Anonymous Quantum Conference Key Agreement

Frederik Hahn,[1,*] Jarn de Jong,[2] and Anna Pappa[2]

[1] *Dahlem Center for Complex Quantum Systems, Freie Universität Berlin, Berlin 14195, Germany*
[2] *Electrical Engineering and Computer Science Department, Technische Universität Berlin, Berlin 10587, Germany*

(Received 9 October 2020; accepted 24 November 2020; published 22 December 2020)

Conference key agreement (CKA) is a cryptographic effort of multiple parties to establish a shared secret key. In future quantum networks, generating secret keys in an anonymous way is of tremendous importance for parties that want to keep their shared key secret and at the same time protect their own identity. We provide a definition of anonymity for general protocols and present a CKA protocol that is provably anonymous under realistic adversarial scenarios. We base our protocol on shared Greenberger-Horne-Zeilinger states, which have been proposed as more efficient resources for CKA protocols, compared to bipartite entangled resources. The existence of secure and anonymous protocols based on multipartite entangled states provides a new insight on their potential as resources and paves the way for further applications.

DOI: 10.1103/PRXQuantum.1.020325

I. INTRODUCTION

One of the main applications of quantum-information processing is to provide additional security for communication. The most common setting is one of two parties, Alice and Bob, who want to establish a shared secret key in order to encrypt further communication. Since their introduction [1], quantum-key-distribution (QKD) protocols have been proposed and implemented in a standard fashion, although several practical challenges remain to be addressed [2]. Here, we examine a more generalized scenario, where several parties want to establish a shared secret key. In this multiparty setting we introduce a new notion of *anonymity*, where we request that the identities of the parties sharing the secret key are all protected. Such scenarios are highly relevant for several reasons. One example is the case of whistleblowing; a person might want to broadcast an encrypted message such that specific parties can decrypt it, while keeping the identities of all involved parties secret. For such anonymous whistleblowing, the underlying protocol needs to involve nonparticipating parties, such that an authority maintaining the network cannot uncover who takes part in the secret communication. To the best of our knowledge, this is the first multipartite protocol that provides anonymity for a sender and multiple receivers alike.

To succeed in attaining this goal, we need to address two different elements, *anonymity* and *multiparty key generation*. For a concise review of the latter, often referred to as conference key agreement (CKA), we refer the interested reader to Ref. [3]. Combining the two elements, we achieve *anonymous conference key agreement*, which allows a sender to transmit a private message to specific receivers of her choice, while keeping their identities secret from external parties and even from each other.

Previous work [4] has shown how to achieve anonymous transmission of classical bits using the correlations natural to the GHZ state [5] and how to anonymously create bipartite entanglement from a larger GHZ state. In Ref. [6] the latter is developed further, by adding a scheme for anonymous notification of the receiver and for verification [7,8] of the anonymous entanglement generation. However, since extracting multiple bipartite Bell states from a single GHZ state is impossible, we need an alternative approach that enables us to perform anonymous CKA between a subset of a given network. One approach could be to use other multipartite entangled quantum states [9–11] to create bipartite entanglement between the sender and all receivers separately; however, that would increase the use of quantum resources. We show that it is in fact possible to anonymously establish the necessary entanglement between sender and receivers simultaneously, using a single GHZ state shared by a source through the network.

In this paper, we introduce a protocol to establish a secret key between the sender "Alice" and m receiving

[*] frederik.hahn@fu-berlin.de

parties of her choice. We use both “Bob” and “receiver” to refer to each of those receiving parties and “participants” to refer to Alice and all Bobs. The $m+1 \leq n$ participants are part of a larger network of n parties. The m Bobs are notified anonymously by Alice through a notification protocol. A large GHZ state $(1/\sqrt{2})\left(|0\rangle^n + |1\rangle^n\right)$ is then shared between the n parties, which can either be done centrally or using a given network infrastructure via quantum repeaters or quantum network coding [12]. From this GHZ$_n$ state, we subsequently show how to anonymously extract a GHZ$_{m+1}$ state shared only between the participants. The resulting state can be either verified or used to run the CKA protocol. Both the participants’ identities and their shared key are hidden from an attacker “Eve” in our protocols. We either assume Eve to follow the protocol and control a single node in the network, or to diverge from the protocol and control multiple nonparticipating nodes.

II. PRELIMINARIES

We label with $\mathbf{N}$ the set of all $n := |\mathbf{N}|$ parties in the network and with $\mathbf{P} := \{A, B_1, \ldots, B_m\}$ the set of the protocol’s participants, where A refers to Alice and $\{B_i\}$ to the m Bobs chosen by her.

Let Eve be an attacker whose goal it is to learn $\mathbf{P}$. If Eve corrupts some parties, she trivially learns their role in the protocol, i.e., whether or not they belong to $\mathbf{P}$. By $\mathcal{I}_{\text{Eve}}$ we denote this information as well as any prior information on $\{\Pr(\mathbf{G} = \mathbf{P})\}_{\mathbf{G}\subset\mathbf{N}}$, i.e., the probability distribution that a subset $\mathbf{G}$ of the parties is equal to $\mathbf{P}$. Denoting with $\mathcal{I}^+_{\text{Eve}}$ the *additional* information that becomes available to Eve during the protocol, we can define *anonymity* by demanding that running the protocol increases Eve’s knowledge only in a trivial way.

Definition 1 (Anonymity)**.** *A protocol is anonymous from the perspective of Eve if for all subsets* $\mathbf{G} \subset \mathbf{N}$

$$\Pr\left(\mathbf{G} = \mathbf{P} \mid \mathcal{I}^+_{\text{Eve}}, \mathcal{I}_{\text{Eve}}\right) = \Pr(\mathbf{G} = \mathbf{P} \mid \mathcal{I}_{\text{Eve}}), \qquad (1)$$

where $\mathcal{I}^+_{\text{Eve}}$ *is the information that becomes available to Eve during the protocol and* $\mathcal{I}_{\text{Eve}}$ *is both the information that Eve has beforehand and trivial information that she obtains about the parties that she corrupts.*

Here, by trivial information we mean the information that is available to each party regarding their role in the protocol, i.e., whether they belong in $\mathbf{P}$ or not. In the context of key agreement, we can assume that the participants are not corrupted by a fully malicious Eve, since this would jeopardize the whole key. We therefore assume that they are *honest but curious*, i.e., that they obey the protocol in order to establish a key, but may otherwise be interested in learning other participants’ identities. For the nonparticipating parties we consider the same honest-but-curious model, as well as a fully dishonest one. Hence, $\mathbf{N}$ can be partitioned into the three disjoint sets of the following:

P: honest-but-curious participating parties;
H: honest-but-curious nonparticipating parties;
C: dishonest and colluding nonparticipating parties.

We either assume Eve to follow the protocol and control a single party in $\mathbf{P}$ or $\mathbf{H}$, or to diverge from the protocol and control $\mathbf{C}$. Note however that our definition of anonymity is applicable to other corruption models and therefore applies more generally to any cryptographic protocol.

As previously mentioned, our CKA protocol exploits the correlations of a shared GHZ state to generate the conference key. Since the parties in $\mathbf{C}$ could apply an arbitrary quantum map to their system, this would result in a state ϵ close to $\rho_{\mathbf{N}} := |\mathbf{N}\rangle\langle\mathbf{N}|$, with $|\mathbf{N}\rangle$ equal to

$$\frac{1}{\sqrt{2}}\left(|0\ldots0\rangle_{\mathbf{P}\cup\mathbf{H}} \otimes |\Psi\rangle_{\mathbf{C}} + |1\ldots1\rangle_{\mathbf{P}\cup\mathbf{H}} \otimes |\Phi\rangle_{\mathbf{C}}\right). \qquad (2)$$

Here, the two states on $\mathbf{C}$ need not be orthogonal. They neither need to be pure, but since mixed states do not offer an advantage to Eve we may assume they are. For a discussion on untrusted or faulty sources we refer to Sec. V.

With the above definitions, we are now ready to introduce the subprotocols of the anonymous conference key agreement protocol. All protocols we propose are anonymous according to Definition 1. See the appendix for detailed proofs.

III. GENERATING ANONYMOUS MULTIPARTY ENTANGLEMENT

We start by presenting two subprotocols, `Notification` (protocol 1) and `Anonymous Multiparty Entanglement` (`AME`, protocol 2). Our version of `Notification` is based on Ref. [13] and is a classical protocol used by Alice to notify the m receiving agents, while maintaining anonymity for all parties involved. The protocol requires pairwise private classical communication—which can be established using a key-generation protocol with a Bell pair—and access to private sources of randomness. See the appendix for an illustration of protocol 1.

Analysis: Anonymity is maintained following the work of Ref. [13]. Remember that by the nature of our goal, the identities of the Bobs are available to Alice since she has chosen them. The `Notification` protocol requires $\mathcal{O}(n^3)$ communication channel uses between pairs of parties. Note that the `Notification` protocol is allowing Alice to anonymously transmit the same bit to all receivers to establish a common key. Such a process would however be extremely inefficient; if one Bell pair is required for each private classical communication round, then for each bit of generated key, $\mathcal{O}(n^3)$ Bell pairs would be consumed.

If instead we use `Notification` only once to notify the receivers, we can exploit the properties of the shared multipartite entanglement to establish a common key more efficiently while maintaining the anonymity that protocol 1 provides.

Protocol 1 `Notification`

Input. Alice's choice of m receivers.
Goal. The m receivers get notified.

For agent $i = 1, \dots, n$:

1. All agents $j \in \{1, \dots, n\}$ do the following.
   (a) When j corresponds to Alice (j_a), and i is not a receiver, she chooses n random bits $\{r^i_{j,k}\}_{k=1}^n$ such that $\bigoplus_{k=1}^n r^i_{j,k} = 0$. If i is a receiver, she chooses n random bits such that $\bigoplus_{k=1}^n r^i_{j,k} = 1$. She sends bit $r^i_{j,k}$ to agent k.
   (b) When $j \neq j_a$, the agent chooses n random bits $\{r^i_{j,k}\}_{k=1}^n$ such that $\bigoplus_{k=1}^n r^i_{j,k} = 0$ and sends bit $r^i_{j,k}$ to agent k.
2. All agents $k \in \{1, \dots, n\}$ receive $\{r^i_{j,k}\}_{j=1}^n$, compute $z^i_k = \bigoplus_{j=1}^n r^i_{j,k}$ and send it to agent i.
3. Agent i takes the received $\{z^i_k\}_{k=1}^n$ to compute $z^i = \bigoplus_{k=1}^n z^i_k$; if $z^i = 1$ they are thereby notified to be a designated receiver.

We now introduce the second subprotocol `AME`, visualized in Fig. 1. As a generalization of the protocol first proposed in Ref. [4] for anonymously distributing Bell states, it is a protocol for anonymously establishing GHZ states. Here, n parties are sharing a GHZ state, and $m + 1$ of them (Alice and m receivers) want to anonymously end up with a smaller, $(m + 1)$-partite GHZ state. To achieve this, all parties require access to a broadcast channel—a necessary requirement to achieve any type of anonymity for participants in a communication setting [14].

Protocol 2 `Anonymous Multiparty Entanglement`

Input. A shared GHZ$_n$ state; Alice knowing the identities of the non-participants $\bar{\mathbf{P}}$.
Goal. A GHZ$_{m+1}$ state shared between $\mathbf{P}$.

1. Alice and the Bobs each draw a random bit. Everyone else measures in the X-basis, yielding a measurement outcome bit x_i for $i \in \bar{\mathbf{P}}$.
2. All parties broadcast their bits in a random order or, if possible, simultaneously.
3. Alice applies a Z gate if the parity of the non-participating parties' bits is odd.

Analysis: The correctness of the protocol follows from the proof in Ref. [4]. With the Hadamard matrix H we can rewrite the GHZ$_n$ state as proportional to

$$\sum_{x \in \{0,1\}^{|\bar{\mathbf{P}}|}} \left[|0 \dots 0\rangle_{\mathbf{P}} + (-1)^{\Delta(x)} |1 \dots 1\rangle_{\mathbf{P}} \right] \otimes H_{\bar{\mathbf{P}}} |x\rangle_{\bar{\mathbf{P}}} ,$$

where $\Delta(x)$ is the Hamming weight of x and the subscripts $\mathbf{P}$ and $\bar{\mathbf{P}}$ indicate the participating and nonparticipating parties, respectively. Since H interchanges the X and Z bases, the state shared between Alice and the Bobs after the X measurements of step 1 is $(1/\sqrt{2})\big[|0 \dots 0\rangle_{\mathbf{P}} + (-1)^{\Delta(x)} |1 \dots 1\rangle_{\mathbf{P}}\big]$, where x contains all measurement outcomes announced in step 2. Finally, calculating $\Delta(x)$ in step 3, Alice locally corrects the state to obtain the desired GHZ$_{m+1}$ state.

With respect to anonymity, the key elements are the intrinsic correlations of GHZ states. As observed in Ref. [4], any rotation around the $\hat{z}$ axis applied to any

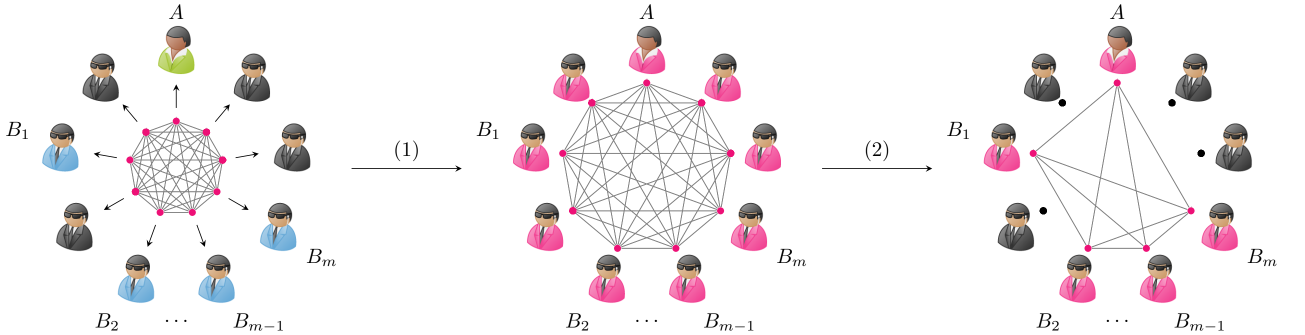


FIG. 1. Visualization of protocol 2. A GHZ$_n$ state is shared with all agents left of arrow (1). Here, the participants are highlighted in green and blue. Since the shared GHZ$_n$ state is agnostic of the receivers' identities and all agents are entangled right of arrow (1), they are all highlighted in pink. Right of arrow (2), all nonparticipating parties are disentangled and therefore not highlighted anymore. The m Bobs and Alice now share a GHZ$_{m+1}$ state after completing the steps of `AME`.

qubit of a GHZ state has the same effect on the global state independent of the chosen qubit. To correct the state, Alice only needs the parity of the measurement outcomes of the nonparticipating parties, yet, masking their identity, each Bob announces a random bit too. No information about the operations performed by the different parties can be inferred, since all announced bits can be shown to be uniformly random and a Z gate does not reveal the position of the qubit it was applied to either. Only Alice knows the identities of the Bobs, so only she is able to discern the measurement outcomes from the random bits. See the appendix for a detailed discussion on why the protocol does not leak any information about the identity of either Alice or the Bobs in untrusted settings.

A combination of the above two protocols allows for an anonymous distribution of a GHZ$_{m+1}$ state, which in turn can be measured in the Z basis by all participants to generate a shared secret key. However, to be secure against dishonest or eavesdropping parties, the state needs to be verified.

IV. ANONYMOUS QUANTUM CONFERENCE KEY AGREEMENT

In the setting of an untrusted source any verification could be performed immediately after the distribution of the state. However, a party in $\bar{\mathbf{P}}$ might not measure in protocol 2, and thereby be part of the extracted, then ($> m + 1$)-partite, GHZ state. This security risk was independently noticed in Ref. [15] for the case of two-party communication. To detect both a faulty source and dishonest parties, the verification of the state has to be postponed until *after* protocol 2. Note that in this setting, only the communication of authorized parties will be considered by Alice. Protocol 3 verifies that the state on $\mathbf{P}$ is close to the GHZ$_{m+1}$ state, and therefore also disentangled from all other parties, including $\mathbf{C}$. Protocol 3 is similar to Ref. [7] and inspired by the pseudotelepathy studies of Ref. [16], but adjusted here to protect the identities of the participants and to always set the verifier to be Alice. It requires private sources of randomness and a classical broadcasting channel.

Protocol 3 `Verification`

Input. A shared state between $|\mathbf{P}| = m + 1$ parties.
Goal. Verification or rejection of the shared state as a GHZ$_{m+1}$ state by Alice.

1. Every B_i draws a random bit b_i and measures in the X- or Y-basis if it equals 0 or 1 respectively, obtaining a measurement outcome o_i.
2. Everyone broadcasts (b_i, o_i), including Alice, who chooses her bits (b_0, o_0) at random.
3. Alice resets her bit such that $\sum_{i=0}^{m} b_i = 0 \pmod 2$. She measures in the X- or Y-basis if her bit equals 0 or 1 respectively, thereby also resetting o_0.
4. If and only if $\frac{1}{2}\sum_i b_i + \sum_{i=0}^{m} o_i = 0 \pmod 2$, Alice accepts the state.

Analysis: From Ref. [7] we know that the state is verified to be increasingly close to the GHZ state with the number of passed `Verification` rounds. To mask their identity, the parties in $\mathbf{P}$ need both $\mathbf{H}$ and $\mathbf{C}$ to announce random bits as well. This renders all public communication uniformly random. Since the relevant quantum correlations are only accessible to Alice, all parties are indistinguishable from the perspective of Eve.

We are now ready to define protocol 4 for anonymously sharing a key between $\mathbf{P}$, where we introduce the parameters L as the number of shared GHZ states and D as a parameter both determining the level of security and the length of the generated shared key. The main difference between the proposed protocol and the one in Ref. [6] is that the nonparticipating parties are asked to announce random values to mask the identities of the authorized parties and that the protocol aborts if the values are not announced in time. Protocol 4 combines all previous protocols and additionally requires a public source of randomness.

Protocol 4 `Anonymous Conference Key Agreement`

Input. Alice as initiator; parameters L and D.
Goal. Anonymous generation of secret key between $\mathbf{P}$.

1. Alice notifies the m Bobs by running the `Notification` protocol.
2. The source generates and shares L GHZ states.
3. The parties run the `AME` protocol on them.
4. For each of the L states, the parties ask a public source of randomness to broadcast a bit b such that $\Pr[b = 1] = \frac{1}{D}$.

   `Verification` **round:** If $b = 0$, Alice runs the `Verification` protocol on the $(m+1)$-partite state. The remaining parties announce random values.

   `KeyGen` **round:** If $b = 1$, Alice and the Bobs Z-measure to obtain a shared secret bit.
5. If Alice accepts all `Verification` rounds, she anonymously validates the protocol.

Analysis: The above protocol establishes a secret key between the participants, while keeping their identities secret from both outsiders and each other. The

`Verification` rounds ensure that the state on **P** is on average ϵ close to the GHZ$_{m+1}$ state with ϵ monotonically decreasing in the number of `Verification` rounds; the state thus contains correlations only observable by Alice. Likewise, neither the public communication nor the remainder of the state are correlated with the identities. On average $L[1-(1/D)]$ states are used to verify the state; therefore the key rate of protocol 4 approaches L/D in the asymptotic regime. See the appendix for a detailed proof of anonymity and Sec. V for the case where Alice does *not* accept the shared state.

Note that `Verification` implicitly verifies the `Notification` protocol, as the bits that Alice takes into consideration will not have the correct correlations otherwise. It is further worth mentioning that as presented, all protocols are self-contained. However, when combined, one could reduce both the communication overhead and the number of applied quantum operations. Specifically, instead of outputting random values, the participants could simply announce the outputs of the verification process during the next round. In the same spirit, Alice does not need to perform the Z correction at the end of the `AME` protocol, since she can choose a complementary set of stabilizer measurements during the `Verification` protocol.

V. DISCUSSION

We demonstrate how to efficiently achieve anonymity for conference key agreement by using multipartite quantum states. Starting from a large GHZ state shared between n parties, our method enables a sender to anonymously notify a set of receivers and establish a secret key that can be used to encrypt a message. This encrypted message can then be anonymously broadcast by the sender, using either a classical [13] or a quantum protocol [4]. While here we focus on GHZ states, other types of quantum states have also been used for creating anonymous entanglement, as well as for CKA [17,18]; it is however unknown whether they can be combined to achieve the same task as presented here.

We assume that the source is not actively malicious. The protocol might still abort—either due to a noisy state or due to malicious participants—but anonymity is preserved. If the source is actively malicious, a privacy leak during the `AME` round can never be caught in time, since the `AME` protocol is run before each `Verification` round. This could be fixed by additionally verifying the GHZ$_n$ after its initial sharing.

Finally, practical sources and channels can be faulty and hence the need for anonymous error correction and privacy amplification arises [12,19]. Likewise, a measure of anonymity should be introduced and is expected to be upper bounded by an appropriate validation via some closeness measure. While our present definition of anonymity aims to capture composability, further study in appropriate security frameworks [20] is required. We intend to address these issues in follow-up work, by also adjusting the validation process for noisy states and taking into account the finite-key effects of real-world implementations.

ACKNOWLEDGMENTS

A.P. and J.d.J. acknowledge support from the DFG via the Emmy Noether Grant No. 418294583 and F.H. from the Studienstiftung des deutschen Volkes. We want to thank Stefanie Barz, Julius Wallnöfer, Jens Eisert, and Nathan Walk for useful discussions.

APPENDIX A: ANONYMITY OF THE PROTOCOL

Here we prove the anonymity of our protocol. We state again the definition of anonymity from the main text.

Definition 2 (Anonymity)**.** *A protocol is anonymous from the perspective of Eve if for all subsets* **G** $\subset$ **N**

$$\Pr\left(\mathbf{G}=\mathbf{P}\mid \mathcal{I}^{+}_{\text{Eve}},\mathcal{I}_{\text{Eve}}\right)=\Pr(\mathbf{G}=\mathbf{P}\mid \mathcal{I}_{\text{Eve}}), \tag{A1}$$

where $\mathcal{I}^{+}_{\text{Eve}}$ *is the information that becomes available to Eve during the protocol and* $\mathcal{I}_{\text{Eve}}$ *is both the information that Eve has beforehand and trivial information that she obtains about the parties that she corrupts.*

In order to satisfy Eq. (A1), $\mathcal{I}^{+}_{\text{Eve}}$ should not change Eve's probability distribution of uncovering the partitioning of **N** into its constituents; it does not reveal anything about **P**, **H** or—implicitly—about **C**. Apart from the trivial attacker A we consider three different types of Eve, namely any party in **P** $\setminus A$ or **H** or all parties in **C**.

TABLE I. The rows are labeled by the types of Eve and the columns by the roles that Eve may try to uncover. The first row is mostly trivial, since the protocol is designed such that A chooses the partitioning $\mathbf{N} = \mathbf{P} \cup \bar{\mathbf{P}}$ herself and it is irrelevant that she is unaware of who in $\bar{\mathbf{P}}$ is colluding. The arguments corresponding to the symbols are given in Appendices A1–A3. As an example, the first proof of the `AME` protocol is referred to as $\bigstar_1$ and applies to the case where the roles of the nonparticipants in $\mathbf{H}$ are protected from either any $B_i \in \mathbf{P} \setminus A$ as Eve or the parties in $\mathbf{C}$ as Eve.

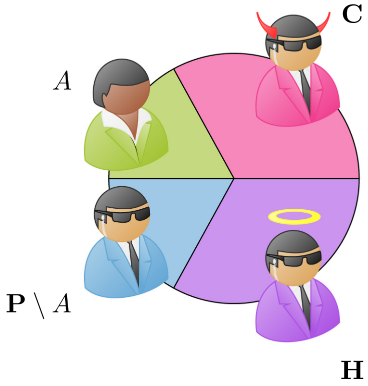
role Eve	A	$B_i \in \mathbf{P} \setminus A$	$P_j \in \mathbf{H}$	$P_k \in \mathbf{C}$
A	trivial	trivial	irrelevant	irrelevant
$B_i \in \mathbf{P} \setminus A$	★$_3$ ✓$_2$ ⚷$_3$	★$_3$ ✓$_2$ ⚷$_3$	★$_1$ ✓$_2$ ⚷$_1$	★$_3$ ✓$_2$ ⚷$_1$
$P_j \in \mathbf{H}$	★$_2$ ✓$_1$ ⚷$_1$	★$_2$ ✓$_1$ ⚷$_1$	★$_2$ ✓$_1$ ⚷$_2$	★$_2$ ✓$_1$ ⚷$_1$
$P_k \in \mathbf{C}$	★$_3$ ✓$_3$ ⚷$_1$	★$_3$ ✓$_3$ ⚷$_1$	★$_1$ ✓$_3$ ⚷$_1$	trivial

We prove anonymity for all involved subprotocols separately; as a shorthand to refer to them, we introduce the symbols ★ (`AME`), ✓ (`Verification`) and ⚷ (`KeyGen`). For each of the subprotocols, we give arguments to prove anonymity for all possible roles within the protocol that Eve may try to uncover—with respect to all types of Eve. Each argument is applicable to multiple Eve and role combinations and is sequentially labeled by indexing the symbol for easy reference. Table I shows the structure of our proof summarizing all arguments for each Eve and role combination.

For the `Notification` protocol we refer to the original paper by Broadbent and Tapp. The `AME` protocol and the `Verification` protocol are examined in Appendices A1 and A2. The `KeyGen` subprotocol does not require any public communication and is examined in Appendix A3. To prove our claim we consider the following two aspects. The *public communication* (cf. Table II) throughout the protocol does not help Eve to reveal the roles of the participating parties. We prove this by showing that all public communication is indistinguishable from Eve's point of view. As A announces only uniformly random and uncorrelated bits, we show the same for the parties in $\mathbf{P} \setminus A$, $\mathbf{H}$, and $\mathbf{C}$ from Eve's perspective. Likewise, the *quantum states* accessible to Eve do not help her to reveal the roles of the participating parties, even given access to the public communication. This means that the postmeasurement states of Eve can neither be correlated with the measurement outcomes of other parties, nor with any direct information regarding their roles. Note that the global quantum state may encode such information regarding the roles as long as it is not accessible to anyone but Alice.

TABLE II. Overview of all public communication for any party in $\mathbf{N} := \mathbf{P} \cup \mathbf{H} \cup \mathbf{C}$ when running the `AME` and `Verification` protocols. The communication summarized in the two columns needs to be indistinguishable from the perspective of any Eve. Since A only announces uniformly random and uncorrelated bits, all other communication must follow the same probability distribution. Only the communication from $\mathbf{C}$ can in principle diverge—should they choose not to hide their identities.

	`AME`	`Verification`
A	random bit r_0	random bits (b_0, o_0)
$B_i \in \mathbf{P} \setminus A$	random bit r_i	random bit b_i, outcome bit o_i
$P_j \in \mathbf{H}$	outcome bit x_j	random bits (b_j, o_j)
$P_k \in \mathbf{C}$	arbitrary bit $\tilde{x}_k$	arbitrary bits $(\tilde{b}_k, \tilde{o}_k)$



1. Anonymity during the AME protocol

At the start of the AME protocol, the shared quantum state is as given by the following equation:

$$|\mathbf{N}\rangle \approx_\epsilon \frac{1}{\sqrt{2}}\left(|0\ldots 0\rangle_{\mathbf{P}\cup\mathbf{H}} \otimes |\Psi\rangle_{\mathbf{C}} + |1\ldots 1\rangle_{\mathbf{P}\cup\mathbf{H}} \otimes |\Phi\rangle_{\mathbf{C}}\right). \tag{A2}$$

While the AME protocol prescribes measurements to both $\mathbf{H}$ and $\mathbf{C}$, the parties in $\mathbf{C}$ might not measure and announce something unrelated to their arbitrary actions on the quantum state—therefore, we now calculate only the probability of the measurement outcomes $\mu^\alpha_{\mathbf{H}} = \{\mu_j \mid j \in \mathbf{H}\}$ of $\mathbf{H}$ taking values $x^\alpha_{\mathbf{H}} = \{x^\alpha_i\} \in \{0,1\}^{|\mathbf{H}|}$. We want to show that they are uniformly random and that there are no correlations between the outcomes and any Eve that she might exploit, where Eve might be anyone in the network but Alice. That is, we want to show

$$\Pr\left(\mu^\alpha_{\mathbf{H}} = x^\alpha_{\mathbf{H}} \mid \mathcal{I}^+_{\text{Eve}}, \mathcal{I}_{\text{Eve}}\right) = \Pr\left(\mu^\alpha_{\mathbf{H}} = x^\alpha_{\mathbf{H}}\right) = \frac{1}{2^{|\mathbf{H}|}}, \tag{A3}$$

where the second equality implies that the probability distribution of the measurement outcomes is uniform and the first equality implies that there are no correlations between the information accessible to Eve—including her quantum state—and the measurement outcomes. Moreover, we also want to show that the postmeasurement state does not possess any other correlations regarding the roles of the parties that are accessible or exploitable by Eve.

The measurements on $\mathbf{H}$ in the AME protocol are a projection-valued measure with outcomes $\{x^\alpha_{\mathbf{H}}\}$ and associated projectors

$$X^\alpha_{\mathbf{H}} := H_{\mathbf{H}}|x^\alpha_{\mathbf{H}}\rangle\langle x^\alpha_{\mathbf{H}}|_{\mathbf{H}}H_{\mathbf{H}} = \bigotimes_{j\in\mathbf{H}} H_j\,|x^\alpha_j\rangle\langle x^\alpha_j|_j\,H_j, \tag{A4}$$

which results in the probability of the measurement outcome $\mu^\alpha_{\mathbf{H}}$ taking the value $x^\alpha_{\mathbf{H}}$ being given by

$$\begin{aligned}
\Pr(\mu^\alpha_{\mathbf{H}} = x^\alpha_{\mathbf{H}}) &= \operatorname{tr}\big[X^\alpha_{\mathbf{H}}|\mathbf{N}\rangle\langle\mathbf{N}|\big] \\
&= \frac{1}{2}\operatorname{tr}\big[\,(|0\ldots 0\rangle\langle 0\ldots 0|_{\mathbf{P}})\,\big]\operatorname{tr}\big[X^\alpha_{\mathbf{H}}|0\ldots 0\rangle\langle 0\ldots 0|_{\mathbf{H}}\big]\operatorname{tr}\big[|\Psi\rangle\langle\Psi|_{\mathbf{C}}\big] \\
&\quad + \frac{1}{2}\operatorname{tr}\big[\,(|0\ldots 0\rangle\langle 1\ldots 1|_{\mathbf{P}})\,\big]\operatorname{tr}\big[X^\alpha_{\mathbf{H}}|0\ldots 0\rangle\langle 1\ldots 1|_{\mathbf{H}}\big]\operatorname{tr}\big[|\Psi\rangle\langle\Phi|_{\mathbf{C}}\big] \\
&\quad + \frac{1}{2}\operatorname{tr}\big[\,(|1\ldots 1\rangle\langle 0\ldots 0|_{\mathbf{P}})\,\big]\operatorname{tr}\big[X^\alpha_{\mathbf{H}}|1\ldots 1\rangle\langle 0\ldots 0|_{\mathbf{H}}\big]\operatorname{tr}\big[|\Phi\rangle\langle\Psi|_{\mathbf{C}}\big] \\
&\quad + \frac{1}{2}\operatorname{tr}\big[\,(|1\ldots 1\rangle\langle 1\ldots 1|_{\mathbf{P}})\,\big]\operatorname{tr}\big[X^\alpha_{\mathbf{H}}|1\ldots 1\rangle\langle 1\ldots 1|_{\mathbf{H}}\big]\operatorname{tr}\big[|\Phi\rangle\langle\Phi|_{\mathbf{C}}\big] \\
&= \frac{1}{2}\operatorname{tr}\Bigg[\left(\bigotimes_{j\in\mathbf{H}} H_j\,|x^\alpha_j\rangle\langle x^\alpha_j|_j\,H_j\right)|0\ldots 0\rangle\langle 0\ldots 0|_{\mathbf{H}}\Bigg] \\
&\quad + \frac{1}{2}\operatorname{tr}\Bigg[\left(\bigotimes_{j\in\mathbf{H}} H_j\,|x^\alpha_j\rangle\langle_j|H_j\right)|1\ldots 1\rangle\langle 1\ldots 1|_{\mathbf{H}}\Bigg] \\
&= \frac{1}{2}\left(\prod_{i\in\mathbf{H}}|\langle x^\alpha_i|\,|+\rangle|^2 + \prod_{i\in\mathbf{H}}|\langle x^\alpha_i|\,|-\rangle|^2\right) \\
&= \frac{1}{2}\left(\frac{1}{2^{|\mathbf{H}|}} + \frac{1}{2^{|\mathbf{H}|}}\right) = \frac{1}{2^{|\mathbf{H}|}}.
\end{aligned} \tag{A5}$$

This satisfies the second equality in Eq. (A3), showing that the measurement outcomes are uniformly random, thereby ensuring that all the communication of the AME column of Table II is indistinguishable—excluding the trivial case where $\mathbf{C}$ reveals itself.

The global postmeasurement state $\rho_{\texttt{postAME}}$ is then

$$\begin{aligned}
\rho_{\texttt{postAME}} &= X^{\alpha}_{\mathbf{H}}|\mathbf{N}\rangle\langle\mathbf{N}|X^{\alpha}_{\mathbf{H}} \\
&= \frac{1}{2}\left(|0\ldots0\rangle\langle0\ldots0|_{\mathbf{P}}\right)\otimes X^{\alpha}_{\mathbf{H}}|0\ldots0\rangle\langle0\ldots0|_{\mathbf{H}}X^{\alpha}_{\mathbf{H}}\otimes|\Psi\rangle\langle\Psi|_{\mathbf{C}} \\
&\quad+\frac{1}{2}\left(|0\ldots0\rangle\langle1\ldots1|_{\mathbf{P}}\right)\otimes X^{\alpha}_{\mathbf{H}}|0\ldots0\rangle\langle1\ldots1|_{\mathbf{H}}X^{\alpha}_{\mathbf{H}}\otimes|\Psi\rangle\langle\Phi|_{\mathbf{C}} \\
&\quad+\frac{1}{2}\left(|1\ldots1\rangle\langle0\ldots0|_{\mathbf{P}}\right)\otimes X^{\alpha}_{\mathbf{H}}|1\ldots1\rangle\langle0\ldots0|_{\mathbf{H}}X^{\alpha}_{\mathbf{H}}\otimes|\Phi\rangle\langle\Psi|_{\mathbf{C}} \\
&\quad+\frac{1}{2}\left(|1\ldots1\rangle\langle1\ldots1|_{\mathbf{P}}\right)\otimes X^{\alpha}_{\mathbf{H}}|1\ldots1\rangle\langle1\ldots1|_{\mathbf{H}}X^{\alpha}_{\mathbf{H}}\otimes|\Phi\rangle\langle\Phi|_{\mathbf{C}} \\
&= \frac{1}{2}\left(|0\ldots0\rangle\langle0\ldots0|_{\mathbf{P}}\right)\otimes|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Psi\rangle\langle\Psi|_{\mathbf{C}} \\
&\quad+\frac{1}{2}\left(|0\ldots0\rangle\langle1\ldots1|_{\mathbf{P}}\right)\otimes(-1)^{\Delta(x^{\alpha}_{\mathbf{H}})}|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Psi\rangle\langle\Phi|_{\mathbf{C}} \\
&\quad+\frac{1}{2}\left(|1\ldots1\rangle\langle0\ldots0|_{\mathbf{P}}\right)\otimes(-1)^{\Delta(x^{\alpha}_{\mathbf{H}})}|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Phi\rangle\langle\Psi|_{\mathbf{C}} \\
&\quad+\frac{1}{2}\left(|1\ldots1\rangle\langle1\ldots1|_{\mathbf{P}}\right)\otimes|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Phi\rangle\langle\Phi|_{\mathbf{C}} \\
&= |\mathbf{N}_{\texttt{postAME}}\rangle\langle\mathbf{N}_{\texttt{postAME}}|,
\end{aligned} \tag{A6}$$

where $|\mathbf{H}\rangle=\bigotimes_{i\in\mathbf{H}}H_i\,|x^{\alpha}_i\rangle_i$ is the postmeasurement state associated with measurement outcome $x^{\alpha}_{\mathbf{H}}$ and $|\mathbf{N}_{\texttt{postAME}}\rangle\langle\mathbf{N}_{\texttt{postAME}}|$ is the pure state

$$|\mathbf{N}_{\texttt{postAME}}\rangle=\frac{1}{\sqrt{2}}\big[\,|0\ldots0\rangle_{\mathbf{P}}\otimes|\Psi\rangle_{\mathbf{C}}+(-1)^{\Delta(x^{\alpha}_{\mathbf{H}})}\,|1\ldots1\rangle_{\mathbf{P}}\otimes|\Phi\rangle_{\mathbf{C}}\,\big]\otimes|\mathbf{H}\rangle\,, \tag{A7}$$

showing that the only correlation between the measurement outcome and the state on $\mathbf{P}\cup\mathbf{C}$ is in the phase, where one could in principle learn the parity of the measurement outcome $x^{\alpha}_{\mathbf{H}}$. However, any such phase estimation is impossible if one does not have access to the complete state (i.e., tracing out $\mathbf{P}$ that does not collude with Eve results in a state on $\mathbf{C}$ that is uncorrelated with the measurement outcome $x^{\alpha}_{\mathbf{H}}$). This means that the postmeasurement state of any attacker in $\mathbf{P}\setminus A$ or $\mathbf{C}$ is uncorrelated from the measurement outcome $x^{\alpha}_{\mathbf{H}}$ and the roles of $\mathbf{H}$. Therefore, for either of these types of Eve everyone in $\mathbf{H}$ remains anonymous (cf. $\bigstar_1$ in Table I).

Furthermore, $\mathbf{H}$ is disentangled from the rest of the network and $|\mathbf{H}\rangle$ itself is separable over the constituents of $\mathbf{H}$. Therefore, nobody in $\mathbf{H}$ can learn anything about the roles of any other party in the network. We can conclude that for Eve in $\mathbf{H}$, Definition 1 holds for any of the subsets of $\mathbf{N}$ (cf. $\bigstar_2$ in Table I).

When Eve is a party in $\mathbf{P}\setminus A$, the roles of the parties in either $\mathbf{P}$ or $\mathbf{C}$ are hidden because the relevant correlations of the state are unchanged by running the AME protocol—they essentially share a GHZ state, possibly including some additional phase, and therefore there are no revealing correlations available to anyone but Alice, meaning that here Definition 1 also holds. The exact same argument holds for Eve in $\mathbf{C}$ with respect to the anonymity of $\mathbf{P}$ (cf. $\bigstar_3$ in Table I).

2. Anonymity during the `Verification` rounds

At the start of the `Verification` round, the state is the postmeasurement state from Eq. (A7), up to the correction by A. We allow for a faulty correction, therefore keeping the phase arbitrary in the following analysis, writing $(-1)^{\Delta}=\pm1$ for the phase. We again calculate the probability that, based on some basis choice $\{b_i\}$ and given the AME measurement outcome $x^{\alpha}_{\mathbf{H}}$, the measurement outcome $\mu^{\alpha}=\{\mu_j\mid j\in\mathbf{P}\setminus A\}$ takes some particular value $o^{\alpha}=\{o^{\alpha}_i\}\in\{0,1\}^{|\mathbf{P}\setminus A|}$, show that the outcome is uniformly random and that there are no correlations between the outcome and the quantum states of all possible Eves. That is, we want to show that

$$\Pr\left(\mu^{\alpha}=o^{\alpha}\mid\mathcal{I}^{+}_{\text{Eve}},\mathcal{I}_{\text{Eve}}\right)=\Pr\left(\mu^{\alpha}=o^{\alpha}\right)=\frac{1}{2^{|\mathbf{P}\setminus A|}}, \tag{A8}$$

where Eve may be anyone in $\mathbf{P}\setminus A$, $\mathbf{H}$, or $\mathbf{C}$. Again, we also show that the postmeasurement states do not possess any other correlations regarding the roles of the parties, which are exploitable by anyone in $\mathbf{P}\setminus A$, $\mathbf{H}$, or $\mathbf{C}$.

Each measurement outcome is associated with a certain measurement projector $O^{\alpha}_{\mathbf{P}\setminus A}$, which is itself dependent on the basis choice $\{b_i\}$. Explicitly, we define

$$O^{\alpha}_{\mathbf{P}\setminus A}(\{b_i\}) := \left(\bigotimes_{\{i\in\mathbf{P}\setminus A|b_i=0\}} H_i|o_i^{\alpha}\rangle\langle o_i^{\alpha}|H_i\right)\otimes\left(\bigotimes_{\{i\in\mathbf{P}\setminus A|b_i=1\}} \sqrt{Z_i}H_i|o_i^{\alpha}\rangle\langle o_i^{\alpha}|H_i\sqrt{Z_i}^{\dagger}\right). \tag{A9}$$

Hence, for any outcome $x^{\alpha}_{\mathbf{H}}$ during the `AME` protocol, the probability of the measurement outcome μ^{α} being equal to o^{α} becomes (remember that Δ may depend on $x^{\alpha}_{\mathbf{H}}$)

$$\begin{aligned}\Pr(\mu^{\alpha}=m^{\alpha}) &= \mathrm{tr}\big[O^{\alpha}|\mathbf{N}_{\mathrm{post}\texttt{AME}}\rangle\langle\mathbf{N}_{\mathrm{post}\texttt{AME}}|\big]\\ &= \frac{1}{2}\mathrm{tr}\big[|0\rangle\langle 0|_A\big]\mathrm{tr}\big[O^{\alpha}|0\ldots0\rangle\langle0\ldots0|_{\mathbf{P}\setminus A}\big]\mathrm{tr}\big[|\mathbf{H}\rangle\langle\mathbf{H}|\big]\mathrm{tr}\big[|\Psi\rangle\langle\Psi|_{\mathbf{C}}\big]\\ &\quad+(-1)^{\Delta}\frac{1}{2}\mathrm{tr}\big[|0\rangle\langle 1|_A\big]\mathrm{tr}\big[O^{\alpha}|0\ldots0\rangle\langle1\ldots1|_{\mathbf{P}\setminus A}\big]\mathrm{tr}\big[|\mathbf{H}\rangle\langle\mathbf{H}|\big]\mathrm{tr}\big[|\Psi\rangle\langle\Phi|_{\mathbf{C}}\big]\\ &\quad+(-1)^{\Delta}\frac{1}{2}\mathrm{tr}\big[|1\rangle\langle 0|_A\big]\mathrm{tr}\big[O^{\alpha}|1\ldots1\rangle\langle0\ldots0|_{\mathbf{P}\setminus A}\big]\mathrm{tr}\big[|\mathbf{H}\rangle\langle\mathbf{H}|\big]\mathrm{tr}\big[|\Phi\rangle\langle\Psi|_{\mathbf{C}}\big]\\ &\quad+\frac{1}{2}\mathrm{tr}\big[|1\rangle\langle 1|_A\big]\mathrm{tr}\big[O^{\alpha}|1\ldots1\rangle\langle1\ldots1|_{\mathbf{P}\setminus A}\big]\mathrm{tr}\big[|\mathbf{H}\rangle\langle\mathbf{H}|\big]\mathrm{tr}\big[|\Phi\rangle\langle\Phi|_{\mathbf{C}}\big]\\ &= \frac{1}{2}\mathrm{tr}\big[O^{\alpha}|0\ldots0\rangle\langle0\ldots0|_{\mathbf{P}\setminus A}\big]\\ &\quad+\frac{1}{2}\mathrm{tr}\big[O^{\alpha}|1\ldots1\rangle\langle1\ldots1|_{\mathbf{P}\setminus A}\big].\end{aligned} \tag{A10}$$

Substituting O^{α} we obtain

$$\begin{aligned}\Pr(\mu^{\alpha}=m^{\alpha}) &= \frac{1}{2}\prod_{\{i\in\mathbf{P}\setminus A|b_i=0\}}\langle o_i^{\alpha}|H_i|0\rangle\langle0|H_i|o_i^{\alpha}\rangle\prod_{\{i\in\mathbf{P}\setminus A|b_i=1\}}\langle o_i^{\alpha}|H_i\sqrt{Z_i}^{\dagger}|0\rangle\langle0|\sqrt{Z_i}|H_i\rangle o_i^{\alpha}\\ &\quad+\frac{1}{2}\prod_{\{i\in\mathbf{P}\setminus A|b_i=0\}}\langle o_i^{\alpha}|H_i|1\rangle\langle1|H_i|o_i^{\alpha}\rangle\prod_{\{i\in\mathbf{P}\setminus A|b_i=1\}}\langle o_i^{\alpha}|H_i\sqrt{Z_i}^{\dagger}|1\rangle\langle1|\sqrt{Z_i}H_i|o_i^{\alpha}\rangle,\\ &= \frac{1}{2}\prod_{\{i\in\mathbf{P}\setminus A|b_i=0\}}|\langle o_i^{\alpha}|\,|+\rangle|^2\prod_{\{i\in\mathbf{P}\setminus A|b_i=1\}}|\langle o_i^{\alpha}|\,|+\rangle|^2\\ &\quad+\frac{1}{2}\prod_{\{i\in\mathbf{P}\setminus A|b_i=0\}}|\langle o_i^{\alpha}|\,|-\rangle|^2\prod_{\{i\in\mathbf{P}\setminus A|b_i=1\}}|\langle o_i^{\alpha}|\,|-\rangle|^2\\ &= \frac{1}{2^{|\mathbf{P}\setminus A|}},\end{aligned} \tag{A11}$$

which satisfies the second equation in Eq. (A8). The global postmeasurement state $\rho_{\mathrm{post}\texttt{VER}}$ becomes

$$\begin{aligned}\rho_{\mathrm{post}\texttt{VER}} =& O^{\alpha}|\mathbf{N}_{\mathrm{postAME}}\rangle\langle\mathbf{N}_{\mathrm{postAME}}|O^{\alpha}\\ &= \frac{1}{2}|0\rangle\langle0|_A\otimes\big(O^{\alpha}|0\ldots0\rangle\langle0\ldots0|_{\mathbf{P}\setminus A}O^{\alpha}\big)\otimes|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Psi\rangle\langle\Psi|_{\mathbf{C}}\\ &\quad+(-1)^{\Delta}\frac{1}{2}|0\rangle\langle1|_A\otimes\big(O^{\alpha}|0\ldots0\rangle\langle1\ldots1|_{\mathbf{P}\setminus A}O^{\alpha}\big)\otimes|\mathbf{H}\rangle\langle\mathbf{H}|\otimes|\Psi\rangle\langle\Phi|_{\mathbf{C}}\end{aligned}$$

$$\begin{aligned}
&+ (-1)^{\Delta}\frac{1}{2}|1\rangle\langle 0|_{A} \otimes \left(O^{\alpha}|1\ldots 1\rangle\langle 0\ldots 0|_{\mathbf{P}\setminus A}O^{\alpha}\right) \otimes |\mathbf{H}\rangle\langle\mathbf{H}| \otimes |\Phi\rangle\langle\Psi|_{\mathbf{C}}\\
&+ \frac{1}{2}|1\rangle\langle 1|_{A} \otimes \left(O^{\alpha}|1\ldots 1\rangle\langle 1\ldots 1|_{\mathbf{P}\setminus A}O^{\alpha}\right) \otimes |\mathbf{H}\rangle\langle\mathbf{H}| \otimes |\Phi\rangle\langle\Phi|_{\mathbf{C}}\\
=&\ \frac{1}{2}|0\rangle\langle 0|_{A} \otimes |\mathbf{P}\setminus A\rangle\langle\mathbf{P}\setminus A| \otimes |\mathbf{H}\rangle\langle\mathbf{H}| \otimes |\Psi\rangle\langle\Psi|_{\mathbf{C}}\\
&+ \gamma^{\dagger}\frac{1}{2}|0\rangle\langle 1|_{A} \otimes |\mathbf{P}\setminus A\rangle\langle\mathbf{P}\setminus A| \otimes |\mathbf{H}\rangle\langle\mathbf{H}| \otimes |\Psi\rangle\langle\Phi|_{\mathbf{C}}\\
&+ \gamma\frac{1}{2}|1\rangle\langle 0|_{A} \otimes |\mathbf{P}\setminus A\rangle\langle\mathbf{P}\setminus A| \otimes |\mathbf{H}\rangle\langle\mathbf{H}| \otimes |\Phi\rangle\langle\Psi|_{\mathbf{C}}\\
&+ \frac{1}{2}|1\rangle\langle 1|_{A} \otimes |\mathbf{P}\setminus A\rangle\langle\mathbf{P}\setminus A| \otimes |\mathbf{H}\rangle\langle\mathbf{H}| \otimes |\Phi\rangle\langle\Phi|_{\mathbf{C}}\big]\\
=&\ |\mathbf{N}_{\mathrm{post}\mathtt{VER}}\rangle\langle\mathbf{N}_{\mathrm{post}\mathtt{VER}}|,
\end{aligned} \tag{A12}$$

where $\gamma = (-1)^{\Delta} \times (-i)^{|\{b_i\}|}$ and $|\mathbf{N}_{\mathrm{post}\mathtt{VER}}\rangle$ is the pure state

$$|\mathbf{N}_{\mathrm{post}\mathtt{VER}}\rangle := \left(|0\rangle_{A} \otimes |\Psi\rangle_{\mathbf{C}} + \gamma\,|1\rangle_{A} \otimes |\Phi\rangle_{\mathbf{C}}\right) \otimes |\mathbf{P}\setminus A\rangle \otimes |\mathbf{H}\rangle \tag{A13}$$

and $|\mathbf{P}\setminus A\rangle$ is the state associated with the measurement outcome o^{α}

$$|\mathbf{P}\setminus A\rangle := \left(\bigotimes_{i\in\{\mathbf{P}\setminus A|b_i=0\}} H_i\,|o_i^{\alpha}\rangle_i\right) \otimes \left(\bigotimes_{i\in\{\mathbf{P}\setminus A|b_i=1\}} \sqrt{Z_i}H_i\,|o_i^{\alpha}\rangle_i\right). \tag{A14}$$

From the perspective of **H**, all communication is indistinguishable (cf. the `Verification` column in Table II); **H** is disentangled from everyone else and the state on **H** is itself separable. We can conclude that—with anyone in **H** as Eve—the anonymity of everyone in the network is preserved (cf. $\checkmark_1$ in Table I).

Moreover, $\mathbf{P}\setminus A$ is disentangled from all other parties in the network and their postmeasurement state is separable as well. Again, all communication from their perspective is uniformly random (cf. the `Verification` column in Table II), so we can conclude that—with anyone in $\mathbf{P}\setminus A$ as Eve—the anonymity of everyone in the network is maintained (cf. $\checkmark_2$ in Table I).

The only relevant information is $|\{b_i\}|$, which is encoded into the phase of the state on $A \cup \mathbf{C}$; any phase estimation algorithm to retrieve this information would require access to the entire state, including the state of A, which is inaccessible to **C**. Again, from the perspective of **C** all communication is indistinguishable (cf. the `Verification` column in Table II) and we can conclude that—with **C** as Eve—here too the anonymity of all parties in the network is preserved (cf. $\checkmark_3$ in Table I).

Note that the `Verification` round can only pass if $|\Psi\rangle_{\mathbf{C}} = |\Phi\rangle_{\mathbf{C}}$, that is when **C** is not entangled to A and $\mathbf{P}\setminus A$. However, this is not a necessary condition for anonymity, since the identity of Alice is preserved even if the `Verification` round fails. There is no information encoded into the state regarding the distribution of **P** and **H**, nor into the measurement outcome o^{α}. The only valuable information in the state is the parity of the number of Y measurements, encoded in the phase of the qubit of A, which is disentangled from all other parties and therefore only accessible to A.

3. Anonymity during the `KeyGen` rounds

As the `Verification` rounds ensure that the GHZ_{m+1} state on **P** is disentangled from the nonparticipating parties in $\bar{\mathbf{P}}$ and after running the `AME` protocol no party in **H** is entangled to any other party, all subsets listed in Table I are disentangled from each other. Hence, we can write the full-network state at the start of the `KeyGen` round as

$$|\mathbf{N}_{\mathtt{KeyGen}}\rangle \mathrel{\hat{=}} |\mathrm{GHZ}\rangle_{\mathbf{P}} \otimes |\mathbf{H}\rangle \otimes |\Psi\rangle_{\mathbf{C}}\,. \tag{A15}$$

Since there is no communication during the `KeyGen` rounds, there is no leakage from $\mathbf{P}, \mathbf{H}, \mathbf{C}$ outside the subset itself (cf. ⚷$_1$ in Table I). As $|\mathbf{H}\rangle$ is a separable state, the case **H** is trivial (cf. ⚷$_2$ in Table I). Finally, due to its symmetries, the GHZ_{m+1} state cannot reveal who the parties sharing the state are. This ensures that there is no privacy leakage for **P** either (cf. ⚷$_3$ in Table I).

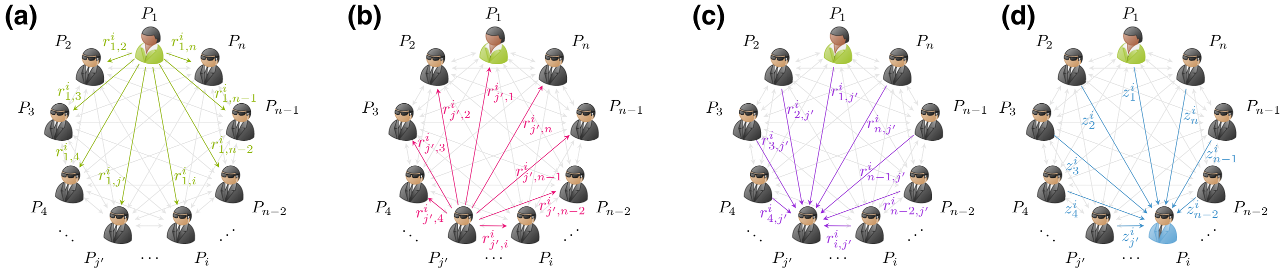
APPENDIX B: VISUALIZATION OF THE `NOTIFICATION` PROTOCOL

Protocol 1 `Notification`

Input. Alice's choice of m receivers.
Goal. The m receivers get notified.

For agent $i = 1, \ldots, n$:

1. All agents $j \in \{1, \ldots, n\}$ do the following.
   (a) When j corresponds to Alice (j_a), and i is not a receiver, she chooses n random bits $\{r^i_{j,k}\}^n_{k=1}$ such that $\bigoplus^n_{k=1} r^i_{j,k} = 0$. If i is a receiver, she chooses n random bits such that $\bigoplus^n_{k=1} r^i_{j,k} = 1$. She sends bit $r^i_{j,k}$ to agent k [Fig. 2(a)].
   (b) When $j \neq j_a$, the agent chooses n random bits $\{r^i_{j,k}\}^n_{k=1}$ such that $\bigoplus^n_{k=1} r^i_{j,k} = 0$ and sends bit $r^i_{j,k}$ to agent k [Fig. 2(b)].
2. All agents $k \in \{1, \ldots, n\}$ receive $\{r^i_{j,k}\}^n_{j=1}$ [Fig. 2(c)] , compute $z^i_k = \bigoplus^n_{j=1} r^i_{j,k}$ and send it to agent i.
3. Agent i takes the received $\{z^i_k\}^n_{k=1}$ [Fig. 2(d)] to compute $z^i = \bigoplus^n_{k=1} z^i_k$; if $z^i = 1$ they are thereby notified to be a designated receiver.



Step 1a with $j_a = 1$.

Step 1b with $j = j'$.

Step 2 with $k = j'$

Step 3 with $i = i_b$.

j k	1	2	3	$\cdots$	j'	$\cdots$	i	$\cdots$	n
1	$r^i_{1,1}$	$r^i_{1,2}$	$r^i_{1,3}$	$\cdots$	$r^i_{1,j'}$	$\cdots$	$r^i_{1,i}$	$\cdots$	$r^i_{1,n}$
2	$r^i_{2,1}$	$r^i_{2,2}$	$r^i_{2,3}$	$\cdots$	$r^i_{2,j'}$	$\cdots$	$r^i_{2,i}$	$\cdots$	$r^i_{2,n}$
3	$r^i_{3,1}$	$r^i_{3,2}$	$r^i_{3,3}$	$\cdots$	$r^i_{3,j'}$	$\cdots$	$r^i_{3,i}$	$\cdots$	$r^i_{3,n}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
j'	$r^i_{j',1}$	$r^i_{j',2}$	$r^i_{j',3}$	$\cdots$	$r^i_{j',j'}$	$\cdots$	$r^i_{j',i}$	$\cdots$	$r^i_{j',n}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
i	$r^i_{i,1}$	$r^i_{i,2}$	$r^i_{i,3}$	$\cdots$	$r^i_{i,j'}$	$\cdots$	$r^i_{i,i}$	$\cdots$	$r^i_{i,n}$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
n	$r^i_{n,1}$	$r^i_{n,2}$	$r^i_{n,3}$	$\cdots$	$r^i_{n,j'}$	$\cdots$	$r^i_{n,i}$	$\cdots$	$r^i_{n,n}$
$\bigoplus_j r^i_{j,k}$	z^i_1	z^i_2	z^i_3	$\cdots$	$z^i_{j'}$	$\cdots$	z^i_i	$\cdots$	z^i_n

FIG. 2. Visualization of protocol 1. The table contains all $r^i_{j,k}$ for a fixed agent $P_i \in \mathbf{N}$ in the `Notification` protocol. Here, we identify Alice with P_1. She chooses $\{r^i_{1,k}\}^n_{k=1}$ and sends them to P_k in step 1a [Fig. 2(a)]. Note that only if P_i is a receiver, the green row adds up to 1 (mod 2); otherwise to 0 (mod 2). Analogously, the pink highlighting shows step 1b from the perspective of $P_{j'}$ [Fig. 2(b)]. This and all other rows add up to 0 (mod 2). The $\{r^i_{j,j'}\}^n_{j=1}$ that $P_{j'}$ receives in step 2 [Fig. 2(c)] are highlighted in purple. The last row, highlighted in blue, shows the $\{z^i_k\}^n_{k=1}$ received by P_i in step 3 [Fig. 2(d)]. By construction, only if P_i is a receiver, it adds up to 1 (mod 2).

[1] C. H. Bennett, and G. Brassard, in *IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, 1984), p. 175.

[2] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, **2**, 1 (2016).

[3] G. Murta, F. Grasselli, H. Kampermann, and D. Bruß, Quantum Conference Key Agreement: A Review, arXiv:2003.10186 [quant-ph] (2020).

[4] M. Christandl, and S. Wehner, in *International Conference on the Theory and Application of Cryptology and Information Security*, edited by B. Roy (Springer, Berlin, Heidelberg, 2005), p. 217.

[5] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, Fundamental Theories of Physics Vol. 37, edited by M. Kafatos (Springer, Dordrecht, 1989).

[6] A. Unnikrishnan, I. J. MacFarlane, R. Yi, E. Diamanti, D. Markham, and I. Kerenidis, Anonymity for Practical Quantum Networks, Phys. Rev. Lett. **122**, 240501 (2019).

[7] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, Multipartite Entanglement Verification Resistant against Dishonest Parties, Phys. Rev. Lett. **108**, 260502 (2012).

[8] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis, J. G. Rarity, and M. S. Tame, Experimental verification of multipartite entanglement in quantum networks, Nat. Commun. **7**, 13251 (2016).

[9] D. Leung, J. Oppenheim, and A. Winter, Quantum network communication–the butterfly and beyond, IEEE Trans. on Inf. Theory **56**, 3478 (2010).

[10] F. Hahn, A. Pappa, and J. Eisert, Quantum network routing and local complementation, Npj Quantum Inf. **5**, 1 (2019).

[11] D. Goyeneche, D. Alsina, J. I. Latorre, A. Riera, and K. Życzkowski, Absolutely maximally entangled states, combinatorial designs, and multiunitary matrices, Phys. Rev. A **92**, 032316 (2015).

[12] M. Epping, H. Kampermann, C. Macchiavello, and D. Bruß, Multi-partite entanglement can speed up quantum key distribution in networks, New J. Phys. **19**, 093012 (2017).

[13] A. Broadbent, and A. Tapp, in *Advances in Cryptology – ASIACRYPT 2007. Lecture Notes in Computer Science*, edited by K. Kurosawa, Vol. 4833 (Springer, Berlin, Heidelberg, 2007), p. 410.

[14] M. Fitzi, N. Gisin, U. Maurer, and O. von Rotz, in *Advances in Cryptology – EUROCRYPT 2002*, edited by L. R. Knudsen (Springer Berlin Heidelberg, Berlin, Heidelberg, 2002), p. 482.

[15] Y.-G. Yang, Y.-L. Yang, X.-L. Lv, Y.-H. Zhou, and W.-M. Shi, Examining the correctness of anonymity for practical quantum networks, Phys. Rev. A **101**, 062311 (2020).

[16] G. Brassard, A. Broadbent, and A. Tapp, in *Algorithms and Data Structures*, Lecture Notes in Computer Science, edited by F. Dehne, J.-R. Sack, and M. Smid (Springer, Berlin, Heidelberg, 2003), p. 1.

[17] V. Lipinska, G. Murta, and S. Wehner, Anonymous transmission in a noisy quantum network using the W state, Phys. Rev. A **98**, 052320 (2018).

[18] F. Grasselli, H. Kampermann, and D. Bruß, Conference key agreement with single-photon interference, New J. Phys. **21**, 123002 (2019).

[19] M. Proietti, J. Ho, F. Grasselli, P. Barrow, M. Malik, and A. Fedrizzi, Experimental quantum conference key agreement, arXiv:2002.01491 [quant-ph] (2020).

[20] D. Unruh, in Advances in Cryptology – EUROCRYPT 2010, edited by H. Gilbert (Springer Berlin Heidelberg, Berlin, Heidelberg, 2010), p. 486.