Anonymity for Practical Quantum Networks

Anupama Unnikrishnan,[1] Ian J. MacFarlane,[2] Richard Yi,[2] Eleni Diamanti,[3]
Damian Markham,[3] and Iordanis Kerenidis[4]
[1]*Clarendon Laboratory, University of Oxford, Oxford OX1 3PU, UK*
[2]*Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA*
[3]*LIP6, CNRS, Sorbonne Université, 75005 Paris, France*
[4]*IRIF, CNRS, Université Paris Diderot, Sorbonne Paris Cité, 75013 Paris, France*

(Received 12 November 2018; published 19 June 2019)

Quantum communication networks have the potential to revolutionize information and communication technologies. Here we are interested in a fundamental property and formidable challenge for any communication network, that of guaranteeing the anonymity of a sender and a receiver when a message is transmitted through the network, even in the presence of malicious parties. We provide the first practical protocol for anonymous communication in realistic quantum networks.

DOI: 10.1103/PhysRevLett.122.240501

The rapid development of quantum communication networks will allow a large number of agents with different technological, classical or quantum, capabilities to securely exchange messages and perform efficiently distributed computational tasks, opening new perspectives for information and communication technologies and eventually leading to the quantum internet [1]. Many applications of quantum networks are known, including, for example, quantum key distribution [2,3] or blind and verifiable delegation of quantum computation [4], and many more are yet to be developed.

A crucial yet challenging functionality required in any network is the ability to guarantee the anonymity of two parties, the sender and the receiver, when they wish to transmit a message through the network. In a realistic network, anonymity should be guaranteed in the presence of malicious parties. We would additionally like that this happens in an information-theoretic setting, meaning without making any assumptions neither on the number nor on the computational power of these malicious parties, who might in fact have a quantum computer in their hands.

In the classical setting, anonymity, as well as any multiparty secure computation, is possible with information-theoretic security when there is an honest majority of agents. Furthermore, Broadbent and Tapp [5] showed how to anonymously transmit a classical message, as well as a number of other secure protocols, in the absence of an honest majority. In order to do this, secure pairwise classical channels are required, as well as classical broadcast channels.

In the quantum setting, the first work to deal with the anonymity of quantum messages was that of Christandl and Wehner [6]. In their work, one assumes that the n agents share a perfect n-party GHZ state, i.e., the state $(|0^n\rangle + |1^n\rangle)/\sqrt{2}$ [7]. Under this assumption, they provide protocols with perfect anonymity both for the broadcast of a classical bit and for the creation of an EPR pair, i.e., the state $(|00\rangle + |11\rangle)/\sqrt{2}$, between a sender and a receiver. Then, they combine the two protocols in order to transmit a quantum message using a teleportation scheme [8]. This first creates an EPR pair anonymously between the sender and the receiver, and then the sender transmits the two classical outcomes of her measurements anonymously. The advantage of this protocol is that it only involves local operations and classical communication once the GHZ state is shared between the agents. However, it requires the assumption that a perfect GHZ state has been honestly shared between the agents. More recently, Lipinska *et al.* [9] showed how to perform a similar protocol starting from trusted W states, albeit only probabilistically.

In order to remedy the drawback of a perfect shared quantum state, Brassard *et al.* [10] devised a different protocol, which includes a verification stage for ensuring that the shared state is at least symmetric with respect to the honest agents, and hence perfect anonymity is preserved. This test involves each agent performing a controlled-NOT operation between her initial quantum bit (qubit) and $n-1$ fresh ancilla qubits that she then sends to all other agents. Each agent then measures $n-1$ qubits in the subspace spanned by the all zeros and all ones strings, and if the measurement accepts then the protocol continues with the remaining n-party GHZ state. While the authors manage in this way to preserve perfect anonymity, their protocol cannot be easily implemented, since each agent needs to perform a size-n quantum circuit and also to have access to quantum communication with all other agents.

We address this problem by considering quantum anonymous transmission in the presence of an untrusted source that may not be producing the GHZ state. Our two main ingredients are the Christandl-Wehner protocol for

anonymous entanglement [6] and a protocol for verifying GHZ states described in Ref. [11]. We then present a new notion of approximate anonymity that is appropriate for realistic quantum networks and show a practical and efficient protocol to achieve such anonymity in the transfer of a quantum message.

Communication scenario.—Let us first describe the communication scenario we consider. Our network consists of n agents who can perform local operations and measurements. A source, who may be malicious, produces GHZ states that our agents wish to use for anonymous quantum communication. The source may produce a different state in every round, or even entangle the states between different rounds.

The agents themselves may be honest or malicious. Honest agents follow the protocol but malicious agents can collaborate with the source, work together, and apply any cheating strategy on their systems, including entangling them with some ancilla that they may store in memory to be accessed at will. The aim of the malicious agents is to break the anonymity or security of the protocol.

In addition to public quantum channels between all agents, we require some classical communication channels. More specifically, we assume there are private classical channels between each pair of agents. This can be ensured by each pair of agents sharing a private random string and is a standard assumption if we have malicious agents in a classical network. Furthermore, each agent has access to a broadcast channel, which she can use to send classical information to all other agents. We will use the term simultaneous broadcast when it is required that all agents must broadcast their bit simultaneously, which is an impractical resource as it is hard to ensure in practice. Crucially, we only need a regular (or nonsimultaneous) broadcast channel in our anonymous quantum communication protocol; all the subprotocols that we use remove the requirement of simultaneous broadcasting.

Anonymous classical protocols.—We start by providing the details of a few known anonymous classical protocols, some of which we will use directly. First, there exists a classical private protocol from Ref. [5], LOGICALOR, where each agent inputs a single bit and the protocol computes the logical OR of these bits. This protocol has correctness in that if the input of all agents is 0, the protocol always outputs the correct answer (i.e., 0). If any agent inputs 1, this protocol succeeds (i.e., outputs 1) with probability $1–2^{-S}$ after S rounds. Privacy here means that only the agent can know their input. LOGICALOR is built using another protocol PARITY [5], which privately computes the parity of the input string; however, contrary to the PARITY protocol, LOGICALOR does not require a simultaneous broadcast channel. Further details of both protocols are given in the Supplemental Material [12].

We will use the LOGICALOR protocol in order to create the functionality RANDOMBIT, given in Protocol 1, which allows the sender to anonymously choose a random bit according to some probability distribution D. The correctness and privacy of RANDOMBIT follow directly from the properties of LOGICALOR, namely the only thing the malicious agents learn is the bit chosen by the sender, but not who the sender is. We then extend the RANDOMBIT functionality to define a RANDOMAGENT functionality, where the sender privately picks a random agent by performing the RANDOMBIT protocol $\log_2 n$ times.

Protocol 1. RANDOMBIT

Input: all: parameter S. Sender: distribution D.
Goal: sender chooses a bit according to D.

1. The agents pick bits $\{x_i\}_{i=1}^n$ as follows: the sender picks bit x_i to be 0 or 1 according to distribution D; all other agents pick $x_i = 0$.
2. Perform the LOGICALOR protocol with input $\{x_i\}_{i=1}^n$ and security parameter S and output its outcome.

Last, we need the NOTIFICATION functionality [5], given in Protocol 2, where the sender anonymously notifies an agent as the receiver. Note that we use the same security parameter S throughout for simplicity; however, this is not required. As we explicitly call on this in our main protocol, we describe it below.

Protocol 2. NOTIFICATION [5]

Input: security parameter S, sender's choice of receiver is agent r.
Goal: sender notifies receiver.

1. For each agent i:
   a. Each agent $j \neq i$ picks p_j as follows: if $i = r$ and agent j is the sender, then $p_j = 1$ with probability $\frac{1}{2}$ and $p_j = 0$ with probability $\frac{1}{2}$. Otherwise, $p_j = 0$. Let $p_i = 0$.
   b. Run the PARITY protocol with input $\{p_i\}_{i=1}^n$, with the following differences: agent i does not broadcast her value, and they use a regular broadcast channel rather than simultaneous broadcast. If the result is 1, then $y_i = 1$.
   c. Repeat steps 1(a) and 1(b) S times. If the result of the PARITY protocol is never 1, then $y_i = 0$.
2. If agent i obtained $y_i = 1$, then she is the receiver.

Anonymous entanglement with perfect trusted GHZ states.—In addition to the previous classical protocols, we will need the ANONYMOUS ENTANGLEMENT protocol from Ref. [6], given in Protocol 3. Here, it is assumed that the agents share a state which in the honest case is the GHZ state, and that the sender and the receiver know their respective identities. It is not hard to see that assuming the initial state is a perfect GHZ state, then the protocol creates an EPR pair between the sender and the receiver perfectly anonymously.

Protocol 3. ANONYMOUS ENTANGLEMENT [6]

Input: n agents share a GHZ state.
Goal: EPR pair shared between the sender and the receiver.

1. Each agent, apart from the sender and the receiver, applies a Hadamard transform to their qubit. They measure in the computational basis and broadcast their outcome.
2. The sender first picks a random bit b, broadcasts it, and applies a phase flip σ_z only when $b = 1$.
3. The receiver picks a random bit b', broadcasts it, and applies a phase flip σ_z only when the parity of everyone else's broadcasted bits is 1.

Efficient verification of GHZ states.—The last ingredient we use is the VERIFICATION protocol for GHZ states from the work of Pappa *et al.* [11] that was also implemented for three- and four-party GHZ states in McCutcheon *et al.* [13]. There, one of the agents, the verifier, would like to verify how close the shared state is to the ideal state. Let k be the number of honest agents. The verification protocol is then given in Protocol 4.

Protocol 4. VERIFICATION [11,13]

Input: n agents share state $|\Psi\rangle$.
Goal: GHZ verification of $|\Psi\rangle$ for k honest agents.

1. The verifier generates random angles $\theta_j \in [0, \pi)$ for all agents including themselves ($j \in [n]$), such that $\sum_j \theta_j$ is a multiple of π. The angles are then sent out to all the agents in the network.
2: Agent j measures in the basis $\{|+_{\theta_j}\rangle, |-_{\theta_j}\rangle\} = \{(1/\sqrt{2})(|0\rangle + e^{i\theta_j}|1\rangle), (1/\sqrt{2})(|0\rangle - e^{i\theta_j}|1\rangle)\}$ and sends the outcome $Y_j = \{0, 1\}$ to the verifier.
3: The state passes the verification test when the following condition is satisfied: if the sum of the randomly chosen angles is an even multiple of π, there must be an even number of 1 outcomes for Y_j, and if the sum is an odd multiple of π, there must be an odd number of 1 outcomes for Y_j. We can write this condition as $\bigoplus_j Y_j = (1/\pi)\sum_j \theta_j \pmod 2$.

From the proofs in Refs. [11] and [13], one can see that the ideal state always passes the verification test, and, more interestingly, a soundness statement can also be proven. As in Ref. [11], we take the ideal n-party state to be $|\Phi_0^n\rangle$, given by

$$|\Phi_0^n\rangle = \frac{1}{\sqrt{2^{n-1}}}\left(\sum_{\Delta(y)=0(\mathrm{mod}\,4)} |y\rangle - \sum_{\Delta(y)=2(\mathrm{mod}\,4)} |y\rangle\right),$$

where $\Delta(y) = \sum_i y_i$ denotes the Hamming weight of the classical n-bit string y. This state is equivalent to the GHZ state up to local unitaries. Analogous to Refs. [11,13], to measure the quality of the state $|\Psi\rangle$ shared between the n agents, we take a fidelity measure given by $F'(|\Psi\rangle) = \max_U F(U|\Psi\rangle, |\Phi_0^n\rangle)$, where U is any unitary operation on the space of the malicious agents. This reflects the fact that we are concerned with certifying the state up to operations on the malicious parts, since these are in any case out of the control of the honest agents. Then, even assuming the malicious agents apply their optimal cheating strategy, the probability of passing the test with the state $|\Psi\rangle$, denoted by $P(|\Psi\rangle)$, satisfies $F'(|\Psi\rangle) \geq 4P(|\Psi\rangle) - 3$ [11,13]. Note that this holds even if the shared state is mixed; however, as we will see later, a clever malicious source will always create pure states.

For our purposes, we will use below a version of this verification protocol that is similar to the Symmetric Verification protocol in Ref. [11]. There, it was shown that with the use of a trusted common random string it was possible for all agents to take random turns verifying the validity of the GHZ state. This leads to the guarantee that if the state is accepted a large number of times before the agents decide to use it, then with high probability, when the state is used it should be very close to the correct one.

Anonymity for realistic quantum networks.—All the quantum protocols we have seen that are used to achieve anonymity assume perfect operations and achieve perfect anonymity. In practice, of course, no operation can be perfect and hence perfect anonymity is unattainable. Nevertheless, it is still possible to define an appropriate notion of anonymity that is relevant for practical protocols.

We define the notion of an $\epsilon-$ *anonymous* protocol, where for any number $n - k$ of malicious agents out of n agents in total, the malicious agents, even when they have in their possession the entire quantum state that corresponds to the protocol, can only guess who the sender is (even when the receiver is malicious) or who the receiver is, with probability that is bounded by $(1/k) + \epsilon$. The perfect anonymity is defined when ϵ is equal to 0.

Efficient anonymous quantum message transmission.—We will now show how to devise an efficient ϵ-anonymous protocol for quantum message transmission. For simplicity, we assume there is only one sender. If not, the agents can run a simple classical protocol in the beginning of the protocol in order to deal with collisions (multiple senders) and achieve the unique sender property. See also Refs. [5] and [6] for details.

Moreover, for simplicity we will describe a protocol where we distribute one EPR pair between the sender and the receiver. Then one can perform anonymous teleportation of the classical measurement results, using in particular the FIXED ROLE ANONYMOUS MESSAGE TRANSMISSION functionality as was described in Ref. [5]. In case we want to increase the fidelity of the transmitted quantum message, we can further use the subroutines from Brassard *et al.* [10] which first create a number of nonperfect EPR pairs, then distill one pair and then perform the teleportation. Given that our main contribution is the efficient anonymous

protocol for the GHZ verification, we do not provide here these details that are explained in Ref. [5].

Our scheme is outlined in Protocol 5.

Protocol 5. ϵ-ANONYMOUS ENTANGLEMENT DISTRIBUTION

Input: security parameter S.
Goal: EPR pair created between the sender and the receiver with ϵ-anonymity.

1. The sender notifies the receiver:
   The agents run the NOTIFICATION protocol.
2. GHZ state generation:
   The source generates a state $|\Psi\rangle$ and distributes it to the agents.
3. The sender anonymously chooses verification or anonymous entanglement:
   a. The agents perform the RANDOMBIT protocol, with the sender choosing her input according to the following probability distribution: she flips S fair classical coins, and if all coins are heads, she inputs 0, else she inputs 1. Let the outcome be x.
   b. If $x = 0$, the agents run ANONYMOUS ENTANGLEMENT, else if $x = 1$:
      i. Run the RANDOMAGENT protocol, where the sender inputs a uniformly random $j \in [n]$, to get output j.
      ii. Agent j runs the VERIFICATION protocol as the verifier, and if she accepts the outcome of the test they return to step 2, otherwise the protocol aborts.

If at any point in the protocol, the sender realizes someone does not follow the protocol, she stops behaving like the sender and behaves as any agent.

We are now ready to analyze the above protocol. First, note that if the state is a perfect GHZ state and the operations of the honest agents are perfect, then the anonymity of the protocol is perfect.

In step 1, the agents run the NOTIFICATION protocol which is perfectly anonymous. In the second step, the GHZ state is shared between the agents, which does not affect the anonymity. Note that the role of the source can be played by an agent, as long as the choice of the agent is independent of who the sender is. In step 3(a), the agents run the RANDOMBIT protocol which is also perfectly anonymous. The analysis of the step 3(b) follows from the analysis of the Symmetric Verification protocol in Ref. [11]. The only difference here is that instead of using a common random string, it is the sender who picks the randomness uniformly. Thus, since the input of the sender completely determines the outcome of the protocol, the sender can immediately see if her choice does not correspond to the outcome, and hence only continues if the randomness is perfectly uniform.

Let C_ϵ be the event that the above protocol does not abort and that the state used for the ANONYMOUS ENTANGLEMENT protocol is such that no matter what operation the malicious agents do to their part, the fidelity of the state with the GHZ state is at most $\sqrt{1-\epsilon^2}$. Then, we prove the following theorem for the honest agents:

Theorem 1: For all $\epsilon > 0$

$$\Pr[C_\epsilon] \leq 2^{-S} \frac{4n}{1-\sqrt{1-\epsilon^2}}. \tag{1}$$

Proof sketch.—As proved in Ref. [11], the optimal cheating strategy of a malicious source, which maximizes the probability of C_ϵ, is to create in each round of the protocol a pure state $|\Psi\rangle$ such that $F'(|\Psi\rangle) = \sqrt{1-\epsilon^2}$.

The probability of event C_ϵ is then given by the probability of the state being used and all the tests being passed in the previous rounds. This in turn will depend on the success probability of RANDOMBIT and if the agent chosen to act as the verifier is honest. Given that a state with $F'(|\Psi\rangle)$ passes the verification protocol with probability $P(|\Psi\rangle)$, we can then determine a bound on $\Pr[C_\epsilon]$ by following the proof in Ref. [11]. The full proof is given in the Supplemental Material [12]. ∎

By taking $S = \log_2[4n/(1-\sqrt{1-\epsilon^2})\delta]$, we have $\Pr[C_\epsilon] \leq \delta$. Let us assume for simplicity that when the event C_ϵ is true, which happens with probability at most δ, the malicious agents can perfectly guess the sender or the receiver. We will now see that when the event C_ϵ is false, which happens with probability at least $1-\delta$, the malicious agents cannot guess the sender or the receiver with probability much higher than a random guess. In other words, there is no strategy for breaking the anonymity of the communication that works much better than simply guessing an honest agent at random.

Note that C_ϵ being false means that the fidelity of the shared state with the GHZ state (up to a local operation on the malicious agents) is at least $\sqrt{1-\epsilon^2}$. By doing enough rounds, we can ensure that the probability of C_ϵ is negligible. Our statement of anonymity is given as follows:

Theorem 2: If the agents share a state $|\Psi\rangle$ such that $F'(|\Psi\rangle) \geq \sqrt{1-\epsilon^2}$, then the probability that the malicious agents can guess the identity of the sender is given by

$$\Pr[\text{guess}] \leq \frac{1}{k} + \epsilon. \tag{2}$$

Proof sketch.—First, we show that when the shared state is close to the GHZ state (up to some operation U on the malicious agents' part of the state), then the fidelity between the final state of the protocol when the sender is agent i, $|\Psi_i\rangle$, and the final state of the protocol when the Sender is agent j, $|\Psi_j\rangle$, is high.

Then, we show that when the fidelity between the states $|\Psi_i\rangle$ and $|\Psi_j\rangle$ is close to 1, the probability that the malicious agents can guess the identity of the sender is close to a random guess. The full proof is given in the Supplemental Material [12].

Finally, we consider the entangled state created anonymously between the sender and the receiver. Although we have not considered a particular noise model, our analysis incorporates a reduced fidelity of $|\Psi\rangle$, the state shared by all the agents at the beginning of the protocol. We can carry this forward to the resulting anonymously entangled state, if we assume all the agents are honest and have followed the protocol. We find that the fidelity of the final entangled state with the EPR pair will be at least the fidelity of $|\Psi\rangle$ with the GHZ state. After the entangled state has been constructed, the sender and the receiver can perform anonymous teleportation of any quantum message $|\phi\rangle$ by anonymously sending a classical message with the teleportation results. Our final statement is then given in Corollary 3.

Corollary 3: Using Protocol 5, we can achieve an ϵ-anonymous protocol for quantum message transmission.

Discussion.—We have proposed a practical protocol for anonymous quantum communications in the presence of malicious parties and an untrusted source. The verification step is carried out using a protocol that has been experimentally demonstrated [13] and is tolerant to losses and noise by design. Our protocol achieves in this full adversarial scenario an approximate notion of anonymity that we call ϵ-anonymity and which is relevant in the context of realistic quantum networks.

While the scheme in Ref. [10] results in an exponential scaling, their protocol is not easily implementable. Recent work in Ref. [9] provides a protocol for anonymous transmission using the W state rather than the GHZ state. While this is beneficial in terms of robustness to noise, the protocol creates the anonymously entangled state only with a probability $2/n$. Furthermore, the security analysis considers only the semiactive adversarial scenario, which requires a trusted source.

Our anonymous quantum communication protocol opens the way to the integration and implementation of this fundamental functionality into quantum networks currently under development.

We acknowledge support of the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement No. 820445 (QIA), the ANR through the ANR-17-CE24-0035 VanQuTe and ANR-17-CE39-0005 quBIC projects, the BPI France project RISQ, the EPSRC (UK), and the MIT-France International Science and Technology Initiative.

[1] J. Kimble, Nature (London) **453**, 1023 (2008).
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[3] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Quantum Info. **2**, 16025 (2016).
[4] A. Gheorghiu, T. Kapourniotis, and E. Kashefi, Theory Comput. Syst. **63**, 715 (2019).
[5] A. Broadbent and A. Tapp, in *Advances in Cryptology – ASIACRYPT 2007*, edited by K. Kurosawa, Lecture Notes in Computer Science, Vol. 4833 (Springer, Berlin, Heidelberg, 2007), pp. 410–426.
[6] M. Christandl and S. Wehner, in *Advances in Cryptology – ASIACRYPT 2005*, edited by B. Roy, Lecture Notes in Computer Science, Vol. 4833 (Springer, Berlin, Heidelberg, 2005), pp. 217–235.
[7] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory, and Conceptions of the Universe*, edited by M. Kafatos (Kluwer, Dordrecht, 1989), pp. 69–72.
[8] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[9] V. Lipinska, G. Murta, and S. Wehner, Phys. Rev. A **98**, 052320 (2018).
[10] G. Brassard, A. Broadbent, J. Fitzsimons, S. Gambs, and A. Tapp, in *Advances in Cryptology – ASIACRYPT 2007*, edited by K. Kurosawa, Lecture Notes in Computer Science, Vol. 4833 (Springer, Berlin, Heidelberg, 2007), pp. 460–473.
[11] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis, Phys. Rev. Lett. **108**, 260502 (2012).
[12] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.122.240501 for anonymous classical subroutines Parity and LogicalOR, and proofs of Theorems 1 and 2.
[13] W. McCutcheon, A. Pappa, B. A. Bell, A. McMillan, A. Chailloux, T. Lawson, M. Mafu, D. Markham, E. Diamanti, I. Kerenidis *et al.*, Nat. Commun. **7**, 13251 (2016).