A trusted source distributes the N-partite W state.
4. *Measurement.*
   $N-2$ nodes (all except for S and R) measure in the $\{|0\rangle, |1\rangle\}$ basis.
5. *Anonymous announcement of outcomes.*
   Nodes use the classical veto protocol [9] which outputs 0 if all the $N-2$ measurement outcomes are 0, and 1 otherwise. If the output is 0 then anonymous entanglement is established, else abort.
6. *Teleportation.*
   Sender S teleports the message state $|\psi\rangle$ to the receiver R. Classical message m associated with teleportation is sent anonymously. The communication is carried out using the classical logical OR protocol [9] which computes $m \oplus$ rand, where rand is a random 2-bit string input by the receiver R.

Protocol 1 is built on a number of classical subroutines: collision detection, receiver notification, veto, and logical OR. Specifically, collision detection checks whether only one of the nodes wishes to be the sender; receiver notification notifies the receiver of her role in the protocol; veto announces if at least one of the parties has given input 1; and logical OR computes the XOR of the input of all the parties. In Ref. [9], protocols for implementing these classical subroutines were proposed. The protocols were proven to be information-theoretically secure in the classical regime, even with an arbitrary number of corrupted participants, assuming the parties share pairwise authenticated private channels and a broadcast channel. However, security against a quantum adversary was not analyzed. Like in related work [6], here we will assume that the protocols listed above remain secure even in the presence of a quantum adversary. We make this assumption explicit in the security proof presented in Appendix A 2, where we assume that the classical subprotocols only act on the classical input register and create the output register, therefore, not revealing any information other than what is specified by the protocol.

The main concern of any anonymous transmission protocol is to hide the identities of sender S and receiver R. Nonetheless, it is also desired that, in the case in which all the parties act honestly, no information about the transmitted message is revealed. In order to achieve this functionality we add the step where R randomizes the output of the logical OR in Step 6 of Protocol 1. In that way, the classical outcome of the teleportation, m, is sent from S to R in a secret way. Indeed, even though the classical bit m could be sent by a simple anonymous broadcast protocol, the probability of obtaining a particular outcome m can depend on which state is teleported if the established anonymous entanglement is not a maximally entangled state. This is the case especially in the presence of noise in the network (for more details see Appendix A 3).

Note that our protocol is probabilistic, as the parties may abort in Step 5. However, since the measurement outcomes are announced, the creation of anonymous entanglement is heralded. Hence, S and R know when the anonymous entanglement failed to be established before they initiate the teleportation, so in the case in which the protocol aborts, S keeps the state $|\psi\rangle$. In the following we first state the correctness of the protocol and then elaborate on the probability of success in the protocol, as a function of the number of parties in the network N.

Lemma 1 (correctness). If all the parties act honestly and Protocol 1 does not abort, the state $|\psi\rangle$ is transferred from the sender S to the receiver R, except with probability ϵ_{corr}, where ϵ_{corr} is an exponentially vanishing function of the number of rounds used to implement the classical subroutines.

Proof. First, recall that Protocol 1 is built on several classical subroutines and in Ref. [9], protocols to implement these subroutines were presented. The protocols were proven to be correct except with a probability that vanishes exponentially with the number of rounds n_{class} used to implement the subroutines. Second, conditioned on the fact that the classical subroutines are correct and the parties act honestly, the measurement in the $\{|0\rangle, |1\rangle\}$ basis can lead to two situations: (i) all parties obtain measurement outcome 0, in which case the anonymous entangled state between S and R is $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, or (ii) a single party obtains a measurement outcome 1 and then the state between S and R is $|00\rangle$, in which case they abort the protocol. If the parties do not abort the protocol in Step 5, then the state shared by S and R is the maximally entangled state $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)$, which is then used to perfectly teleport state $|\psi\rangle$ from S to R. Altogether, this implies that Protocol 1 is correct except with probability ϵ_{corr} which vanishes exponentially with n_{class}. ■

Lemma 2 (probability of success). Given sender S and receiver R, the probability of obtaining the anonymous entangled state $|\psi^+\rangle$ in Step 4 of Protocol 1 is $\frac{2}{N}$.

Proof. Let $|\vec{0}\rangle\langle\vec{0}|_{N-2}$ denote the projection on the $|0\rangle$ state of $N-2$ parties. The probability P_{ψ^+} of obtaining this state can be expressed as $P_{\psi^+} = [|\text{W}\rangle\langle\text{W}|_N(\mathbb{1}_{SR} \otimes |\vec{0}\rangle\langle\vec{0}|_{N-2})] = \frac{2}{N}[|\psi^+\rangle\langle\psi^+|] = \frac{2}{N}$. ■

Lemma 2 states that in the honest implementation, the probability of not aborting in Step 4 of Protocol 1 decreases with the number of parties. Protocols based on the GHZ state [4,6], on the other hand, are deterministic in creating anonymous entanglement. However, we remark that a fair comparison between the success rate of the two protocols should also take into account the rate of state generation. Note that recently, a linear optical setup for generating the W state in nitrogen-vacancy systems was proposed [10], which could offer a potential advantage in generation rates of the W state, over the GHZ state.

III. SECURITY

As discussed in the previous section, in the task of anonymous transmission the main goal is to keep the identities of sender S and receiver R secret. In this section we present the security definitions and prove the security of Protocol 1 against a semiactive adversary.

Let $[N] = \{1, \ldots, N\}$ be the set of nodes. We say that dishonest nodes are a subset $\mathcal{A} \in [N]$, with $|\mathcal{A}| = t$. This set is defined at the beginning of the protocol, which is known as a *nonadaptive* adversary.

Definition 1 (semiactive adversary). We define the *semiactive adversary* scenario as one in which the adversaries are active, i.e., can perform arbitrary joint operations on their state during the execution of the protocol, but the source distributing a quantum state is trusted.

In particular, for Protocol 1 this means that the state in Step 3 is exactly the W state. This adversarial model is stronger than a *passive* adversary, where it is assumed that the parties follow all the steps of the protocol and only collect the available classical information. However, note that a fully active adversarial scenario would allow the cheating participants to corrupt the source.

We define security in terms of the guessing probability, i.e., the maximum probability that adversaries guess the identity of the S or R given all the classical and quantum information they have available at the end of the protocol. Intuitively, we say that the protocol is secure when the guessing probability is no larger than the uncertainty the adversaries have about the identity of the sender before the protocol begins. This uncertainty is defined by the prior probability, $P[S=i|S\notin\mathcal{A}]$. For example, in the case where all the nodes are equally likely to be the sender, the prior probability is uniform and, therefore, $P[S = i|S \notin \mathcal{A}] = \frac{1}{N-t}$.

In Protocol 1 it is assumed that the message $|\psi\rangle$ to be sent carries no information about the sender's identity. We remark that anonymous transmission is concerned with ensuring anonymity and not secrecy. In the case in which secrecy of the message is required, anonymous transmission could be combined with another primitive that allows one to encrypt the message. However, here, we do not address this issue.

Definition 2 (guessing probability). Let $\mathcal{A}$ be the subset of semiactive adversaries. Let C be the register that contains all classical and quantum side information accessible to the adversaries. Let $W^{\mathcal{A}}$ denote the adversaries' quantum register of the state distributed by the source. Then, the probability of adversaries guessing the sender is given by

$$P_{\text{guess}}[S|W^{\mathcal{A}}, C, S \notin \mathcal{A}] = \max_{\{M^i\}} \sum_{i\in[N]} P[S = i|S \notin \mathcal{A}][M^i \rho_{W^{\mathcal{A}}C|S=i}], \quad (1)$$

where the maximization is taken over the set of POVMs $\{M^i\}$ for the adversaries and $\rho_{W^{\mathcal{A}}C|S=i}$ is the state of the adversaries at the end of the protocol, given that node i is the sender.

Definition 3 (sender security). We say that an anonymous transmission protocol is *sender-secure* if, given that the sender is honest, the probability of the adversary guessing the sender is

$$P_{\text{guess}}[S|W^{\mathcal{A}}, C, S \notin \mathcal{A}] \leqslant \max_{i\in[N]} P[S = i|S \notin \mathcal{A}]. \quad (2)$$

In words, the protocol is sender-secure if the probability that the adversaries guess the identity of S at the end of the protocol is not larger than the probability that an honest node i is the sender, maximized over all the nodes. An analogous definition can be given for the *receiver security*.

We remark that even if S and R are honest, it is trivially possible for the *malicious* parties to prevent S and R from exchanging the desired message. For example, the dishonest parties can measure the W state in a different basis affecting the resulting anonymous entanglement. In this sense, the correctness of Protocol 1 is not robust to malicious attacks. However, in what follows, we show that Protocol 1 is secure, and even in the presence of dishonest parties, the anonymity of S and R is preserved.

Theorem 1. The anonymous transmission protocol with the W state, Protocol 1, is sender- and receiver-secure in the semiactive adversary scenario.

Idea of the proof. For clarity, here we present the main idea of our security proof and we refer the reader to Appendix A 3 for details. Note that in the semiactive adversary scenario we allow the adversaries to apply an arbitrary cheating strategy, which in particular includes not following the steps of the protocol and performing global operations on their joint state. First, let us discuss the sender security. We consider the case when R is honest, $R \notin \mathcal{A}$, as well as when she is dishonest, $R \in \mathcal{A}$. In both cases, the gist of our sender-security proof is to show that the reduced quantum state of the adversary $\rho_{W^{\mathcal{A}}C|S=i}$ at the end of the protocol is independent of the sender, i.e., $\forall i \notin \mathcal{A}$, $\rho_{W^{\mathcal{A}}C|S=i} = \rho_{W^{\mathcal{A}}C}$. To show it, we explicitly use the assumption that the classical protocols do not leak any information about S or R's identity even if the adversary has access to quantum correlations. Therefore, any quantum side information the adversary holds is independent of S. This, together with the fact that the state distributed by the source is permutationally invariant yields the desired equality. Since now the reduced quantum state of the adversary is independent of S we can easily upper-bound the guessing probability by $\max_{i\in[N]} P[S = i|S \notin \mathcal{A}]$. The receiver security can be proven following the same structure. ■

Note that our security proof tolerates any number of cheating nodes. It is also general enough to make a security statement about any resource state that is invariant under permutation of nodes.

Let us now discuss a passive adversarial model, also called the honest-but-curious model. This is the case when the malicious parties follow all the steps of the protocol (in particular, they measure in the $\{0, 1\}$ basis in Step 4), but can collaborate to compare their classical data. Note that the passive adversary model is a special case of the semiactive adversary scenario. However, this model is interesting by itself, since in the case in which the nodes build their anonymous transmission protocol using weaker versions of classical subroutines, i.e., those that are not secure against quantum adversary, the security still holds. Indeed, it restricts the power of the adversary, so that they cannot share any quantum side information. Then, the probability of the adversaries guessing the sender simplifies to $P_{\text{guess}}[S|W^{\mathcal{A}}, C, S \notin \mathcal{A}] = \sum_{a,c} P[W^{\mathcal{A}} = a, C = c] \max_{i\in[N]} P[S = i|W^{\mathcal{A}} = a, C = c, S \notin \mathcal{A}]$, where maximization is taken over all the values of the random variable S, and a, c are possible values of random variables $W^{\mathcal{A}}$ and C, respectively [11]. Note that, unlike before, here $W^{\mathcal{A}}$ is a classical register of the adversary, since their share of the W state was measured in the $\{0, 1\}$ basis. An analogous expression holds for receiver security.

Theorem 2. The anonymous transmission protocol with the W state, Protocol 1, is sender- and receiver-secure in the passive adversary scenario.

The proof of this statement is a special case of the proof of Theorem 1. As before, we use the fact that classical protocols do not leak identities of S and R and the permutational invariance of the resource state to conclude that the classical information generated during the protocol is independent of who is sender and receiver. For details see Appendix A 3.

IV. ANONYMOUS TRANSMISSION IN A NOISY QUANTUM NETWORK

Equipped with the security tools from the previous section, here we analyze the security and performance of Protocol 1 in a noisy quantum network. We consider a noise model in which each qubit is subjected to the same individual noisy channel. One can think that a trusted source prepared the multipartite state for the network, but each qubit is individually affected by a noise map Λ while being transmitted to the nodes. Note that this model can also encompass noise on the local measurements performed on the state. Therefore, in our noisy network, if $|W\rangle_N$ is the perfect N-partite W state prepared by a trusted source, then

$$\omega_N^{\Lambda} = \Lambda^{\otimes N}(|\mathrm{W}\rangle\langle\mathrm{W}|_N) \tag{3}$$

is the state distributed to the parties at Step 3 of Protocol 1.

A. Security in the presence of noise

Perfect security. In what follows we will show that our protocol is perfectly secure in the semiactive adversary scenario in the noisy network defined by Eq. (3). We start by defining what it means for a map to preserve permutational invariance.

Definition 4 (permutational-invariance preserving map). Let π be a permutationally invariant state, such that for all permutations Σ, $\pi = \mathcal{V}_\Sigma(\pi)$, where $\mathcal{V}_\Sigma$ is a map that performs the permutation Σ on the subsystems. A map $\mathcal{E}$ is permutational-invariance preserving if the state after the action of the map $\pi' = \mathcal{E}(\pi)$ is permutationally invariant, i.e., $\pi' = \mathcal{V}_\Sigma(\pi')$.

Note that the noise channel of our interest, $\Lambda^{\otimes N}$, preserves permutational invariance according to the above definition, due to the tensor structure.

Theorem 3. The anonymous transmission protocol with the W state, Protocol 1, is sender- and receiver-secure in the semiactive adversary scenario in a noisy network, where noise is defined by Eq. (3).

Proof. According to Definition 4, the noise channel $\Lambda^{\otimes N}$ is permutational-invariance preserving. Therefore, the proof of Theorem 3 follows exactly the same steps as the proof of Theorem 1, where one replaces the state distributed by the source, $|\mathrm{W}\rangle\langle\mathrm{W}|_N$, with ω_N^{Λ}. Therefore if $\rho^{\Lambda}_{W^{\mathcal{A}}C|S=i}$ is the state of the adversaries at the end of the protocol, given that node i is the sender, we have that $\rho^{\Lambda}_{W^{\mathcal{A}}C|S=i} = \rho^{\Lambda}_{W^{\mathcal{A}}C}$, for all $i \notin \mathcal{A}$, and

$$\begin{aligned} &P_{\text{guess}}[S|A, C, S \notin \mathcal{A}] \\ &\quad := \max_{\{M^i\}} \sum_{i\in[N]} P[S = i|S \notin \mathcal{A}]\left[M^i \rho^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right] \\ &\quad \leqslant \max_{i\in[N]} P[S = i|S \notin \mathcal{A}]. \end{aligned} \tag{4}$$

The same statement holds for receiver security. ■

ε security. In a realistic quantum network, it is quite unlikely that one will be able to control the noise channels perfectly and ensure that all qubits are subjected to the action of exactly the same noise channel. Here we would like to analyze what happens in the case when the network noise is slightly perturbed, in the sense that each qubit experiences a slightly different noise. We say that in the perturbed case, the network noise is such that each individual qubit of the multipartite W state, $|W\rangle_N$, is subjected to an action of a channel Λ_i,

$$\hat{\omega}_N^{\Lambda} = \bigotimes_{i=1}^{N} \Lambda_i(|\mathrm{W}\rangle\langle\mathrm{W}|_N), \tag{5}$$

where $\|\Lambda - \Lambda_i\|_1 \leqslant \varepsilon_i$ for some map Λ, and $\|\cdot\|_1$ denotes the induced trace norm [12].

Since each channel is slightly perturbed, the state after the action of the channel, $\hat{\omega}_N^{\Lambda}$, is no longer perfectly permutationally invariant. Yet, intuitively, since the perturbation is small, the state $\hat{\omega}_N^{\Lambda}$ is ε-close to a permutationally invariant state, for some small ε, and, consequently, the protocol should be ε-secure. In the following we show that this intuition is, indeed, true. First, let us formalize the notion of ε security.

Definition 5 (ε-sender security). We say that the anonymous transmission protocol is *ε-sender-secure* if, given that the sender is not the adversary, the probability of the adversaries guessing the sender is

$$P_{\text{guess}}[S|W^{\mathcal{A}}, C, S \notin \mathcal{A}] \leqslant \max_{i\in[N]} P[S = i|S \notin \mathcal{A}] + \varepsilon. \tag{6}$$

And analogously for ε-receiver security.

Theorem 4. The anonymous transmission protocol with the W state, Protocol 1, is $N\varepsilon_{\max}$-sender-secure in the semiactive adversary scenario when the noise in the network is defined by

Eq. (5), i.e.,

$$\begin{aligned} &P_{\text{guess}}[S|W^{\mathcal{A}}, C, S \notin \mathcal{A}] \\ &= \max_{\{M^i\}} \sum_{i\in[N]} P[S=i|S\notin\mathcal{A}]\big[M^i \hat{\rho}^{\Lambda}_{W^{\mathcal{A}}C|S=i}\big] \\ &\leqslant \max_{i\in[N]} P[S=i|S\notin\mathcal{A}] + N\varepsilon_{\max}, \end{aligned} \tag{7}$$

where $\hat{\rho}^{\Lambda}_{W^{\mathcal{A}}C|S=i}$ is the state of the adversaries at the end of the protocol, and $\varepsilon_{\max} = \max_{i\in[N]} \varepsilon_i$, with ε_i given by Eq. (5).

The idea of the proof is to show that, for all $i \in [N]$, the trace $[M^i \hat{\rho}^{\Lambda}_{W^{\mathcal{A}}C|S=i}]$ is upper-bounded by $[M^i \rho^{\Lambda}_{W^{\mathcal{A}}C|S=i}] + N\varepsilon_{\max}$. Then using the fact that $N\varepsilon_{\max}$ is independent of i, the rest of the proof follows from Theorem 3. For details see Appendix A 3.

B. Performance in a noisy network

In this section we analyze the performance of Protocol 1 in a noisy quantum network. To do so reliably, we assume honest implementation; i.e., all of the parties follow the protocol. In the honest implementation, given success in the protocol, the anonymous entangled state between S and R after Step 5 is

$$\omega_{SR} = \frac{1}{\mathcal{N}} \text{Tr}_{N-2}[\Lambda^{\otimes N}(|\text{W}\rangle\langle\text{W}|_N)(\mathbb{1}_{SR} \otimes |\vec{0}\rangle\langle\vec{0}|_{N-2})], \tag{8}$$

where $|\text{W}\rangle\langle\text{W}|_N$ is the N-partite W state, $|\vec{0}\rangle\langle\vec{0}|_{N-2}$ is a projection onto the $|0\rangle$ state of $N-2$ parties, and $\mathcal{N}$ is a normalization factor. Note that in the case where no noise is present we recover the maximally entangled state, i.e., $\omega_{SR} = |\psi^+\rangle\langle\psi^+|$, where $|\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |01\rangle)$.

Throughout the rest of the paper, we will be interested in discussing the performance of anonymous transmission protocols under two types of noise:

(1) Λ is the dephasing channel

$$\Lambda(\rho) = \mathcal{P}_q(\rho) = q\rho + (1-q)Z\rho Z, \tag{9}$$

where ρ is a single-qubit state, Z is the Pauli Z gate, and $q \in [0, 1]$ is the noise parameter.

(2) Λ is the depolarizing channel

$$\Lambda(\rho) = \mathcal{D}_q(\rho) = q\rho + (1-q)\frac{\mathbb{1}}{2}, \tag{10}$$

where ρ is a single-qubit state, $\frac{\mathbb{1}}{2}$ is a maximally mixed single-qubit state, and $q \in [0, 1]$ is the noise parameter.

Comparison with the GHZ protocol [4]. In the following we are interested in comparing the performance of our protocol using the W state with the protocol that uses the GHZ state (for reference see [4,6]). The main differences between our protocol and the protocol presented in Ref. [4] lie in (i) the initial resource state: W in our case and GHZ for [4]; (ii) the measurement basis: standard basis for our protocol and X basis for [4]; (iii) the fact that our protocol is probabilistic, whereas the one with the GHZ state continues regardless of the measurement outcome.

For the noise under consideration, all measurement outcomes in the GHZ protocol are equally likely and the resulting states are equivalent up to a local unitary operation. Therefore, without loss of generality, we consider the state between S and R created in this protocol to be

$$\gamma_{SR} = \frac{1}{\mathcal{N}'} \text{Tr}_{N-2}[\Lambda^{\otimes N}(|\text{GHZ}\rangle\langle\text{GHZ}|_N)(\mathbb{1}_{SR} \otimes |\vec{+}\rangle\langle\vec{+}|_{N-2})], \tag{11}$$

where $|\text{GHZ}\rangle\langle\text{GHZ}|_N$ is the N-partite GHZ state, $|\vec{+}\rangle\langle\vec{+}|_{N-2}$ is a projection onto the $|+\rangle$ state of $N-2$ honest parties, and $\mathcal{N}'$ is a normalization factor. In the case where no noise is present in the network, the ideal state of S and R is the maximally entangled state $\gamma_{SR} = |\phi^+\rangle\langle\phi^+|$, with $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Note that this is a different maximally entangled state than in our W state protocol, but both states are equally useful for teleportation.

To compare the performance of the two protocols, we fix the figure of merit to be the *fidelity* of the obtained anonymous entangled (AE) state with the ideal state that is obtained in the protocol when no noise is present,

$$F_{AE}(\omega_{SR}) = [\omega_{SR}|\psi^+\rangle\langle\psi^+|], \tag{12}$$

$$F_{AE}(\gamma_{SR}) = [\gamma_{SR}|\phi^+\rangle\langle\phi^+|], \tag{13}$$

where ω_{SR} and γ_{SR} are anonymous entangled states between S and R arising from measuring W and GHZ states subjected to the network noise.

In what follows we define what it means for an anonymous entangled state to be useful. Before that, let us motivate it twofold. First, not all states are entangled enough to be a resource for teleportation. It has been shown in Ref. [13] that any two-qubit entangled state can be used for teleportation if and only if its singlet fidelity exceeds $\frac{1}{2}$. Second, note that the quality of a low-fidelity anonymous entanglement could be further improved by performing entanglement distillation [14]—a protocol which creates an entangled state with high fidelity out of a few lower-fidelity states. However, entanglement distillation protocols can be carried out only when fidelities of initial states are larger than $\frac{1}{2}$. We remark that performing entanglement distillation without compromising security of anonymous transfer requires support of anonymous two-way classical communication between S and R. This can be achieved, for example, by using a classical anonymous broadcast protocol [9].

We are now ready to define what it means to say that a resource state is useful for anonymous transmission.

Definition 6 (usefulness). We say that the anonymous entangled state is a *useful* resource for transmission of a quantum message if its fidelity is strictly larger than $\frac{1}{2}$, i.e., $F_{AE} > \frac{1}{2}$. Therefore an N-partite state is a useful resource state for anonymous transmission if, upon the parties acting honestly, it can generate anonymous entanglement between any two nodes with $F_{AE} > \frac{1}{2}$.

To evaluate the behavior of the protocols, we calculate the fidelity of anonymous entanglement as a function of the noise parameter q and the number of nodes N, for the depolarizing and dephasing channels. Examples of the performance of the

W and GHZ protocols for $N = \{4, 10, 50\}$ are shown in Fig. 1.

	$F_{AE}(\omega_{SR})$	$F_{AE}(\gamma_{SR})$
Dephasing noise $\mathcal{P}_q^{\otimes N}$	$1 - 2q(1-q)$	$\frac{1+(2q-1)^N}{2}$
Depolarizing noise $\mathcal{D}_q^{\otimes N}$	$\frac{(1+q)(N(q-1)^2+4q(1+q))}{4(N(1-q)+4q)}$	$\frac{2q^N+q^2+1}{4}$

We can now ask ourselves which of the states, GHZ or W, tolerates more noise. Note that if one has access to both parameters of the network, noise parameter q and number of nodes N, it is easy to determine which of the states would perform better by simply looking at values of F_{AE} calculated from our analytical expressions.

We start by looking at the dephasing noise. Observe that in this case the fidelity of anonymous entanglement created with the W state $F_{AE}(\omega_{SR})$ is constant in N. Specifically, this implies that when fixed dephasing noise is present in the network, the quality of the anonymous link is always the same, regardless of the number of nodes N. Moreover, for the dephasing noise, one can observe that $F_{AE}(\omega_{SR}) \geqslant F_{AE}(\gamma_{SR})$ for all $N \geqslant 2$ and all q, which implies that our Protocol 1 tolerates more noise than the GHZ-based protocol [4,6].

When depolarizing noise is present in the network, unlike for the dephasing noise, the fidelity of the anonymous entanglement generated by Protocol 1 decreases as the number N of parties increases. Let us define the noise threshold q^* as the minimum value of noise parameter q for which the anonymous entangled state is still useful in the sense of Definition 6. One can see that, for small networks (e.g., $N < 50$), the threshold q^* is lower for the W state than for the GHZ state $q^*_W < q^*_{\mathrm{GHZ}}$, see Fig. 2, which implies that the W state tolerates more noise in these cases. However, for $N \geqslant 182$ one finds that the converse is true, $q^*_W > q^*_{\mathrm{GHZ}}$, and therefore the GHZ-based protocol tolerates more noise in this regime. Nevertheless, in Appendix B 2 we show that for $N \geqslant 182$ and larger values of q, $q > q^*_W$, we still recover the behavior $F_{AE}(\omega_{SR}) \geqslant F_{AE}(\gamma_{SR})$. Lastly, we remark that the challenge to create a multipartite state scales with the number of parties. Therefore, applications of anonymous transmission of interest in the near future will likely be in the range of $N < 50$, in which case Protocol 1 has proven to be the most noise-tolerant.

Let us also comment on the probability of success of our protocol in the presence of noise. Recall that a round of the protocol only succeeds if in Step 3 the measurement outcome of the $N-2$ measuring parties is 0. For the dephasing noise the probability of success in our protocol remains $\frac{2}{N}$, which is due to the fact that the noise commutes with the measurement basis. However, for the depolarizing noise the probability of success drops exponentially in N. In contrast, for the GHZ state, the outcomes do not need to be postselected; therefore the protocol [4] remains deterministic.

Comparison with the relay protocol [7]. We now compare our protocol to a scheme proposed in Ref. [7], which only requires the creation of local Bell pairs and therefore could potentially offer an advantage for a quantum network implementation. The main idea of the relay protocol [7] is to locally prepare and transmit Bell pairs in order to create a four-partite GHZ state, which will then be turned into anonymous entanglement.

In the protocol proposed in Ref. [7], the nodes are consecutively ordered and each node locally prepares a Bell pair. The first node sends half of her Bell pair to the second node. The second node performs entanglement swapping with a half of her own Bell pair and sends the other half of the state to the next node. This relay continues until the last Nth node is reached. S and R, however, perform an additional CNOT operation, where they locally entangle the state received from another node with an additional qubit initiated in $|0\rangle$. At

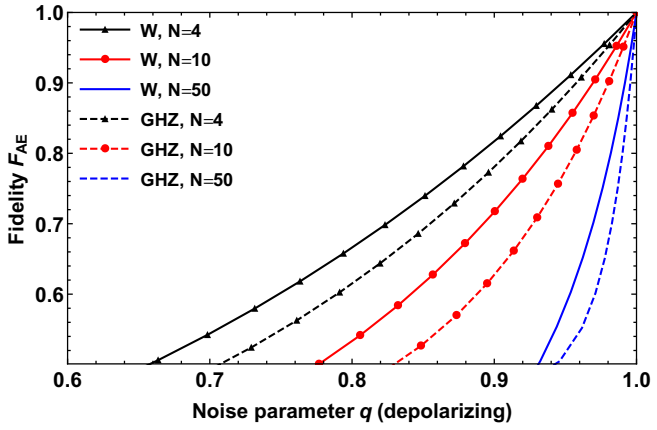


FIG. 1. Fidelity of anonymous entanglement as a function of the noise parameter q for depolarizing network noise. Examples for $N = \{4, 10, 50\}$.

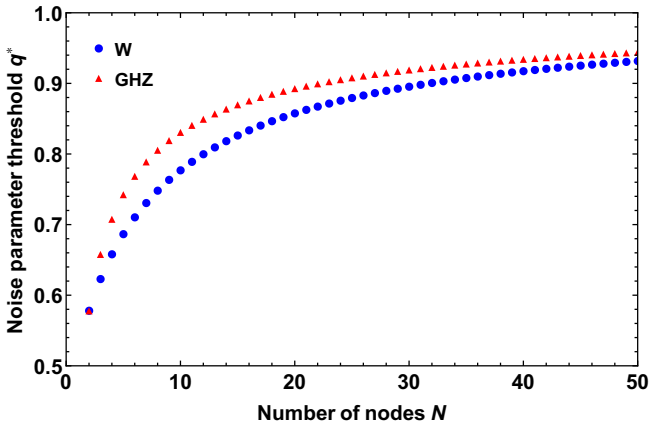


FIG. 2. Depolarizing parameter thresholds for fidelity of anonymous entanglement $F_{AE} = \frac{1}{2}$.

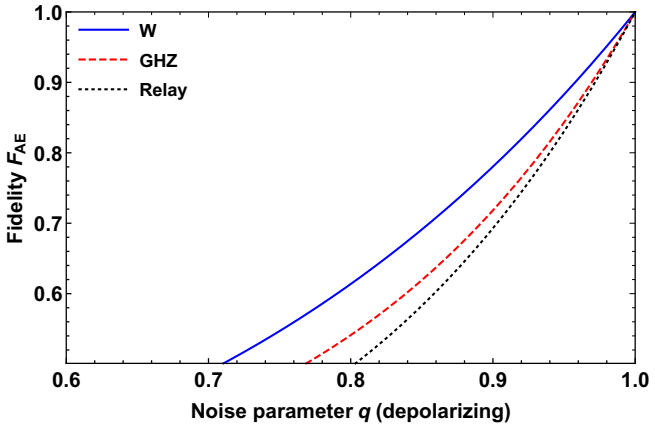


FIG. 3. Comparison of the fidelity of anonymous entanglement F_{AE} for the W state protocol (Protocol 1), the GHZ protocol [4], and the relay scheme [7] for $N = 6$ nodes.

the end of this relay a four-partite GHZ state is created among S, R, the first and the last node. Finally, anonymous entanglement is established after the first and the last node perform a measurement.

We explore a scenario for $N = 6$ nodes, assuming that the network is such that quantum channels between parties are depolarizing channels $\Lambda = \mathcal{D}_q$; i.e., whenever a qubit is sent from one party to another it is subject to depolarization. We calculate fidelities of anonymous entanglement for different locations of the S and R in the network. Our results are summarized in Appendix B 2. The numerical evidence shows that in the presence of the depolarizing noise in the network, the fidelity of anonymous entanglement is different depending on the ordering of S and R in the network. Note that this does not necessarily imply that the security of the protocol is broken, in the sense that nodes can learn the identity of S and R. However, we can see that the performance of the protocol strongly depends on who is sender and receiver, which is not a desirable feature for the anonymous transmission task.

With this in mind, we define the usefulness of the anonymous entanglement created with the relay scheme as the worst case fidelity achieved by the scheme. This is practical if one wants to make sure that the scheme achieves at least a certain fidelity threshold. We then compare the behavior of the relay scheme with the behavior of Protocol 1 in the presence of depolarizing noise. In Fig. 3 one can see that in the presence of the depolarizing noise in the network the relay protocol achieves lower fidelity than both the GHZ and the W state protocols.

Nonresponsive nodes. Finally, let us consider the scenario where some of the nodes, that are neither S nor R, stop responding. This can happen, for example, due to particle losses in the multipartite state. Note that if S or R lose their particle the teleportation cannot be carried out and, therefore, the protocol is not correct.

Let us consider that the resource state prepared by the source suffers from the action of a noise channel where particles might get lost. Then, with some probability k out of N nodes experience particle loss. Here we ask the question of how many particle losses can be tolerated in an anonymous transmission protocol. Say that a protocol tolerates k' particle losses. After the distribution of the state, if k particles are lost, (i) the nodes abort the protocol if $k > k'$, or (ii) the remaining $N - k$ parties proceed with the protocol if $k \leqslant k'$.

It is known that the entanglement of the GHZ state is not robust to particle losses; i.e., if one particle is lost the remaining $N - 1$ parties are left with a separable state. On the other hand, if the W state is subjected to $N - 2$ particle losses the remaining bipartite state is still entangled. In fact, the W state is the most robust to particle losses among all N qubit states [15]. Motivated by this property of the W state, we show that Protocol 1 can tolerate one nonresponsive node. Observe that the N-partite W state has the following form after tracing out k out of N parties,

$$\mathrm{Tr}_k|\mathrm{W}\rangle\langle\mathrm{W}|_N = \frac{N-k}{N}|\mathrm{W}\rangle\langle\mathrm{W}|_{N-k} + \frac{k}{N}|\vec{0}\rangle\langle\vec{0}|_{N-k}, \tag{14}$$

where $|\mathrm{W}\rangle\langle\mathrm{W}|_{N-k}$ is the W state of $N - k$ parties.

In the following theorem we show that Protocol 1 tolerates one particle loss.

Theorem 5. Protocol 1 tolerates one nonresponsive node $i \in [N] \setminus \{S, R\}$ to produce useful anonymous entanglement, regardless of the number of parties.

Proof. The proof of the above theorem involves two steps. We first show the correctness of Protocol 1 when one of the nodes stopped responding, and then show that the created entangled link between S and R is in fact anonymous, i.e., that the security is preserved.

Let us look at the correctness. The measurement of the state (14) in the standard basis and after obtaining all 0 outcomes on $N - k - 2$ parties yields a normalized state

$$\tilde{\omega}_{SR} = \frac{2}{2+k}|\psi^+\rangle\langle\psi^+| + \frac{k}{2+k}|00\rangle\langle 00|, \tag{15}$$

which has entanglement fidelity $F_{AE}(\tilde{\omega}_{SR}) = \frac{2}{2+k}$. By Definition 6 the state $\tilde{\omega}_{SR}$ is useful for anonymous transmission if $\frac{2}{2+k} > \frac{1}{2}$ which implies $k < 2$. This yields the desired result.

To show that the created entanglement is anonymous, observe that when one of the nodes stops responding the resource state is the state from Eq. (14) with $k = 1$. This state is invariant under permutations of nodes and, therefore, we can treat it as a new resource state. Then the security proof follows the same pattern as the proof of Theorem 1. ■

For completeness, in Appendix B 2 we provide analytical expressions for the fidelity of anonymous entanglement when the W state is subjected to one particle loss, as well as dephasing and depolarizing noise. Figure 4 shows the comparison of anonymous entanglement fidelity of Protocol 1 under depolarizing noise without particle loss, $F_{AE}(\omega_{SR})$, and when one particle is lost, $F_{AE}(\tilde{\omega}_{SR})$, for $N = \{4, 10, 50\}$ nodes. Note that with the growing number of nodes the fidelity of anonymous entanglement in the lossy case approaches the one with no loss. Indeed, the larger N the smaller the admixture of the $|\vec{0}\rangle\langle\vec{0}|_{N-1}$ term in Eq. (14), and so, with growing N the fidelity is less affected by the loss of a particle. On the other hand, for a larger number of nodes more than one particle loss is more likely to occur. Therefore, the probability that the protocol aborts also increases with the number of nodes.

Lastly, we point out that when one particle is lost in the protocol of Ref. [7], the relay cannot be completed. Therefore,

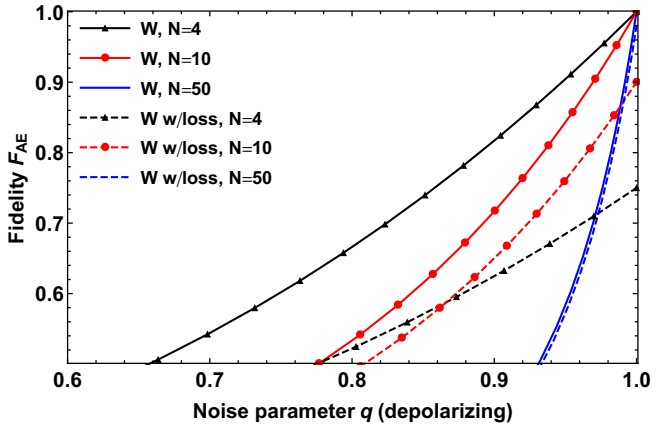


FIG. 4. Fidelity of anonymous entanglement as a function of the noise parameter q for depolarizing network noise when the resource W state is subjected to one particle loss. Examples for $N = \{4, 10, 50\}$.

much like the GHZ protocol, the relay protocol also cannot be used to create anonymous entanglement whenever one of the nodes is not responsive.

V. OUTLOOK

We presented a protocol for quantum anonymous transmission using the W state, and proved its security in the semiactive adversary scenario, i.e., when the adversary is active and the source of a quantum state is trusted. Moreover, we analyzed the behavior of our protocol under the action of common noise models that occur in a realistic quantum network. An important question is whether our security proof can be extended to the case where the source might be corrupted, i.e., the fully active adversary scenario. Note that to achieve full security in the noiseless case for the GHZ protocol, Refs. [6,16] introduced a certification step of the resource state shared by the trusted parties. We remark that for the noiseless W state protocol, it may be possible to achieve full security in a similar way by employing self-testing techniques [17,18]. The problem of certifying the resource state in the presence of noise in the network remains an open question.

We have also analyzed the security of our protocol when each qubit suffers the action of a noise channel with slightly different parameters. This bound, however, may not be tight, so another interesting question is whether the security proof can be improved and a stronger bound can be derived for this case.

Finally, we have seen that in many instances our W-state based protocol outperforms the GHZ-state and Bell-pair based protocols. For the values of parameters N and q, where all the protocols produce useful anonymous entanglement, we remark that a more refined comparison of their performance should take into account the generation rates and resources required to produce the states in every particular experimental setup.

ACKNOWLEDGMENTS

We would like to thank J. Ribeiro, V. Caprara Vivoli, A. Dahlberg, F. Rozpędek, I. Kerenidis, and E. Diamanti for valuable discussions and insights. We also thank K. Chakraborty, B. Dirkse, M. Steudtner, and K. Goodenough for feedback on the manuscript. This work was supported by STW Netherlands, NWO VIDI, ERC Starting Grant, and NWO Zwaartekracht QSC.

APPENDIX A: SECURITY

1. Classical subroutines

Our anonymous transmission protocol, Protocol 1, is built on a few classical subroutines. As mentioned, in Ref. [9], protocols for implementing these classical subroutines were proposed. Here we list the protocols which we will use as building blocks of our anonymous transmission protocol.

Theorem 6 (collision detection [9]). There exists an information-theoretically secure collision detection protocol that takes as input the classical register Cd_{in} of all the participants, $Cd^i_{\text{in}} = 1$ if node i wishes to be a sender and $Cd^i_{\text{in}} = 0$ otherwise, and outputs $Cd_{\text{out}} = 0$ if only one register wants to be the sender and $Cd_{\text{out}} = 1$ otherwise.

Theorem 7 (receiver notification [9]). There exists an information-theoretically secure receiver notification protocol that takes as input the classical register Rn_{in} of the participants and outputs Rn_{out}, where $Rn^R_{\text{out}} = 1$ for the receiver, and all the other parties get output 0.

Theorem 8 (veto [9]). There exists an information-theoretically secure veto protocol that takes as input the classical register O_{in} of the parties and outputs $O_{\text{out}} = 0$ if all the parties input 0, $O_{\text{in}} = 0$, and $O_{\text{out}} = 1$ otherwise.

Theorem 9 (logical OR [9]). There exists an information-theoretically secure logical OR protocol that takes as input the classical register T_{in} and publicly outputs $T_{\text{out}} = \oplus_{i=1}^{N} T^i_{\text{in}}$.

The protocols are information-theoretically secure, in the sense that they do not reveal any classical information other than the one specified by the protocol. The security holds even with an arbitrary number of corrupted participants, assuming the parties share pairwise authenticated private channels and a broadcast channel. However, security against a quantum adversary was not analyzed. Here we assume that the protocols listed above remain secure even in the presence of a quantum adversary. This assumption is made explicit in Appendix A 2 where we assume that the classical subprotocols only act on the classical input register and create the output register, therefore not revealing any information other than what is specified by the protocol, also in the quantum setting.

2. States and registers

In what follows we make a detailed description of the state in each step of Protocol 1. Our main goal is to show that the quantum state of the adversary at the end of the protocol does not depend on who is the sender or the receiver. We will later use this fact in the security proof in Sec. III.

Here we adopt the notation that A denotes registers held by the adversary $\mathcal{A}$, and $\bar{A}$ denotes all the other registers, i.e., of the honest parties (including the sender and the receiver).

TABLE I. Registers available to parties at each step of Protocol 1. All registers are classical unless specified otherwise.

Step	Available registers	Description
0	A_0, $\bar{A}_0$	Quantum side information of dishonest and honest parties before the beginning of Protocol 1.
1	Cd_{in}^{A}, $Cd_{\text{in}}^{\bar{A}}$	Private input of the parties in the collision detection protocol.
		The node which wants to be a sender inputs 1, the rest 0.
	Cd_{out}^{A}, $Cd_{\text{out}}^{\bar{A}}$	Outputs of the collision detection protocol.
2	Rn_{in}^{A}, $Rn_{\text{in}}^{\bar{A}}$	Private input of the receiver notification protocol.
		S inputs the identifier of R, everyone else 0.
	Rn_{out}^{A}, $Rn_{\text{out}}^{\bar{A}}$	Private outputs of receiver notification protocol.
		Output 0 for R, 1 for everyone else.
	$D^{\mathcal{A}}$, $D^{\mathcal{H}SR}$	Redefined register of dishonest parties $D^{\mathcal{A}} = \{A_0 Cd_{\text{in}}^{A} Cd_{\text{out}}^{A} Rn_{\text{in}}^{A} Rn_{\text{out}}^{A}\}$
		and honest parties $D^{\mathcal{H}SR} = \{\bar{A}_0 Cd_{\text{in}}^{\bar{A}} Cd_{\text{out}}^{\bar{A}} Rn_{\text{in}}^{\bar{A}} Rn_{\text{out}}^{\bar{A}}\}$ after Step 2.
3	$W^{\mathcal{H}}$, $W^{\mathcal{A}}$, W^{S}, W^{R}	Quantum registers of the state prepared by the source.
4	$W^{\mathcal{H}}$, $W^{\mathcal{A}}$, W^{S}, W^{R}	Quantum registers of the state prepared by the source.
5	$O_{\text{in}}^{\mathcal{H}}$	Private input of the honest parties to the veto protocol.
		Represented by a string of measurement outcomes $\vec{\nu}$.
	$O_{\text{in}}^{\mathcal{A}}$	Private input of dishonest parties to the veto protocol.
		Represented by a string of measurement outcomes $\vec{\mu}$.
	O_{out}	Public output of the veto protocol.
		0 if all entries of strings $\vec{\nu}$ and $\vec{\mu}$ are 0, 1 otherwise.
6	Q	Quantum register of quantum message $\|\psi\rangle$ which S wants to transmit.
	T_{in}^{S}, T_{in}^{R}	Private inputs of S and R to the logical OR protocol.
		S inputs teleportation message m and R inputs random bit rand.
	$T_{\text{in}}^{\mathcal{H}}$, $T_{\text{in}}^{\mathcal{A}}$	Private input of the honest and dishonest parties to the logical OR protocol.
	T	Public outcome the logical OR protocol. Outputs XOR of all the inputs.

After Step 2, i.e., once S and R are defined, we distinguish S and R registers from the registers of honest parties $\mathcal{H}$.

In the following we specify what are the assumptions associated with each step of the protocol. Additionally, we explicitly write out the state $\xi^{(j)}$ after each step j of the protocol, taking into account all the registers that play a role in the particular step. Therefore, we remark that our notation may be cumbersome at the first glance. However, we advise the reader to refer to Table I at any point of our proof.

Step 1: Collision detection

Assumption 1. Let A_0 be the quantum side information of dishonest parties and $\bar{A}_0$ be the quantum side information of the honest parties, including sender and receiver, before the beginning of the protocol. We assume that before the start of the protocol the parties share the following state:

$$\xi^{(0)}_{A_0\bar{A}_0 Cd_{\text{in}} Rn_{\text{in}}} = \sigma^{(0)}_{A_0\bar{A}_0 Cd_{\text{in}}^{A} Rn_{\text{in}}^{A}} \otimes \sigma^{(0)}_{Cd_{\text{in}}^{\bar{A}} Rn_{\text{in}}^{\bar{A}}}. \tag{A1}$$

In words, we assume the adversaries have a quantum side information, A_0, and classical inputs to the collision detection and receiver notification protocols, Cd_{in}^{A} and Rn_{in}^{A}, that might be correlated with some quantum side information $\bar{A}_0$ of the remaining parties. However the inputs of the honest parties $Cd_{\text{in}}^{\bar{A}}$ and $Rn_{\text{in}}^{\bar{A}}$ are uncorrelated with the adversary's state.

Assumption 2. We assume that the classical collision detection protocol is secure against a quantum adversary; that is, it acts on classical registers Cd_{in} and outputs Cd_{out} without revealing any other information to the dishonest parties. In particular, if sender and receiver are honest, it does not leak their identity.

Let $\xi^{(1)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}}}$ be the global output state after collision detection (Step 1). Assumption 2 implies that tracing out the registers of honest parties (all registers of $\bar{A}$) we obtain a partial state of the adversary (all registers of A) which is independent of the sender, if the sender is honest. That is, for all honest parties, $\forall i \notin \mathcal{A}$, the state after the collision detection step (Step 1 of Protocol 1) is

$$\text{Tr}_{\bar{A}_0 Cd_{\text{in}}^{\bar{A}} Cd_{\text{out}}^{\bar{A}} Rn_{\text{in}}^{\bar{A}}}\left(\xi^{(1)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}}|S=i}\right) = \xi^{(1)}_{A_0 Cd_{\text{in}}^{A} Cd_{\text{out}}^{A} Rn_{\text{in}}^{A}|S=i} \tag{A2}$$

$$= \xi^{(1)}_{A_0 Cd_{\text{in}}^{A} Cd_{\text{out}}^{A} Rn_{\text{in}}^{A}}. \tag{A3}$$

Step 2: Receiver notification

Assumption 3. We assume that the classical receiver notification protocol is secure against the quantum adversary; that is, the protocol acts on the classical register Rn_{in} and outputs Rn_{out}, without revealing any other information to the dishonest parties. In particular, if sender and receiver are honest, it does not leak their identity.

Let the input state to the receiver notification protocol be $\xi^{(1)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}}}$ and the output state conditioned on node i being the sender be $\xi^{(2)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}} Rn_{\text{out}}|S=i}$. Assumption 3 implies that, again, tracing out the registers of honest parties (all registers of $\bar{A}$) we obtain a partial state of the adversary (all registers of A) which is independent of the sender. That is, for all honest parties $\forall i \notin \mathcal{A}$, the state after the receiver notification step (Step 2 of Protocol 1) is

$$\text{Tr}_{\bar{A}_0 Cd_{\text{in}}^{\bar{A}} Cd_{\text{out}}^{\bar{A}} Rn_{\text{in}}^{\bar{A}} Rn_{\text{in}}^{\bar{A}} Rn_{\text{out}}^{\bar{A}}}\left(\xi^{(2)}_{A_0\bar{A}_0 Cd_{\text{in}} Cd_{\text{out}} Rn_{\text{in}} Rn_{\text{out}}|S=i}\right) = \xi^{(2)}_{A_0 Cd_{\text{in}}^{A} Cd_{\text{out}}^{A} Rn_{\text{in}}^{A} Rn_{\text{out}}^{A}|S=i} \tag{A4}$$

$$= \xi^{(2)}_{A_0 C d^A_{\text{in}} C d^A_{\text{out}} R n^A_{\text{in}} R n^A_{\text{out}}}. \tag{A5}$$

For clarity, we denote the state after the receiver notification (Step 2), given that node i is the sender, by

$$\xi^{(2)}_{A_0 \bar{A}_0 C d_{\text{in}} C d_{\text{out}} R n_{\text{in}} R n_{\text{out}} | S=i} \equiv \sigma_{D^{\mathcal{A}} D^{\mathcal{H}SR} | S=i}, \tag{A6}$$

where $D^{\mathcal{A}} = \{A_0 C d^A_{\text{in}} C d^A_{\text{out}} R n^A_{\text{in}} R n^A_{\text{out}}\}$ denotes all the registers in possession of the adversary at the end of Step 2. And similarly, $D^{\mathcal{H}SR}$ denotes the registers of the honest parties. Note that now that sender S and receiver R are defined, we distinguish them from the subset of honest players.

Lemma 3. If S and R are honest, the state of the adversary at the end of the receiver notification protocol does not carry any information about their identity. Let $\sigma_{D^{\mathcal{A}}|S=i} := \text{Tr}_{D^{\mathcal{H}SR}}[\sigma_{D^{\mathcal{A}} D^{\mathcal{H}SR}|S=i}]$; by Assumptions 2 and 3 it holds that

$$\sigma_{D^{\mathcal{A}}|S=i} = \sigma_{D^{\mathcal{A}}|S=j} = \sigma_{D^{\mathcal{A}}} \quad \forall i, j \notin \mathcal{A} \tag{A7}$$

and

$$\sigma_{D^{\mathcal{A}}|R=i} = \sigma_{D^{\mathcal{A}}|R=j} = \sigma_{D^{\mathcal{A}}} \quad \forall i, j \notin \mathcal{A}. \tag{A8}$$

Step 3: State distribution

Assumption 4. The N-partite state distributed by a trusted source is $|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R}$. Here $W^{\mathcal{H}}$ is the *quantum* register of the honest parties, $W^{\mathcal{A}}$ is the *quantum* register of dishonest parties, and W^S and W^R are *quantum* registers of the sender and receiver.

Therefore, the global state after the source distributed the quantum state (Step 3 of Protocol 1) is

$$\xi^{(3)}_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R D^{\mathcal{A}} D^{\mathcal{H}SR} | S=i} = |\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R} \otimes \sigma_{D^{\mathcal{A}} D^{\mathcal{H}SR}|S=i}. \tag{A9}$$

Step 4: Measurement

Step 4 describes a measurement on quantum registers $W^{\mathcal{H}} W^{\mathcal{A}}$ and creates the classical registers $O^{\mathcal{H}}_{\text{in}}$ and $O^{\mathcal{A}}_{\text{in}}$. The honest parties perform a projection $\Pi^{\vec{\nu}}_{W^{\mathcal{H}}}$ on the $\{0, 1\}$ basis and the string of outcomes $\vec{\nu}$ is recorded on register $O^{\mathcal{H}}_{\text{in}}$. The adversaries, however, instead of performing the measurement specified by the protocol, can apply an arbitrary map on their registers and produce a classical outcome $|\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathcal{A}}_{\text{in}}}$. This action is descried by applying a map $\mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}} D^{\mathcal{A}}}$ labeled by $\vec{\mu}$, which acts on registers $W^{\mathcal{A}} D^{\mathcal{A}}$ and producing a classical outcome $|\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathcal{A}}_{\text{in}}}$ in register $O^{\mathcal{A}}_{\text{in}}$. Note that this outcome can be a strategy upon which dishonest parties agree and, in particular, it does not have to represent the actual action of the map $\mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}} D^{\mathcal{A}}}$. Therefore, the state after the parties perform local measurements (Step 4 of Protocol 1) is described as

$$\xi^{(4)}_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R D^{\mathcal{A}} D^{\mathcal{H}SR} O^{\mathcal{H}}_{\text{in}} O^{\mathcal{A}}_{\text{in}} | S=i} = \sum_{\vec{\mu}, \vec{\nu}} \Pi^{\vec{\nu}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}} D^{\mathcal{A}}} (|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R} \otimes \sigma_{D^{\mathcal{A}} D^{\mathcal{H}SR}|S=i}) \otimes |\vec{\nu}\rangle\langle\vec{\nu}|_{O^{\mathcal{H}}_{\text{in}}} \otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathcal{A}}_{\text{in}}}, \tag{A10}$$

where $\Pi^{\vec{\nu}}_{W^{\mathcal{H}}}$ corresponds to a projection of register $W^{\mathcal{H}}$ onto the state $|\vec{\nu}\rangle\langle\vec{\nu}|$ in the standard basis.

Step 5: Anonymous announcement of outcomes

Each of the parties inputs their measurement outcome into the veto protocol. In particular, $O^{\mathcal{H}}_{\text{in}} = |\vec{\nu}\rangle\langle\vec{\nu}|_{O^{\mathcal{H}}_{\text{in}}}$ is a private input of the honest parties and $O^{\mathcal{A}}_{\text{in}} = |\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathcal{A}}_{\text{in}}}$ is a private input of the dishonest parties.

Assumption 5. We assume that the classical veto protocol is secure against the quantum adversary; i.e., the veto protocol acts on the classical registers $O^{\mathcal{H}}_{\text{in}}$, $O^{\mathcal{A}}_{\text{in}}$, and only outputs $O_{\text{out}} = 0$ if $O^{\mathcal{H}}_{\text{in}} = O^{\mathcal{A}}_{\text{in}} = |\vec{0}\rangle\langle\vec{0}|$ and 1 otherwise, and does not reveal any other information.

Then, the state after the veto protocol, where the parties announce their outcomes (Step 5 of Protocol 1), is

$$\begin{aligned}\xi^{(5)}_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R D^{\mathcal{HASR}} O^{\mathcal{H}}_{\text{in}} O^{\mathcal{A}}_{\text{in}} O_{\text{out}} | S=i} &= \Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{0}}_{W^{\mathcal{A}} D^{\mathcal{A}}} (|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R} \otimes \sigma_{D^{\mathcal{A}} D^{\mathcal{H}SR}|S=i}) \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathcal{H}}_{\text{in}}} \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathcal{A}}_{\text{in}}} \otimes |0\rangle\langle 0|_{O_{\text{out}}} \\ &\quad + \sum_{\vec{\mu} \neq 0, \vec{\nu}} \Pi^{\vec{\nu}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}} D^{\mathcal{A}}} (|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R} \otimes \sigma_{D^{\mathcal{A}} D^{\mathcal{H}SR}|S=i}) \otimes |\vec{\nu}\rangle\langle\vec{\nu}|_{O^{\mathcal{H}}_{\text{in}}} \otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathcal{A}}_{\text{in}}} \otimes |1\rangle\langle 1|_{O_{\text{out}}}.\end{aligned} \tag{A11}$$

Step 6: Teleportation

In Step 6, sender and receiver wish to perform the teleportation. To do so, the sender performs the Bell state measurement and communicates the classical outcome to the receiver, so that she can correct the teleported state. The classical communication is carried out by using the classical protocol logical OR.

Assumption 6. The classical logical OR protocol acts on classical registers and does not reveal any information other than the logical OR of the inputs.

Let Q denote the register of the quantum message which sender S wishes to transmit. More formally, this step consists of applying a map, a Bell state measurement, acting on the registers of the sender W^S and Q and producing a classical message in the public register T, followed by the receiver applying a unitary operation according to the outcome m of the Bell measurement. We denote the map that describes the teleportation step by $\mathcal{T}_{W^S W^R Q O_{\text{out}} \to W^S W^R Q O_{\text{out}} T^S_{\text{in}} T^R_{\text{in}} T}$. Its action is conditioned on the outcome of Step 5, i.e., public output of the veto protocol. We define its action on a state $\phi_{W^S W^R} \otimes |\psi\rangle\langle\psi|_Q$ as follows,

$$\mathcal{T}_{W^S W^R Q | O_{\text{out}}=0 \to W^S W^R Q O_{\text{out}} T^S_{\text{in}} T^R_{\text{in}} T} := \sum_m \mathcal{R}^m_{W^R} \circ \mathcal{B}^m_{W^S Q} (\phi_{W^S W^R} \otimes |\psi\rangle\langle\psi|_Q) \otimes \sum_{\text{rand}} \frac{1}{4} |m\rangle\langle m|_{T^S_{\text{in}}}$$

$$\otimes |\text{rand}\rangle\langle\text{rand}|_{T_{\text{in}}^R} \otimes |m \oplus \text{rand}\rangle\langle m \oplus \text{rand}|_T, \tag{A12}$$

$$\mathcal{T}_{W^S W^R Q|O_{\text{out}}=1 \to W^S W^R Q O_{\text{out}} T_{\text{in}}^S T_{\text{in}}^R T} := \mathbb{1}_{W^S W^R Q}(\phi_{W^S W^R} \otimes |\psi\rangle\langle\psi|_Q) \otimes |\perp\rangle\langle\perp|_{T_{\text{in}}^S} \otimes |\perp\rangle\langle\perp|_{T_{\text{in}}^R} \otimes |\perp\rangle\langle\perp|_T. \tag{A13}$$

The map $\mathcal{B}^m_{W^S Q}$ represents the Bell state measurement, on registers $W^S Q$, with outcome m, and the map $\mathcal{R}^m_{W^R}$ corresponds to the unitary the receiver applies to correct the teleported state. The action of the map $\mathcal{T}_{W^S W^R Q O_{\text{out}} \to W^S W^R Q O_{\text{out}} T_{\text{in}}^S T_{\text{in}}^R T}$ describes that the state $|\psi\rangle\langle\psi|_Q$ is either teleported to register W^R when $O_{\text{out}} = 0$ or the protocol aborts when $O_{\text{out}} = 1$, which we represent by the state $|\perp\rangle\langle\perp|_T$ in register T.

However, we note that in this step the adversaries could also deviate from the protocol. In general, they could perform an arbitrary map in their registers and input a string $\vec{\kappa} \neq \vec{0}$ to the logical OR protocol. In that case, the teleportation step can be described as

$$\begin{aligned}
&\mathcal{T}_{W^S W^R W^{\mathcal{A}} D^{\mathcal{A}} Q|O_{\text{out}}=0 \to W^S W^R W^{\mathcal{A}} D^{\mathcal{A}} Q O_{\text{out}} T_{\text{in}}^S T_{\text{in}}^R T_{\text{in}}^{\mathcal{A}} T}\left(\xi^{(5)}_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R Q D^{\mathcal{H}\mathcal{A}SR} O_{\text{in}}^{\mathcal{H}} O_{\text{in}}^{\mathcal{A}} O_{\text{out}}|S=i}\right) \\
&\quad := \sum_{m,\vec{\kappa}} \mathcal{R}^{m\oplus_i \kappa_i}_{W^R} \circ \mathcal{G}^{\vec{\kappa}}_{W^{\mathcal{A}} D^{\mathcal{A}}} \circ \mathcal{B}^m_{W^S Q}\left(\Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{0}}_{W^{\mathcal{A}} D^{\mathcal{A}}}(|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{A}} D^{\mathcal{H}SR}|S=i})\right) \\
&\qquad \otimes \sum_{\text{rand}} \frac{1}{4} |m\rangle\langle m|_{T_{\text{in}}^S} \otimes |\text{rand}\rangle\langle\text{rand}|_{T_{\text{in}}^R} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T_{\text{in}}^{\mathcal{A}}} \otimes |m \oplus \text{rand} \oplus_i \kappa_i\rangle\langle m \oplus \text{rand} \oplus_i \kappa_i|_T,
\end{aligned} \tag{A14}$$

where $\mathcal{G}^{\vec{\kappa}}_{W^{\mathcal{A}} D^{\mathcal{A}}}$ represents an arbitrary map the adversaries apply to registers $W^{\mathcal{A}} D^{\mathcal{A}}$, which is followed by the creation of classical register $T_{\text{in}}^{\mathcal{A}}$. $\mathcal{R}_R^{m\oplus_i \kappa_i}$ expresses the fact that the receiver now applies a unitary labeled by $m \oplus_i \kappa_i$ instead of m.

Note that the map $\mathcal{G}^{\vec{\kappa}}_{W^{\mathcal{A}} D^{\mathcal{A}}}$ only acts on the registers of the adversaries and after the teleportation step (Step 6) no other operations are performed by the honest parties. The security of the protocol is defined in terms of the guessing probability, which takes into account an optimization over all maps on the register of the adversary. Therefore, for the security analysis, we can, without loss of generality, neglect the map $\mathcal{G}^{\vec{\kappa}}_{A D^{\mathcal{A}}}$ in the final state, since it is taken into account in the definition of the guessing probability.

Finally, the state after the teleportation protocol (Step 6 of Protocol 1) is

$$\begin{aligned}
&\xi^{(6)}_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R Q D^{\mathcal{H}\mathcal{A}SR} O_{\text{in}}^{\mathcal{H}} O_{\text{in}}^{\mathcal{A}} O_{\text{out}} T_{\text{in}}^S T_{\text{in}}^R T_{\text{in}}^{\mathcal{A}} T|S=i} \\
&\quad = \sum_{m,\vec{\kappa}} \mathcal{R}^{m\oplus_i \kappa_i}_{W^R} \circ \mathcal{B}^m_{W^S Q}\left(\Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{0}}_{W^{\mathcal{A}} D^{\mathcal{A}}}(|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{A}} D^{\mathcal{H}SR}|S=i})\right) \\
&\qquad \otimes |\vec{0}\rangle\langle\vec{0}|_{O_{\text{in}}^{\mathcal{H}}} \otimes |\vec{0}\rangle\langle\vec{0}|_{O_{\text{in}}^{\mathcal{A}}} \otimes |0\rangle\langle 0|_{O_{\text{out}}} \otimes \sum_{\text{rand}} \frac{1}{4} |m\rangle\langle m|_{T_{\text{in}}^S} \otimes |\text{rand}\rangle\langle\text{rand}|_{T_{\text{in}}^R} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T_{\text{in}}^{\mathcal{A}}} \otimes |m \oplus \text{rand} \oplus_i \kappa_i\rangle\langle m \oplus \text{rand} \oplus_i \kappa_i|_T \\
&\qquad + \sum_{\vec{\mu}\neq 0,\vec{\nu}} \mathbb{1}_{W^S W^R Q}\left(\Pi^{\vec{\nu}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}} D^{\mathcal{A}}}(|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{A}} D^{\mathcal{H}SR}|S=i})\right) \\
&\qquad \otimes |\vec{\nu}\rangle\langle\vec{\nu}|_{O_{\text{in}}^{\mathcal{H}}} \otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O_{\text{in}}^{\mathcal{A}}} \otimes |1\rangle\langle 1|_{O_{\text{out}}} \otimes |\perp\rangle\langle\perp|_{T_{\text{in}}^S} \otimes |\perp\rangle\langle\perp|_{T_{\text{in}}^R} \otimes |\perp\rangle\langle\perp|_{T_{\text{in}}^{\mathcal{A}}} \otimes |\perp\rangle\langle\perp|_T.
\end{aligned} \tag{A15}$$

Observe, however, that the classical registers $D^{\mathcal{H}SR}$, $O_{\text{in}}^{\mathcal{H}}$, $T_{\text{in}}^S T_{\text{in}}^R$ are not further acted upon with any map. Moreover, their content is private, as by Lemma 3 and Assumptions 5 and 6 no information about it is revealed to the adversary. Since we are interested in the information available to the adversary we will trace out these subsystems.

Lemma 4. Let $C = \{D^{\mathcal{A}}, O_{\text{in}}^{\mathcal{A}}, O_{\text{out}}, T_{\text{in}}^{\mathcal{A}}, T\}$ represent all the classical and quantum side information accessible to the adversary at the end of the protocol. The reduced output state of the anonymous transmission protocol with the W state, where we trace out all private information of the honest parties $\mathcal{H}$, S, and R, given that node i is the sender, can be described as follows,

$$\begin{aligned}
\rho_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R Q C|S=i} = &\sum_{m,\vec{\kappa}} \mathcal{R}^{m\oplus_i \kappa_i}_{W^R} \circ \mathcal{B}^m_{W^S Q}\left(\Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{0}}_{W^{\mathcal{A}} D^{\mathcal{A}}}(|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{A}}})\right) \\
&\otimes |\vec{0}\rangle\langle\vec{0}|_{O_{\text{in}}^{\mathcal{A}}} \otimes |0\rangle\langle 0|_{O_{\text{out}}} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T_{\text{in}}^{\mathcal{A}}} \otimes \frac{\mathbb{1}_T}{4} \\
&+ \sum_{\vec{\mu}\neq 0,\vec{\nu}} \mathbb{1}_{W^S W^R Q}\left(\Pi^{\vec{\nu}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}} D^{\mathcal{A}}}(|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}} W^{\mathcal{A}} W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{A}}})\right) \\
&\otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O_{\text{in}}^{\mathcal{A}}} \otimes |1\rangle\langle 1|_{O_{\text{out}}} \otimes |\perp\rangle\langle\perp|_{T_{\text{in}}^{\mathcal{A}}} \otimes |\perp\rangle\langle\perp|_T,
\end{aligned} \tag{A16}$$

where we made use of Lemma 3 and the explicitly wrote that the state of register T is maximally mixed.

In summary, Lemma 4 represents the state at the end of the protocol, given that the adversaries might have acted arbitrarily in Step 4 and under the assumption that, in particular, the classical protocols do not reveal the identities of the sender and the receiver. We will use this state to prove security in the following section.

3. Security analysis

a. Semiactive adversary

In this section we show that Protocol 1 is sender-secure. The key point of the proof is that security follows from permutational invariance of the state. Before proving Theorem 1, we first prove the following useful lemma.

Lemma 5. The reduced quantum state of the adversary at the end of the protocol is independent of the sender, i.e., $\forall i \notin \mathcal{A}$,

$$\rho_{W^{\mathcal{A}}C|S=i} = \rho_{W^{\mathcal{A}}C}. \tag{A17}$$

Proof. Let us first consider the case where the receiver is not an adversary, $R \notin \mathcal{A}$.

By tracing out we have that

$$\rho_{W^{\mathcal{A}}C|S=i} = \mathrm{Tr}_{W^{\mathcal{H}}W^{S}W^{R}Q}[\rho_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S}W^{R}QC|S=i}], \tag{A18}$$

where $\rho_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S}W^{R}QC|S=i}$ is the total state at the end of the protocol (A16), Lemma 4, given that i is the sender. Since $\mathcal{R}^{m\oplus_i\kappa_i}_{W^R}$ and $\sum_m \mathcal{B}^m_{W^SQ}$ are CPTP, they do not change the trace and thus we can write the first part of Eq. (A16) as

$$\begin{aligned}
&\mathrm{Tr}_{W^{\mathcal{H}}W^{S}W^{R}Q}\Bigg[\sum_{m,\vec{\kappa}} \mathcal{R}^{m\oplus_i\kappa_i}_{W^R} \circ \mathcal{B}^m_{W^SQ}\big(\Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{0}}_{W^{\mathcal{A}}D^{\mathcal{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S}W^{R}} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{A}}})\big) \\
&\quad \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathcal{A}}_{\mathrm{in}}} \otimes |0\rangle\langle 0|_{O_{\mathrm{out}}} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathcal{A}}_{\mathrm{in}}} \otimes \frac{\mathbb{1}_T}{4}\Bigg] \\
&= \mathrm{Tr}_{W^{\mathcal{H}}W^{S}W^{R}Q}\Bigg[\Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{0}}_{W^{\mathcal{A}}D^{\mathcal{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S}W^{R}} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{A}}}) \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathcal{A}}_{\mathrm{in}}} \otimes |0\rangle\langle 0|_{O_{\mathrm{out}}} \otimes \sum_{\vec{\kappa}} |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathcal{A}}_{\mathrm{in}}} \otimes \frac{\mathbb{1}_T}{4}\Bigg] \\
&= \mathrm{Tr}_{W^{\mathcal{H}}}\big[\Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{0}}_{W^{\mathcal{A}}D^{\mathcal{A}}}(\tilde{W}_{W^{\mathcal{H}}W^{\mathcal{A}}} \otimes \sigma_{D^{\mathcal{A}}})\big] \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathcal{A}}_{\mathrm{in}}} \otimes |0\rangle\langle 0|_{O_{\mathrm{out}}} \otimes \sum_{\vec{\kappa}} |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathcal{A}}_{\mathrm{in}}} \otimes \frac{\mathbb{1}_T}{4},
\end{aligned} \tag{A19}$$

where $\tilde{W}_{W^{\mathcal{H}}W^{\mathcal{A}}}$ is the reduced W state on registers $W^{\mathcal{H}}$ and $W^{\mathcal{A}}$ after tracing out W^S and W^R, i.e., $\tilde{W}_{W^{\mathcal{H}}W^{\mathcal{A}}} = \mathrm{Tr}_{W^SW^R}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^SW^R})$, and similarly for the second term of (A16). So,

$$\begin{aligned}
\rho_{W^{\mathcal{A}}C|S=i} =& \mathrm{Tr}_{W^{\mathcal{H}}}\big[\Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{0}}_{W^{\mathcal{A}}D^{\mathcal{A}}}(\tilde{W}_{W^{\mathcal{H}}W^{\mathcal{A}}} \otimes \sigma_{D^{\mathcal{A}}})\big] \otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathcal{A}}_{\mathrm{in}}} \otimes |0\rangle\langle 0|_{O_{\mathrm{out}}} \otimes \sum_{\vec{\kappa}} |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathcal{A}}_{\mathrm{in}}} \otimes \frac{\mathbb{1}_T}{4} \\
&+ \sum_{\vec{\mu}\neq 0,\vec{\nu}} \mathrm{Tr}_{W^{\mathcal{H}}}\big[\Pi^{\vec{\nu}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}}D^{\mathcal{A}}}(\tilde{W}_{W^{\mathcal{H}}W^{\mathcal{A}}} \otimes \sigma_{D^{\mathcal{A}}})\big] \otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathcal{A}}_{\mathrm{in}}} \otimes |1\rangle\langle 1|_{O_{\mathrm{out}}} \otimes |\perp\rangle\langle\perp|_{T^{\mathcal{A}}_{\mathrm{in}}} \otimes |\perp\rangle\langle\perp|_T.
\end{aligned} \tag{A20}$$

But since the state distributed by the source is permutationally invariant, it holds that

$$\tilde{W}_{W^{\mathcal{H}}W^{\mathcal{A}}} = \mathrm{Tr}_{W^{S=i}W^R}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S=i}W^R}) = \mathrm{Tr}_{W^{S=j}W^R}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S=j}W^R}), \quad \forall i, j \notin \mathcal{A}. \tag{A21}$$

Since no other part of the state $\rho_{W^{\mathcal{A}}C|S=i}$ depends on the sender, the state $\rho_{W^{\mathcal{A}}C|S=i}$ must be the same for all senders and we denote $\rho_{W^{\mathcal{A}}C|S=i} = \rho_{W^{\mathcal{A}}C}$. Note that the same statement holds when the receiver is honest, since

$$\mathrm{Tr}_{W^SW^{R=i}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^SW^{R=i}}) = \mathrm{Tr}_{W^SW^{R=j}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^SW^{R=j}}), \quad \forall i, j \notin \mathcal{A}, \tag{A22}$$

and therefore, $\rho_{W^{\mathcal{A}}C|R=i} = \rho_{W^{\mathcal{A}}C}$.

Now we proceed to the proof of this statement in the case where the receiver is an adversary.

If the receiver is dishonest then the teleportation map has to take into account the fact that the adversaries can apply an arbitrary map instead of $\mathcal{R}^{m\oplus_i\kappa_i}_{W^R}$. Also, now the output of the teleportation m is known to the adversaries and the map $\mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}}D^{\mathcal{A}}}$ could initially also act on the receiver's register. Now we can model the action of the receiver after receiving m by an arbitrary map that acts on all the registers in possession of the adversaries, i.e., $\mathcal{R}^{m\oplus_i\kappa_i}_{W^R} \to \mathcal{R}'_{W^{\mathcal{A}}W^RCT^{\mathcal{A}}_{\mathrm{in}}T}$ and instead of (A16), the final state of the protocol is described by

$$\begin{aligned}
\rho_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S}W^{R}QC|S=i} =& \mathcal{R}'_{W^{\mathcal{A}}W^RCT^{\mathcal{A}}_{\mathrm{in}}T} \circ \Bigg(\sum_{m,\vec{\kappa}} \mathcal{B}^m_{W^SQ}\big(\Pi^{\vec{0}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{0}}_{W^{\mathcal{A}}D^{\mathcal{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^SW^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{A}}})\big) \\
&\otimes |\vec{0}\rangle\langle\vec{0}|_{O^{\mathcal{A}}_{\mathrm{in}}} \otimes |0\rangle\langle 0|_{O_{\mathrm{out}}} \otimes |\vec{\kappa}\rangle\langle\vec{\kappa}|_{T^{\mathcal{A}}_{\mathrm{in}}} \otimes |m\rangle\langle m|_T\Bigg) \\
&+ \sum_{\vec{\mu}\neq 0,\vec{\nu}} \mathbb{1}_{W^SW^RQ} \circ \big(\Pi^{\vec{\nu}}_{W^{\mathcal{H}}} \otimes \mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}}D^{\mathcal{A}}}(|\mathrm{W}\rangle\langle\mathrm{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^SW^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{A}}})\big) \\
&\otimes |\vec{\mu}\rangle\langle\vec{\mu}|_{O^{\mathcal{A}}_{\mathrm{in}}} \otimes |1\rangle\langle 1|_{O_{\mathrm{out}}} \otimes |\perp\rangle\langle\perp|_{T^{\mathcal{A}}_{\mathrm{in}}} \otimes |\perp\rangle\langle\perp|_T.
\end{aligned} \tag{A23}$$

Let us look at the reduced final state of the adversary, which now includes the receiver, $\rho_{W^{\mathcal{A}}W^{R}C|S=i} = \mathrm{Tr}_{W^{\mathcal{H}}W^{S}Q}[\rho_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S}W^{R}QC|S=i}]$. By the permutational invariance of the state generated by the source we have that the state at the end of the protocol given that node i is the sender is equivalent to the state given that node j is the sender up to a permutation of i and j,

$$\rho_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S}W^{R}QC|S=i} = \mathcal{P}_{i\leftrightarrow j}(\rho_{W^{\mathcal{H}}W^{\mathcal{A}}W^{S}W^{R}QC|S=j}). \tag{A24}$$

Therefore after tracing out the sender and the other honest parties, the remaining states are equal,

$$\rho_{W^{\mathcal{A}}W^{R}C|S=i} = \rho_{W^{\mathcal{A}}W^{R}C|S=j}, \tag{A25}$$

which proves anonymity of the sender even if the receiver is dishonest. ■

Proof of Theorem 1 (sender security). Here we focus on proving sender security. The receiver security is formally stated in Theorem 10. Given Lemma 5, we have that

$$P_{\mathrm{guess}}[S|W^{\mathcal{A}}, C, S\notin\mathcal{A}] = \max_{\{M^i\}}\sum_{i\in[N]} P[S=i|S\notin\mathcal{A}]\mathrm{Tr}[M^i\rho_{W^{\mathcal{A}}C|S=i}] \tag{A26}$$

$$= \max_{\{M^i\}}\sum_{i\in[N]} P[S=i|S\notin\mathcal{A}]\mathrm{Tr}[M^i\rho_{W^{\mathcal{A}}C}] \tag{A27}$$

$$\leqslant \max_i P[S=i|S\notin\mathcal{A}]\max_{\{M^i\}}\mathrm{Tr}\left[\underbrace{\sum_{i\in[N]} M^i}_{\mathbb{1}_{W^{\mathcal{A}}C}}\rho_{W^{\mathcal{A}}C}\right] \tag{A28}$$

$$= \max_i P[S=i|S\notin\mathcal{A}]. \tag{A29}$$

■

Analogously, we will prove the following statement for the receiver security.

Theorem 10 (receiver security). The anonymous transmission protocol with the W state, Protocol 1, is receiver-secure in the semiactive adversary scenario, i.e.,

$$\max_{\{M^i\}}\sum_{i\in[N]} P[R=i|W^{\mathcal{A}}, C, R\notin\mathcal{A}]\mathrm{Tr}[M^i\rho_{W^{\mathcal{A}}C|R=i}] \leqslant \max_i P[R=i|R\notin\mathcal{A}], \tag{A30}$$

given that the receiver is honest.

Proof. By the proof of Lemma 5, it follows that the reduced quantum state of the adversary at the end of the protocol is independent of the receiver, i.e., $\rho_{W^{\mathcal{A}}C|R=i} = \rho_{W^{\mathcal{A}}C}, \forall i\notin\mathcal{A}$. Therefore,

$$P_{\mathrm{guess}}[R|W^{\mathcal{A}}, C, R\notin\mathcal{A}] = \max_{\{M^i\}}\sum_{i\in[N]} P[R=i|R\notin\mathcal{A}]\mathrm{Tr}[M^i\rho_{W^{\mathcal{A}}C|R=i}] \tag{A31}$$

$$\leqslant \max_i P[R=i|R\notin\mathcal{A}]\max_{\{M^i\}}\mathrm{Tr}\left[\underbrace{\sum_{i\in[N]} M^i}_{\mathbb{1}_{W^{\mathcal{A}}C}}\rho_{W^{\mathcal{A}}C}\right] \tag{A32}$$

$$= \max_i P[R=i|R\notin\mathcal{A}]. \tag{A33}$$

■

b. Passive adversary

Definition 7. Let $\mathcal{H}$ be the subset of honest players, excluding S and R, and $\mathcal{A}$ be the subset of passive adversaries. Let C be the register that contains all classical information accessible to the adversaries, i.e., the public outputs of the classical subprotocols, plus all the inputs and outputs of the adversaries to these classical subprotocols, $C = \{D^{\mathcal{A}}, O_{\mathrm{in}}^{\mathcal{A}}, O_{\mathrm{out}}, T_{\mathrm{in}}^{\mathcal{A}}, T\}$. Then probability of the adversaries guessing the sender is given by

$$P_{\mathrm{guess}}[S|W^{\mathcal{A}}, C, S\notin\mathcal{A}] = \sum_{a,c} P[W^{\mathcal{A}}=a, C=c]\max_{i\in[N]} P[S=i|W^{\mathcal{A}}=a, C=c, S\notin\mathcal{A}], \tag{A34}$$

where maximization is taken over all the values of random variable S, and a and c are possible values of random variables $W^{\mathcal{A}}$ and C, respectively. Note that unlike before, here $W^{\mathcal{A}}$ is a classical register of the adversary, since their share of the W state was measured in the $\{0, 1\}$ basis. An analogous expression holds for receiver security.

The proof for the passive adversary security scenario is a special case of the proof for the semiactive adversary scenario. Indeed, it corresponds to the case where the arbitrary map of the adversary, $\mathcal{F}^{\vec{\mu}}_{W^{\mathcal{A}}D^{\mathcal{A}}}$, is a measurement in the $\{|0\rangle, |1\rangle\}$ basis and $T^{\mathcal{A}}_{\text{in}} = \vec{0}$. Let us first prove the following lemma.

Lemma 6. The probability of registers $W^{\mathcal{A}}$ and C assuming certain values a and c is independent of the sender,

$$P[W^{\mathcal{A}} = a, C = c | S = i, S \notin \mathcal{A}] = P[W^{\mathcal{A}} = a, C = c]. \tag{A35}$$

Proof. In the passive adversary scenario, the dishonest parties follow the protocol; therefore the map $\mathcal{F}^{\vec{0}}_{W^{\mathcal{A}}D^{\mathcal{A}}}$ is replaced by a projector onto the $|\vec{0}\rangle\langle\vec{0}|_{W^{\mathcal{A}}}$ subspace, i.e., $\Pi^{\vec{0}}_{W^{\mathcal{A}}}$. By the permutational invariance argument the state, in this case classical, is independent of the sender S (or the receiver R), which completes the proof. ■

Proof of Theorem 2. Let us expand the probability appearing in the security definition (A34),

$$P[S = i | W^{\mathcal{A}} = a, C = c, S \notin \mathcal{A}] = \frac{P[W^{\mathcal{A}} = a, C = c | S = i, S \notin \mathcal{A}] P[S = i | S \notin \mathcal{A}]}{P[W^{\mathcal{A}} = a, C = c]} \tag{A36}$$

$$= \frac{P[W^{\mathcal{A}} = a, C = c | S = i] P[S = i | S \notin \mathcal{A}]}{P[W^{\mathcal{A}} = a, C = c]} \tag{A37}$$

$$= P[S = i | S \notin \mathcal{A}], \tag{A38}$$

where in Eq. (A37) we used Lemma 6. Therefore, (A34) becomes

$$P_{\text{guess}}[S | W^{\mathcal{A}}, C, S \notin \mathcal{A}] = \sum_{a,c} P[W^{\mathcal{A}} = a, C = c] \max_{i \in [N]} P[S = i | S \notin \mathcal{A}] \tag{A39}$$

$$= \max_{i \in [N]} P[S = i | S \notin \mathcal{A}]. \tag{A40}$$

■

APPENDIX B: ANONYMOUS TRANSMISSION IN A NOISY QUANTUM NETWORK

1. Proof for ε security

Here we provide a proof of Theorem 4 for ε-sender security.

Proof of Theorem 4. The idea of our proof is to show that, for all i, the trace $\text{Tr}[M^i \hat{\rho}^{\Lambda}_{W^{\mathcal{A}}C|S=i}]$ can be upper-bounded by $\text{Tr}[M^i \rho^{\Lambda}_{W^{\mathcal{A}}C|S=i}] + N\varepsilon_{\max}$. Then using the fact that $N\varepsilon_{\max}$ is independent of i, the rest of the proof follows from Theorem 3. Let us look at the following expression, $\forall i$,

$$\begin{aligned} &\left|\text{Tr}\left[M^i \hat{\rho}^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right] - \text{Tr}\left[M^i \rho^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right]\right| \\ &\leqslant \left\| \hat{\rho}^{\Lambda}_{W^{\mathcal{A}}C|S=i} - \rho^{\Lambda}_{W^{\mathcal{A}}C|S=i} \right\|_1 \\ &\leqslant \left\| \xi'^{\Lambda\ (6)}_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R Q D^{\mathcal{H}\mathcal{A}SR} O^{\mathcal{H}}_{\text{in}} O^{\mathcal{A}}_{\text{in}} O_{\text{out}} T^S_{\text{in}} T^R_{\text{in}} T^{\mathcal{A}}_{\text{in}} T|S=i} - \xi^{\Lambda\ (6)}_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R Q D^{\mathcal{H}\mathcal{A}SR} O^{\mathcal{H}}_{\text{in}} O^{\mathcal{A}}_{\text{in}} O_{\text{out}} T^S_{\text{in}} T^R_{\text{in}} T^{\mathcal{A}}_{\text{in}} T|S=i} \right\|_1, \end{aligned} \tag{B1}$$

where $\xi'^{\Lambda\ (6)}_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R Q D^{\mathcal{H}\mathcal{A}SR} O^{\mathcal{H}}_{\text{in}} O^{\mathcal{A}}_{\text{in}} O_{\text{out}} T^S_{\text{in}} T^R_{\text{in}} T^{\mathcal{A}}_{\text{in}} T|S=i}$ and $\xi^{\Lambda\ (6)}_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R Q D^{\mathcal{H}\mathcal{A}SR} O^{\mathcal{H}}_{\text{in}} O^{\mathcal{A}}_{\text{in}} O_{\text{out}} T^S_{\text{in}} T^R_{\text{in}} T^{\mathcal{A}}_{\text{in}} T|S=i}$ are final states of the protocol after Step 6 [defined analogously to Eq. (A15)] when the network is perturbed (5), or not (3), respectively. Since the protocol is described by a CPTP map, the trace distance of the final state is upper-bounded by the trace distance of the initial state,

$$\left|\text{Tr}\left[M^i \hat{\rho}^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right] - \text{Tr}\left[M^i \rho^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right]\right| \leqslant \left\| \omega'^{\Lambda}_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{H}\mathcal{A}SR}|S=i} - \omega^{\Lambda}_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R} \otimes |\psi\rangle\langle\psi|_Q \otimes \sigma_{D^{\mathcal{H}\mathcal{A}SR}|S=i} \right\|_1 \tag{B2}$$

$$\leqslant \left\| \omega'^{\Lambda}_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R} - \omega^{\Lambda}_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R} \right\|_1 \tag{B3}$$

$$\leqslant \left\| \bigotimes_{i=1}^{N} \Lambda_i(|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R}) - \Lambda^{\otimes N}(|\text{W}\rangle\langle\text{W}|_{W^{\mathcal{H}}W^{\mathcal{A}}W^S W^R}) \right\|_1 \tag{B4}$$

$$\leqslant \left\| \bigotimes_{i=1}^{N} \Lambda_i - \Lambda^{\otimes N} \right\|_1 \leqslant \sum_{i=1}^{N} \|\Lambda_i - \Lambda\|_1 = \sum_{i=1}^{N} \varepsilon_i \leqslant N\varepsilon_{\max}, \tag{B5}$$

where we used the properties of the trace distance and the induced trace norm. Therefore we have that, $\forall i$,

$$\text{Tr}\left[M^i \hat{\rho}^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right] \leqslant \text{Tr}\left[M^i \rho^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right] + N\varepsilon_{\max}, \tag{B6}$$

so using Theorem 3,

$$P_{\text{guess}}[S | W^{\mathcal{A}}, C, S \notin \mathcal{A}] = \max_{\{M^i\}} \sum_{i \in [N]} P[S = i | S \notin \mathcal{A}] \text{Tr}\left[M^i \hat{\rho}^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right] \tag{B7}$$

$$\leqslant \max_{\{M^i\}} \sum_{i\in[N]} P[S=i|S\notin\mathcal{A}]\left(\mathrm{Tr}\left[M^i \rho^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right] + N\varepsilon_{\max}\right) \tag{B8}$$

$$= \max_{\{M^i\}} \sum_{i\in[N]} P[S=i|S\notin\mathcal{A}]\mathrm{Tr}\left[M^i \rho^{\Lambda}_{W^{\mathcal{A}}C|S=i}\right] + \sum_{i\in[N]} P[S=i|S\notin\mathcal{A}]N\varepsilon_{\max} \tag{B9}$$

$$\leqslant \max_{i\in[N]} P[S=i|S\notin\mathcal{A}] + N\varepsilon_{\max}. \tag{B10}$$

■

The same argument holds for receiver security.

2. Performance in a noisy network

Fidelity derivation. In general, it is nontrivial to derive analytical expressions for fidelity of anonymous entanglement in the presence of noise. The most troublesome part is to obtain analytical expressions for anonymous entangled states shared between S and R, which are affected by the noise. Nevertheless, to obtain these explicit formulas, we used the fact that the noise is described by a linear map which acts on each qubit individually. We will illustrate the gist of our derivation with an example for the GHZ state, since it is easier to follow than the one for the W state.

As defined in the main text, the state shared by S and R in the noisy case is

$$\gamma_{SR} = \frac{1}{\mathcal{N}'}\mathrm{Tr}_{N-2}[\Lambda^{\otimes N}(|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_N)|\vec{+}\rangle\langle\vec{+}|_{N-2}], \tag{B11}$$

where $\mathcal{N}$ is the normalization factor. Note that the GHZ state can be written as

$$|\mathrm{GHZ}\rangle\langle\mathrm{GHZ}|_N = \tfrac{1}{2}(|0\rangle\langle 0|^{\otimes N} + |0\rangle\langle 1|^{\otimes N} + |1\rangle\langle 0|^{\otimes N} + |1\rangle\langle 1|^{\otimes N}). \tag{B12}$$

Due to the tensor structure and linearity of the noise, we can write that

$$\begin{aligned}\gamma_{SR} &= \frac{1}{2\mathcal{N}'}\mathrm{Tr}_{N-2}\{[\Lambda(|0\rangle\langle 0|)^{\otimes N} + \Lambda(|0\rangle\langle 1|)^{\otimes N} + \Lambda(|1\rangle\langle 0|)^{\otimes N} + \Lambda(|1\rangle\langle 1|)^{\otimes N}]|+\rangle\langle+|^{\otimes N-2}\}\\ &= \frac{1}{2\mathcal{N}'}\{\mathrm{Tr}[\Lambda(|0\rangle\langle 0|)]^{N-2}\Lambda(|0\rangle\langle 0|)^{\otimes 2} + \mathrm{Tr}[\Lambda(|0\rangle\langle 1|)]^{N-2}\Lambda(|0\rangle\langle 1|)^{\otimes 2}\\ &\quad + \mathrm{Tr}[\Lambda(|1\rangle\langle 0|)]^{N-2}\Lambda(|1\rangle\langle 0|)^{\otimes 2} + \mathrm{Tr}[\Lambda(|1\rangle\langle 1|)]^{N-2}\Lambda(|1\rangle\langle 1|)^{\otimes 2}\}.\end{aligned} \tag{B13}$$

This way one only takes the tensor product of the two terms corresponding to S and R, instead of taking the tensor of N terms. The expression for the W state follows the exact same pattern, but one has to account for all the combinations of 0's and 1's occurring in the state $|\mathrm{W}\rangle\langle\mathrm{W}|_N$. Let $\mathrm{tr}_{xy} := \mathrm{Tr}[\Lambda(|x\rangle\langle y|)|0\rangle\langle 0|]$ with $x, y = \{0, 1\}$. Then the state ω_{SR} shared between S and R in the noisy implementation of Protocol 1 is

$$\begin{aligned}\omega_{SR} = \frac{1}{\mathcal{N}}\big\{&(N-2)(N-3)\mathrm{tr}_{01}\mathrm{tr}_{10}\mathrm{tr}_{00}^{N-4}\Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|)\\ &+ (N-2)\mathrm{tr}_{10}\mathrm{tr}_{00}^{N-3}[\Lambda(|0\rangle\langle 1|)\otimes\Lambda(|0\rangle\langle 0|) + \Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 1|)]\\ &+ (N-2)\mathrm{tr}_{01}\mathrm{tr}_{00}^{N-3}[\Lambda(|1\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|) + \Lambda(|0\rangle\langle 0|)\otimes\Lambda(|1\rangle\langle 0|)] + (N-2)\mathrm{tr}_{11}\mathrm{tr}_{00}^{N-3}\Lambda(|0\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 0|)\\ &+ \mathrm{tr}_{00}^{N-2}\big(\Lambda(|0\rangle\langle 1|)\otimes\Lambda(|1\rangle\langle 0|) + \Lambda(|1\rangle\langle 0|)\otimes\Lambda(|0\rangle\langle 1|) + \Lambda(|0\rangle\langle 0|)\otimes\Lambda(|1\rangle\langle 1|) + \Lambda(|1\rangle\langle 1|)\otimes\Lambda(|0\rangle\langle 0|)\big)\big\}.\end{aligned} \tag{B14}$$

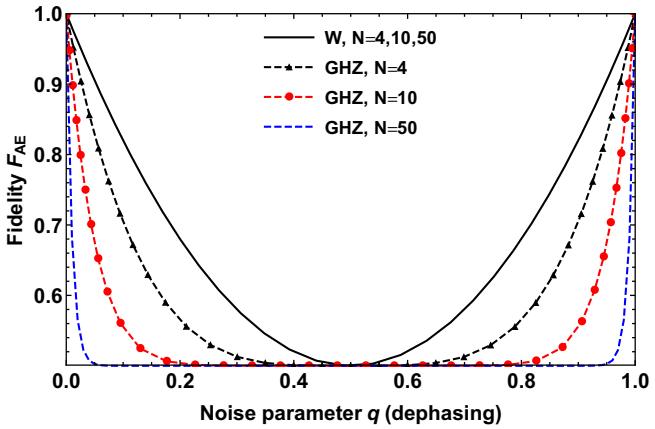


FIG. 5. Fidelity of anonymous entanglement as a function of the noise parameter for the dephasing channel.

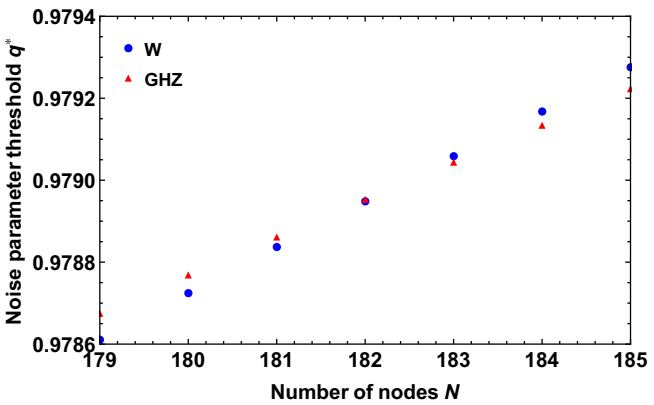


FIG. 6. Noise parameter threshold for the depolarizing noise. Close-up to $179 \leqslant N \leqslant 185$.

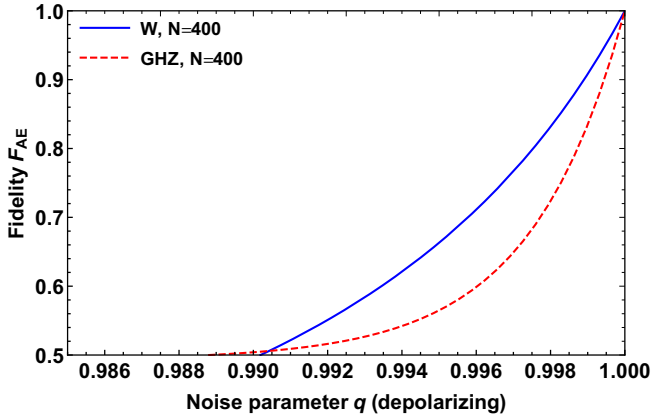


FIG. 7. Fidelity of anonymous entanglement for $N = 400$.

Using the explicit form of Λ for the depolarizing and dephasing noise, after easy but tedious calculations, one obtains explicit fidelity expressions derived from Eqs. (12) and (13).

Dephasing and depolarizing noise. In this section we provide additional details to the noise analysis provided in the main text. First, we plot the behavior of our protocol vs the GHZ-based protocol under the dephasing noise, for example, $N = \{4, 10, 50\}$, Fig. 5. Note that the GHZ state is increasingly useful according to Definition 6 for $q < 0.5$. For anonymous entanglement created with the W state this is always the case, however, for the GHZ—only for even N. To observe the same behavior for odd N and the GHZ state one would have to redefine Eq. (13) to compare the fidelity with the state $|\phi^-\rangle\langle\phi^-|$.

As discussed, the noise parameter threshold q^* for $N = 182$ nodes becomes larger for the W state: $q^*_W = 0.979057$, $q^*_{\mathrm{GHZ}} = 0.979043$, $q^*_W > q^*_{\mathrm{GHZ}}$. This means that for $N \geqslant 182$ the W state tolerates less noise than the GHZ; see Fig. 6. However, we numerically see that there exists a value of $q > q^*_W$ for which $F_{AE}(\omega_{SR}) > F_{AE}(\gamma_{SR})$. As an example for $N = 400$ see Fig. 7.

Moreover, we provide an analytical expression for the probability of success in our protocol, defined as $P_{\omega_{SR}} := \mathrm{Tr}[\Lambda^{\otimes N}(|\mathrm{W}\rangle\langle\mathrm{W}|_N)|\vec{0}\rangle\langle\vec{0}|_{N-2}]$, which for the depolarizing

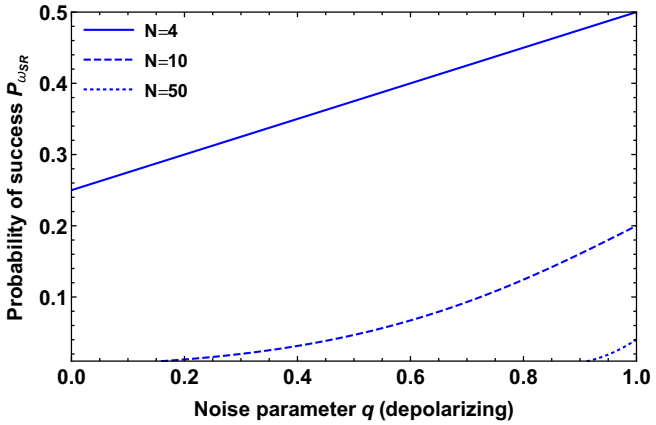


FIG. 8. Probability of success in Protocol 1 in the presence of the depolarizing noise, $N = \{4, 10, 50\}$.

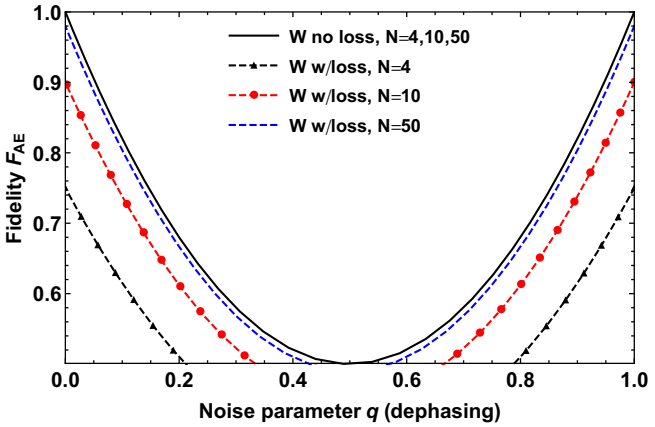
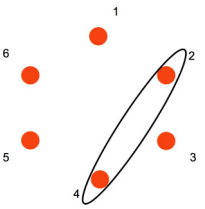
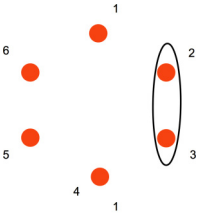
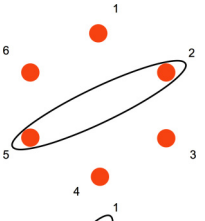
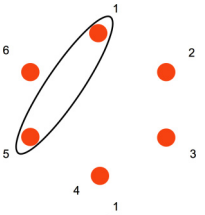
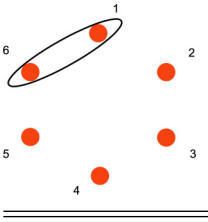


FIG. 9. Fidelity of anonymous entanglement for Protocol 1, as a function of the noise parameter for the dephasing channel in the presence of one particle loss.

TABLE II. Fidelity of anonymous entanglement for the relay scheme [7] in the N-fold noisy network for the depolarizing channel. Note that for the depolarizing parameter $q = 0.8$ the anonymous entanglement created between nodes 1 and 6 is not useful in the sense of Definition 6.

Scenario	F_{AE} for $q = 0.8$	F_{AE} for $q = 0.95$
	0.5738	0.8625
	0.6138	0.8744
	0.5418	0.8512
	0.5162	0.8405
	0.4958	0.8303

noise assumes the form

$$P_{\omega_{SR}} = \frac{(q+1)^{N-3}[N(1-q)+4q]}{N2^{N-2}}. \tag{B15}$$

Examples of $P_{\omega_{SR}}$ as a function of q for $N = \{4, 10, 50\}$ are plotted in Fig. 8. Note that for the dephasing noise $P_{\omega_{SR}} = \frac{2}{N}$, since the measurement basis is not affected by the Z noise.

Particle loss. In the case when one of the particles of the W state is lost and the state is subjected to the network noise, the fidelity of anonymous entanglement can be expressed as

$$F_{AE}(\tilde{\omega}_{SR}) = \frac{(1+q)[N^2(q-1)^2 - 8q^2 + 4Nq(1+q)]}{4N[N(1-q)+4q]} \tag{B16}$$

for the depolarizing noise, and

$$F_{AE}(\tilde{\omega}_{SR}) = \frac{N-1}{N}[1-2q(1-q)] \tag{B17}$$

for the dephasing noise. In Fig. 9 we plot the examples of F_{AE} for $N = \{4, 10, 50\}$ when the initial W state is subjected to one particle loss and the dephasing noise.

Relay protocol. Finally, in Table II we present the values for anonymous entanglement in the relay protocol [7] in the presence of the depolarizing noise.

[1] F. Stajano and R. Anderson, in *Information Hiding*, edited by A. Pfitzmann (Springer, Berlin, 2000), pp. 434–447.

[2] D. Chaum, Commun. ACM **24**, 84 (1981).

[3] D. Chaum, J. Cryptology **1**, 65 (1988).

[4] M. Christandl and S. Wehner, in *Advances in Cryptology: ASIACRYPT 2005*, edited by B. Roy (Springer, Berlin, 2005), pp. 217–235.

[5] J. Bouda and J. Sprojcar, in *Quantum, Nano, and Micro Technologies, 2007: ICQNM '07, First International Conference on* (IEEE, Piscataway, 2007), p. 12.

[6] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, in *Advances in Cryptology: ASIACRYPT 2007*, edited by K. Kurosawa (Springer, Berlin, 2007), pp. 460–473.

[7] W. Yang, L. Huang, and F. Song, Sci. Rep. **6**, 26762 (2016).

[8] A. Acín *et al.*, New J. Phys. **20**, 080201 (2018).

[9] A. Broadbent and A. Tapp, in *Advances in Cryptology: ASIACRYPT 2007*, edited by K. Kurosawa (Springer, Berlin, 2007), pp. 410–426.

[10] N. Kalb, Ph.D. thesis, TU Delft, 2018.

[11] M. Tomamichel, Ph.D. thesis, ETH Zürich, 2012.

[12] J. Watrous, *The Theory of Quantum Information* (Cambridge University Press, Cambridge, 2018).

[13] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Rev. A **60**, 1888 (1999).

[14] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[15] M. Koashi, V. Bužek, and N. Imoto, Phys. Rev. A **62**, 050302 (2000).

[16] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, Phys. Rev. Lett. **108**, 260502 (2012).

[17] I. Šupić, A. Coladangelo, R. Augusiak, and A. Acín, New J. Phys. **20**, 083041 (2018).

[18] M. Fadel, arXiv:1707.01215.