Random-Receiver Quantum Communication

Some Sankar Bhattacharya,[1,*] Ananda G. Maity,[2] Tamal Guha,[3] Giulio Chiribella,[1,4] and
Manik Banik[5]

[1]*Department of Computer Science, The University of Hong Kong, Pokfulam Road, Hong Kong*

[2]*S.N. Bose National Center for Basic Sciences, Block JD, Sector III, Salt Lake, Kolkata 700098, India*

[3]*Physics and Applied Mathematics Unit, Indian Statistical Institute, 203 B.T. Road, Kolkata 700108, India*

[4]*Department of Computer Science, University of Oxford, Wolfson Building, Parks Road, Oxford, United Kingdom*

[5]*School of Physics, IISER Thiruvanathapuram, Vithura, Kerala 695551, India*

We introduce the task of random-receiver quantum communication, in which a sender transmits a quantum message to a receiver selected from a list of *n* spatially separated parties. At the moment of transmission, the choice of receiver is unknown to the sender. Later, it becomes known to the *n* parties, who coordinate their actions by exchanging classical messages. In normal conditions, random-receiver quantum communication requires a noiseless quantum communication channel between the sender and each of the *n* receivers. In contrast, we show that random-receiver quantum communication can take place through noisy, entanglement-breaking channels if the order of such channels is coherently controlled by a quantum bit that is accessible through measurements. While this phenomenon is achieved with a single control qubit, it cannot be mimicked by adding a noiseless qubit channel from the sender to any of the receivers, or more generally, from the sender to any subset of $k < n$ parties.

I. INTRODUCTION

The point-to-point transmission of quantum messages from a sender to a receiver is the cornerstone of quantum communication. When the identity of the receiver is known, this task can be achieved with a reliable quantum communication channel between the sender and the receiver. But what if the identity of the receiver is unknown at the moment of transmission? This situation is relevant to delegated quantum computation [1–5], where a client sends quantum states to a server, which is then required to perform a quantum computation on them. *A priori*, several servers could be available, and the client may not know in advance which server will be assigned the computation. In this situation, it is convenient to have a way to transmit the message simultaneously to all potentially available servers, so that, once one of them is assigned the computation, the designated server is able to retrieve the message and to operate on it. We call this task *random-receiver quantum communication.*

Random-receiver quantum communication can be described as follows. A sender, labeled as *A*, is connected to *n* spatially separated parties $(B_i)_{i=1}^n$ through *n* communication channels $(\mathcal{C}_i)_{i=1}^n$, as illustrated in Fig. 1. The sender wants to transmit a quantum message to one of the parties, say the *x*th party, for some $x \in \{1, \ldots, n\}$. However, the identity of such party (i.e., the value of *x*) is unknown at the moment of transmission. After the transmission has taken place, the value of *x* is decided. For example, the *n* parties could communicate classically to each other and decide which of them should receive the message and act upon it. In the following, we assume that, after the value of *x* has been decided, all the *n* parties know the value of *x* and cooperate in order to let the message reach party B_x. To coordinate their actions, the parties are allowed to exchange classical messages. We say that a communication protocol is successful if it reliably transmits an arbitrary quantum state for arbitrary values of $x \in \{1, \ldots, n\}$.

Besides the application to delegated quantum computing, random-receiver quantum communication is interesting for foundational reasons. At the most basic level, the transmission of quantum states to multiple receivers has a nontrivial relation with the no-cloning theorem [6,7], which forbids trivial protocols where the sender makes many copies of the message and sends one copy to each receiver. Random-receiver quantum communication is also
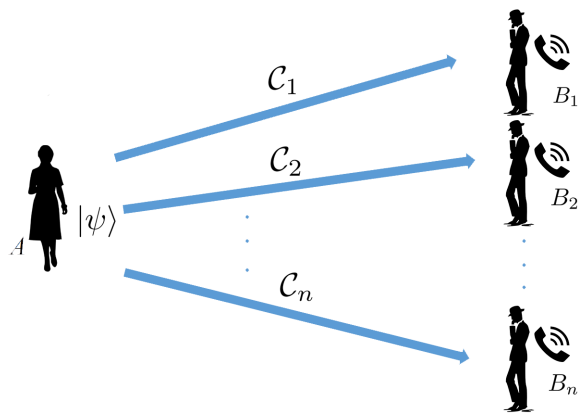

FIG. 1. Random-receiver quantum communication. The sender A wants to transmit a quantum message to one of n receivers $(B_i)_{i=1}^n$. The identity of the designated receiver B_x is unknown at the moment of transmission. After the designated receiver B_x is revealed, the other receivers cooperate with B_x in order to transfer the message to its laboratory. The receivers are allowed to coordinate their actions through classical communication, while quantum communication among them is forbidden.
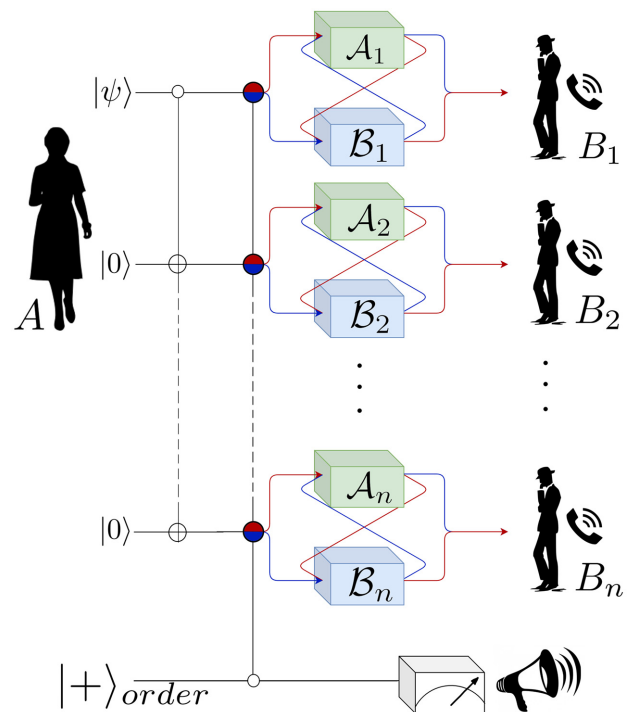

FIG. 2. Random-receiver quantum communication through noisy channels. Perfect protocol with entanglement-breaking channels in a superposition of orders. Alice encodes the unknown qubit state ψ in an n-partite GHZ state and sends it through the noisy channels. An *order qubit* controls the order in which the subsystems pass through noisy channels, i.e., either $\mathcal{A}_i$ before $\mathcal{B}_i$, or $\mathcal{B}_i$ before $\mathcal{A}_i$, for all $i \in \{1, \ldots, n\}$. When the order qubit is prepared a superposition of the two classical states $|0\rangle$ and $|1\rangle$, the channels are executed in a coherent superposition of these two orderings. The goal of the protocol is to transfer a generic state $|\psi\rangle$ from the sender to one of the n receivers (in this picture, receiver B_1). To achieve this goal, local measurements are performed on the order qubit and on all the qubits other than the qubit of the designated receiver B_1. The measurement outcomes are then communicated to B_1, who performs a correction operation that retrieves Alice's message without error.

related to the task of quantum summoning [8–13], where a quantum message has to be revealed at a given set of spacetime points. The crucial difference is that summoning includes fundamental limits on the exchange of signals induced by the causal structure of the underlying spacetime. As a consequence, if a party can communicate to another then it can transmit both classical and quantum messages. In contrast, random-receiver quantum communication only includes limits on the ability to send quantum messages, while no restriction is imposed on the ability to send classical messages.

Perhaps less expectedly, random-receiver quantum communication also turns out to have implications for the study of indefinite causal order in quantum mechanics [14–18]. Consider a scenario where each receiver is connected to the sender by a pair of noisy channels, say channels $\mathcal{A}_i$ and $\mathcal{B}_i$ for the ith receiver. Suppose that the two channels can act in two alternative orders, $\mathcal{A}_i \mathcal{B}_i$ and $\mathcal{B}_i \mathcal{A}_i$, and that their order is coherently controlled by a qubit, called the *order qubit*, in the thought experiment known as the quantum SWITCH [15,17]. In this scenario, illustrated in Fig. 2, we show that perfect random-receiver communication is possible even if all the channels $(\mathcal{A}_i, \mathcal{B}_i)_{i=1}^n$ have zero capacity to transmit quantum information. This counterintuitive phenomenon is made possible by the correlations between the order qubit and the output of the channels, which enable random-receiver quantum communication using classical information about the outcome of a binary measurement on the control system.

Our results show that a single qubit controlling the causal order can unlock quantum communication to a randomly chosen receiver. Remarkably, this unlocking effect cannot be reproduced by replacing the access to the control qubit with a constant number of side channels from the sender to the receivers, as illustrated in Fig. 3. In this scenario, a side channel to receiver B_i can be used to "smuggle" information directly to receiver B_i, bypassing the noisy channels $\mathcal{A}_i$ and $\mathcal{B}_i$. While this approach can trivially transfer information to a known receiver, we show that it cannot achieve random receiver quantum communication, unless the sender is provided with one side channel for every receiver, and each of these side channels permits the faithful transmission of one qubit.

Comparing the quantum SWITCH with the side-channel scenario of Fig. 3, one can see that the access to the order qubit is a more powerful resource than the access to $n - 1$
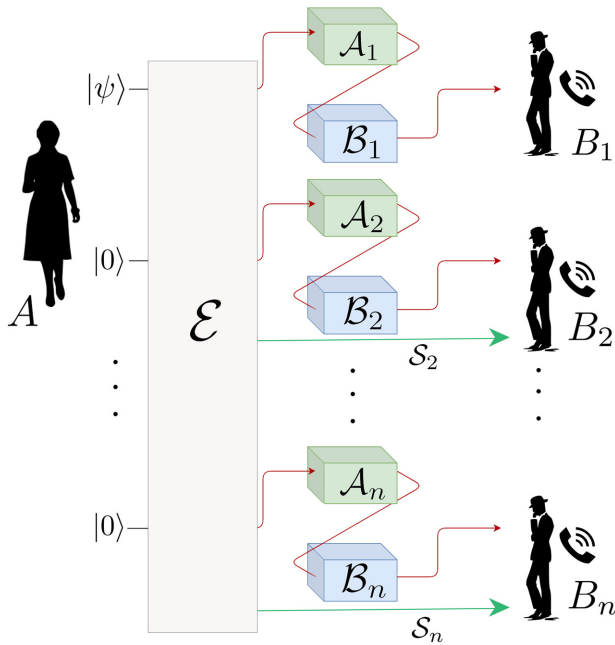
FIG. 3. Random-receiver quantum communication with $k < n$ noiseless side channels. Alice communicates to the n receivers through entanglement-breaking channels in a fixed order, with the assistance of $k < n$ noiseless qubit channels, transferring quantum information from her lab to the labs of the k receivers. In the figure, $k = n - 1$ and the k side channels reach receivers $B_2, \ldots, B_n$. Despite the assistance of the noiseless side channels, random-receiver quantum communication cannot be accomplished when the designated receiver is B_1.

qubit side channels. This observation indicates that the communication advantages of the quantum SWITCH are not trivially due to use of the order qubit as a noiseless side channel that delivers messages to the receivers by bypassing the noisy channels placed between them and the sender.

A. Protocol using noiseless qubit channels

To get insights into the task of random-receiver quantum communication, it is useful to consider first the scenario where the quantum message is a qubit, and all the channels from the sender to the receivers are noiseless. In this setting, one has the following simple protocol. To transmit the quantum state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$, the sender encodes it into the generalized Greenberger-Horne-Zeilinger (GHZ) state $|\psi_n\rangle := \alpha|0\rangle^{\otimes n} + \beta|1\rangle^{\otimes n}$. Then, the sender sends the n qubits to the n receivers. To let party B_x retrieve the message, each of the other $n - 1$ parties performs a measurement on the Fourier basis $\{|+\rangle, |-\rangle\}$, $|\pm\rangle := (|0\rangle \pm |1\rangle)/\sqrt{2}$, collapsing the state of party B_x to $|\psi_s\rangle := \alpha|0\rangle + (-1)^s\beta|1\rangle$, where $s := \sum_{y \neq x} o_y$ is the sum of the measurement outcomes, o_y being the measurement outcome obtained by the yth party. Finally, the $n - 1$ parties communicate their outcomes to B_x, who performs

the correction operation Z^s, with $Z := |0\rangle\langle 0| - |1\rangle\langle 1|$. It is easy to see that party B_x eventually receives the quantum state $|\psi\rangle$ without any error. All together, this protocol requires 1 qubit of quantum communication from the sender to each receiver.

B. Conditions for random-receiver quantum communication

Suppose now that the quantum channels from the sender to the receivers are general noisy channels. For protocols involving a single round of classical communication to the chosen receiver, we show that perfect random-receiver quantum communication is possible only if each of the channels $(\mathcal{C}_i)_{i=1}^n$ can transfer at least one qubit without errors.

Theorem 1. *Every one-way protocol for random-receiver communication of a d-dimensional quantum message requires each of the channels $(\mathcal{C}_i)_{i=1}^n$ to have a quantum capacity of at least* $\log d$ *qubits.*

The proof is provided in Appendix A.

Theorem 1 implies that the simple noiseless protocol presented in the previous section is already optimal in terms of quantum communication cost.

As a special case, Theorem 1 implies that random-receiver quantum communication cannot take place when some of the channels $(\mathcal{C}_i)_{i=1}^n$ are entanglement breaking [19,20]. We recall that entanglement-breaking channels are of the measure-and-prepare form $\mathcal{C}(\rho) = \sum_j \text{Tr}[M_j \rho]\rho_j$, where (M_j) is a quantum measurement and $\{\rho_j\}$ is a set of output states [21]. Entanglement-breaking channels are the prototype of channels with zero quantum capacity, and therefore they cannot achieve random-receiver quantum communication. As it turns out, the impossibility of random-receiver quantum communication with entanglement-breaking channels holds not only for one-way protocols, but also for protocols involving arbitrarily many rounds of local operations and classical communication (LOCC) (see Appendix B).

In the rest of the paper, we focus on the scenario where *all* channels are entanglement breaking, and ask which additional resources should be added in order to enable random-receiver quantum communication. In the basic model of Fig. 1, we replace each entanglement-breaking channel $\mathcal{C}_i$ with a new channel $\mathcal{C}_i \otimes \mathcal{S}_i$, where $\mathcal{S}_i$ is an additional channel from the sender to the ith receiver. For simplicity, we assume that each side channel $\mathcal{S}_i$ outputs a quantum system of dimension d, equal to the dimension of the quantum message. In this setting, we prove that random-receiver communication is possible if and only if each side channel has maximal capacity, that is, if and only if each side channel can faithfully transmit $\log d$.

Theorem 2. *Random-receiver quantum communication with entanglement-breaking channels $(\mathcal{C}_i)_{i=1}^n$ and side channels $(\mathcal{S}_i)_{i=1}^n$ with d-dimensional output is possible if and only if all side channels have a capacity of $\log d$ qubits.*

The proof is provided in Appendix B. In particular, Theorem 2 shows that random-receiver quantum communication with entanglement-breaking channels is impossible even if one provides perfect side channels to any finite number $k < n$ of receivers.

C. Random-receiver quantum communication through the quantum SWITCH

We now show a protocol that exploits indefinite causal order to achieve random-receiver quantum communication even if all the channels from the sender to the n receivers are entanglement breaking. Let $\mathcal{A} := \bigotimes_{i=1}^n \mathcal{A}_i$ and $\mathcal{B} := \bigotimes_{i=1}^n \mathcal{B}_i$ be two quantum channels, describing the noise experienced by the data transmitted by a sender to n receivers. The action of the channels $\mathcal{A}$ and $\mathcal{B}$ in a superposition of two alternative orders is described by the quantum SWITCH [15,17], a higher-order map that transforms the pair of channels $(\mathcal{A}, \mathcal{B})$ into a new quantum channel $\mathcal{S}(\mathcal{A}, \mathcal{B})$, involving a control qubit that determines the order of application of channels $\mathcal{A}$ and $\mathcal{B}$. In its simplest version, the quantum SWITCH produces the channel $\mathcal{S}(\mathcal{A}, \mathcal{B})$ with Kraus operators

$$S_{jk} := A_j B_k \otimes |0\rangle\langle 0| + B_k A_j \otimes |1\rangle\langle 1|, \qquad (1)$$

where $\{A_j\}$ and $\{B_k\}$ are Kraus representations for channels $\mathcal{A}$ and $\mathcal{B}$, respectively. It is easy to verify that the definition of channel $\mathcal{S}(\mathcal{A}, \mathcal{B})$ is independent of the choice of Kraus representations.

When the order qubit is initialized in the state ω, we use the shorthand $\mathcal{S}_\omega(\mathcal{A}, \mathcal{B})(\rho) := \mathcal{S}(\mathcal{A}, \mathcal{B})(\rho \otimes \omega)$ and we call $\mathcal{S}_\omega(\mathcal{A}, \mathcal{B})$ the *switched channel*. Note that, in order for the switched channel to exhibit an interesting behavior, the Kraus operators of the two channels $\mathcal{A}$ and $\mathcal{B}$ should exhibit some amount of noncommutativity: if all the Kraus operators A_j and B_k were to commute then the switched channel would simply be $\mathcal{S}_\omega = \mathcal{A}\mathcal{B} \otimes \omega$.

When $\mathcal{A}$ and $\mathcal{B}$ are products of Pauli channels, the switched channel has the simple expression

$$\mathcal{S}_\omega(\mathcal{A}, \mathcal{B}) = p_+ \mathcal{C}_+ \otimes \omega_+ + p_- \mathcal{C}_- \otimes \omega_-, \qquad (2)$$

where (p_+, p_-) are two probabilities, $\omega_+ := \omega$ and $\omega_- := Z\omega Z$ are states of the order qubit, and $(\mathcal{C}_+, \mathcal{C}_-)$ are two quantum channels (see Appendix C for the explicit expression). In the following, we focus on the case where all channels $(\mathcal{A}_i)_{i=1}^n$ and $(\mathcal{B}_i)_{i=1}^n$ are equal to the Pauli channel $\mathcal{N}_{XY}$, defined by $\mathcal{N}_{XY}(\rho) = \frac{1}{2}(X\rho X + Y\rho Y)$. This channel is entanglement breaking and therefore cannot directly transmit quantum information. However, the use of this

channel in a superposition of orders achieves perfect quantum communication to a single receiver [22]. In the following, we show that perfect quantum communication can also be achieved by an arbitrary receiver, chosen from a list of $n \geq 2$ candidates.

For simplicity, we illustrate the idea for $n = 2$. First, the sender encodes the message $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ into the state $|\psi_2\rangle := \alpha|0\rangle|0\rangle + \beta|1\rangle|1\rangle$, as in the noiseless protocol. Then, the sender sends the two qubits to receivers 1 and 2, using the channels $\mathcal{A} = \mathcal{N}_{XY} \otimes \mathcal{N}_{XY}$ and $\mathcal{B} = \mathcal{N}_{XY} \otimes \mathcal{N}_{XY}$ in a superposition of orders. When the order qubit is initialized in the state $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, the channels $\mathcal{C}_\pm$ in Eq. (2) are

$$\mathcal{C}_+(\rho) = \frac{\rho + (Z \otimes Z)\rho(Z \otimes Z)}{2},$$
$$\mathcal{C}_-(\rho) = \frac{(I \otimes Z)\rho(I \otimes Z) + (Z \otimes I)\rho(Z \otimes I)}{2}, \qquad (3)$$

and the probabilities $p_\pm$ are both equal to $\frac{1}{2}$. The output states of the order qubit are either $\omega_+ = |+\rangle\langle +|$ or $\omega_- = |-\rangle\langle -|$, with $|-\rangle := (|0\rangle - |1\rangle)/\sqrt{2}$. Since these two states are orthogonal, a measurement on the order qubit postselects one of the two channels $\mathcal{C}_+$ or $\mathcal{C}_-$. Moreover, the channels $\mathcal{C}_+$ and $\mathcal{C}_-$ are equivalent under local unitary operations: for example, party 1 can turn channel $\mathcal{C}_-$ into channel $\mathcal{C}_+$ by applying the Pauli gate Z on its qubit. If the outcome of the measurement on the order qubit is shared to the two receivers, they can ensure that their qubits have gone through the channel $\mathcal{C}_+$. Now, the pure state $\rho = |\psi_2\rangle\langle\psi_2|$ is invariant under the action of channel $\mathcal{C}_+$, and therefore it reaches the two receivers without any error. Hence, the two receivers end up with two qubits in the same state as in the noiseless protocol, and can achieve random-receiver quantum communication. Summarizing, classical communication of the outcome of a measurement on the order qubit enables perfect random-receiver quantum communication.

The above protocol can be generalized from $n = 2$ to arbitrary numbers of receivers, as shown in Appendix D. The crucial feature of the protocol is that access to a single qubit (the order qubit) is enough to unlock quantum communication to n independent receivers. This feature cannot be reproduced by adding a qubit side channel in a causally ordered scenario. In fact, Theorem 2 implies that random-receiver quantum communication is impossible even if one adds any number $k < n$ of qubit side channels. In short, the mere access to the order qubit is a more powerful resource than the access to $n - 1$ qubit side channels.

D. Generalization to multiqubit quantum communication

The protocol for random-receiver quantum communication with assistance of the quantum SWITCH can also be

used for the transmission of multiqubit entangled states. Suppose that the sender wants to transmit an m-qubit system to m receivers, chosen from a list of n candidate receivers. By applying the basic protocol, the sender can transmit one qubit to any of the n candidate receivers. Now, suppose that the protocol is performed independently on each of the input qubits, thus sending each of them to one of the n possible receivers. The net result is that the whole m-qubit state is transmitted to an arbitrary list of designated receivers, as one can infer from the linearity of quantum evolutions, in a similar way as it is done in the analysis of quantum teleportation [23]. In this way, it is possible to send the m qubits to m receivers, or, more generally, to send k disjoint subsets of the m qubits to k receivers.

The above protocol could be used for distributing entanglement in a network of quantum computers. This application is potentially appealing because shared entanglement among the nodes of a quantum network can be used to achieve nonlocal computation [24–26]. In this scenario, our protocol can be used to generate multiqubit entangled states on demand, as they become needed during the run of a quantum computation. The alternative would be to generate all the entangled resources before the computation starts, and store them in a quantum memory. Treating entanglement as an offline resource, however, is practically challenging, because quantum memories have a limited lifetime and are likely to be costly to maintain. In addition, it may not be known in advance which servers will perform a certain part of the computation, and, providing all servers with all the necessary entanglement resources may not be an efficient approach in general. In comparison, our protocols allows one to generate entanglement during the run of the computation, and to distribute entanglement only to those subsets of the servers that are expected to carry out the next computational step.

E. Discussion

Quantum communication with the assistance of the quantum SWITCH is similar to quantum communication with classical assistance from the environment [27–30]. In both cases, the access to a measurement outcome unlocks some quantum information that would be inaccessible otherwise. The analogy goes even further, because the quantum SWITCH of two channels $\mathcal{A}$ and $\mathcal{B}$ is an *extension* of the quantum channel $\frac{1}{2}(\mathcal{A}\mathcal{B} + \mathcal{B}\mathcal{A})$. Precisely, the channel $\frac{1}{2}(\mathcal{A}\mathcal{B} + \mathcal{B}\mathcal{A})$ can be obtained from the switched channel $\tilde{\mathcal{S}}_{|+\rangle\langle+|}(\mathcal{A}, \mathcal{B})$ by discarding the order system. From this point of view, the order qubit is indeed part of the environment of the channel $\frac{1}{2}(\mathcal{A}\mathcal{B} + \mathcal{B}\mathcal{A})$, and quantum communication with the assistance of the quantum SWITCH is a special case of quantum communication with classical assistance from the environment. The key difference is that, in the case of the quantum SWITCH, only a small part of the environment needs to be accessible, while in the

other examples of quantum communication with the assistance of environment it is generally assumed that the whole environment be accessible.

Another class of communication protocols that exhibit similarities with the quantum SWITCH are the communication protocols using controlled operations before and after the communication channels [31]. Like the quantum SWITCH, these protocols use a control qubit, which determines the choice of operations performed on the input and output of the communication channels. The key difference with the quantum SWITCH is that such protocols generally transfer information to the control system in a way that bypasses the original channels [32,33]. In contrast, in all the protocols considered in the literature, the quantum SWITCH does not deposit information into the order qubit. For protocols involving Pauli channels, this feature is evident from Eq. (2), where the states $\omega_\pm$ of the order qubit are independent of the message, and so are their probabilities $p_\pm$ (see Appendix C for the explicit expression).

Here we observe that, if we allow arbitrary controlled operations before and after the noisy channels then protocols for random-receiver quantum communication with entanglement-breaking channels can be constructed also in the causally ordered scenario. This is because controlled operations can be used (i) to transfer information directly from the message to the control qubit, bypassing the noisy channels $\mathcal{A}$ and $\mathcal{B}$, and (ii) to generate the generalized GHZ state $\alpha|0\rangle^{\otimes n} + \beta|1\rangle^{\otimes n}$ from the state of the control qubit, evading the locality restriction that affects the receivers. An example of a protocol that achieves random-receiver communication through controlled operations in a definite causal order is presented in Appendix E.

The possibility of random-receiver quantum communication through controlled operations in a definite order can be interpreted in two ways. On the one hand, controlled operations can generate entanglement among the n receivers, and therefore appear to be too powerful to be interesting in the problem of random-receiver quantum communication, where locality in space is an essential constraint.

On the other hand, controlled operations bear some similarity with the quantum SWITCH, which can be regarded as a controlled-SWAP operation *in time*. Controlled-SWAP operations and, more generally, controlled permutations, are a special subset of the set of all controlled operations, and one may wonder whether this special subset can reproduce the features of the quantum SWITCH. Interestingly, the answer is negative: in Appendix E we show that no controlled permutations of the inputs and outputs of channels $\mathcal{A}$ and $\mathcal{B}$ permit random-receiver quantum communication for odd n.

We conclude the discussion by mentioning possible photonic simulations of random-receiver quantum communication. The quantum SWITCH has been reproduced with standard physics in several photonic setups [34–39].

For instance, in the scheme of Ref. [36] the photon's transverse spatial mode behaves as the target system evolving under two quantum operations whose relative order is controlled by the photon's polarization degrees of freedom (DOF). Compared to the existing experiments, the implementation of random-receiver quantum communication through quantum SWITCH is more challenging, because it requires control over the order of multiqubit quantum processes. On the other hand, multiple DOF of a photon, such as polarization, spatial modes, orbital angular momentum, frequency, and time-bin modes, have already been addressed simultaneously in different photonic experiments [40–43]. Using similar techniques, one could consider a first proof-of-principle experiment that simulates random-receiver quantum communication with a single photon. A further approach would be to use multiple photons, e.g., using the polarization degrees of freedom as the target qubits, and to consider their transmissions through a correlated noisy channel, where the order of processes taking place on different photons is perfectly correlated, and controlled, by a single quantum bit.

II. CONCLUSIONS

In this paper we have introduced a quantum communication protocol, called random-receiver quantum communication. Using this protocol, a sender can transmit an arbitrary quantum state to a receiver, chosen from a set of n candidate receivers after the transmission has taken place.

Random-receiver quantum communication has an interesting connection with foundational questions about causal order in quantum mechanics. Specifically, we have shown that random-receiver quantum communication is possible even with highly noisy channels between the sender and the receivers, provided that the order of such noisy channels is coherently controlled by a quantum bit, as in the quantum SWITCH thought experiment [15,17].

Coherent control of the order of quantum processes has recently gained increasing interest, as it finds useful applications in communication tasks [22,44–47]. In this context, a much debated issue is to what extent the communication advantages appearing in these applications are specific to superpositions of causal orders, rather than being generic to other forms of coherent superpositions of communication protocols [22,31–33,48].

A key question is: can the control system alone be used to achieve the desired communication advantages, without involving the superposition of orders? In this respect, our work provides an important contribution. We establish that protocols using the superposition of orders offer an advantage over arbitrary protocols where the order is fixed and a number of side channels connects the sender directly to a subset of $k < n$ receivers, as illustrated in Fig. 3. A special case of this scenario is to have communication protocols where a qubit controls the choice of encoding operations

performed before the noisy channels. Even if the control qubit is sent to one of the receivers, random-receiver quantum communication cannot be achieved when the channels connecting the sender to the other receivers are entanglement breaking. Even more generally, one can consider protocols where multiple qubits control the encoding operations and each of these qubits is sent to a different receiver. No protocol of this kind can achieve random-receiver quantum communication, unless one noiseless qubit is sent to each of the n receivers.

The advantage shown in our paper implies that access to a *single*-qubit system controlling the order of quantum processes is a more powerful resource than $(n − 1)$-qubit side channels for any natural number $n > 1$. The present study also opens up a potential use of indefinite causal order in distributed quantum protocols, such as multipartite quantum state transfer and entanglement distribution [49,50], which are promising for the emerging technology of the quantum internet [51,52].

APPENDIX A: PROOF OF THEOREM 1

The proof uses a general result, expressed in terms of the following definition: for a generic quantum channel $\mathcal{C}_L$ acting on a generic quantum system L, we say that $\mathcal{C}_L$ *can transmit a d-dimensional quantum system in a one-way protocol* if there exists an encoding channel $\mathcal{E}_{LR} : L(\mathbb{C}^d) \to L(\mathcal{H}_L \otimes \mathcal{H}_R)$, a measurement $(P_j)_j$ on system R, and a set of local operations $(\mathcal{D}_j)_j$, with $\mathcal{D}_j : L(\mathcal{H}_L) \to L(\mathbb{C}^d)$, such that $\sum_j \mathrm{Tr}_R[(\mathcal{D}_j \mathcal{C}_L \otimes P_j)\mathcal{E}_{LR}(\rho)] = \rho$ for every state $\rho \in \mathsf{St}(\mathbb{C}^d)$.

Proposition 1. *If channel $\mathcal{C}_L$ can transfer the state of a d-dimensional quantum system in a one-way protocol then channel $\mathcal{C}_L$ has a quantum capacity of at least* $\log d$.

Proof. Defining $\mathcal{E}_j := \mathrm{Tr}_R[(\mathcal{I}_L \otimes P_j)\mathcal{E}_{LR}]$, we obtain the equivalent condition $\sum_j \mathcal{D}_j \mathcal{C}_L \mathcal{E}_j = \mathcal{I}_d$. This condition is satisfied if and only if each term in the sum is proportional to the identity map, namely, $\mathcal{D}_j \mathcal{C}_L \mathcal{E}_j = p_j \mathcal{I}_d$ for some probability distribution $(p_j)_j$. Since $\mathcal{D}_j$ and $\mathcal{C}_L$ are trace preserving, this condition implies that $\mathcal{E}'_j := \mathcal{E}_j / p_j$ is trace preserving. Since the condition $\mathcal{D}_j \mathcal{C}_L \mathcal{E}'_j = \mathcal{I}_d$ holds, there exists a communication protocol, consisting of an encoding channel $\mathcal{E}'_j$ and of a decoding channel $\mathcal{D}_j$, such that a d-dimensional system is transmitted faithfully through $\mathcal{C}_L$. Hence, $\mathcal{C}_L$ has a quantum capacity of at least $\log d$ qubits. ∎

Proof of Theorem 1. Suppose that there exists a one-way protocol for random-receiver quantum communication using channels $(\mathcal{C}_i)_{i=1}^n$, and suppose that the protocol can successfully transfer a d-dimensional quantum system to any of the receivers $(B_i)_{i=1}^n$. Let $\mathcal{E}: L(\mathbb{C}^d) \to L(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n)$ be the encoding channel used in the protocol. For every $x \in \{1, \ldots, n\}$, let $(M_j^{(x)})$ be the measurement performed by the $n-1$ parties other than party x, and let $(\mathcal{B}_j^{(x)})$ be the conditional operations performed by party x. We can then use Proposition 1, defining the systems $L := B_x$ and $R := \bigotimes_{y \neq x} B_y$, and the encoding channel $\mathcal{E}_{LR} := (\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n)\mathcal{E}$ with $\mathcal{F}_y := \mathcal{C}_y$ for $y \neq x$ and $\mathcal{F}_x := \mathcal{I}_x$. Applying Proposition 1 to channel $\mathcal{C}_L := \mathcal{C}_x$, we then find that channel $\mathcal{C}_x$ must have a capacity of at least $\log d$ qubits. Since x is an arbitrary number in $\{1, \ldots, n\}$, every channel in the set $(\mathcal{C}_i)_{i=1}^n$ must have a capacity of at least $\log d$. ∎

APPENDIX B: PROOF OF THEOREM 2

The proof uses a generalization of Proposition 1 to arbitrary separable protocols. For a generic quantum channel $\mathcal{S}_L$ transforming system L into system L', we say that $\mathcal{C}$ *can transmit a d-dimensional quantum system in a separable protocol* if there exists a system R, an encoding channel $\mathcal{E}_{LR}: L(\mathbb{C}^d) \to L(\mathcal{H}_L \otimes \mathcal{H}_R)$, and a separable channel $\mathcal{D}_{LR} = \sum_j \mathcal{L}_j \otimes \mathcal{R}_j$, where $\mathcal{L}_j: L(\mathcal{H}_{L'}) \to L(\mathbb{C}^d)$ and $\mathcal{R}_j: L(\mathcal{H}_R) \to \mathbb{C}$ are completely positive maps for every j, such that

$$\mathcal{D}_{LR}(\mathcal{S}_L \otimes \mathcal{I}_R)\mathcal{E}_{LR} = \mathcal{I}_d, \qquad (B1)$$

where $\mathcal{I}_R$ is the identity channel on system R.

Proposition 2. *If the output of channel $\mathcal{S}_L$ is a d-dimensional quantum system and $\mathcal{S}_L$ can transfer the state of a d-dimensional quantum system in a separable protocol, then $\mathcal{S}_L$ has a capacity of at least* $\log d$ *qubits.*

Proof. Defining $\mathcal{E}_j := [(\mathcal{I}_L \otimes \mathcal{R}_j)\mathcal{E}_{LR}]$, we can rewrite Eq. (B1) as $\sum_j \mathcal{L}_j \mathcal{S}_L \mathcal{E}_j = \mathcal{I}_d$. This condition is satisfied if and only if each term in the sum is proportional to the identity map, namely, $\mathcal{L}_j \mathcal{S}_L \mathcal{E}_j = p_j \mathcal{I}_d$ for some probability distribution $(p_j)_j$. Now, there must exist at least one value of j such that $p_j \neq 0$. Let j_0 be one such value. Since $\mathcal{L}_{j_0}$ and $\mathcal{S}_L \mathcal{E}_{j_0}$ are linear maps from $L(\mathbb{C}^d)$ to itself, the condition $\mathcal{L}_{j_0} \mathcal{S}_L \mathcal{E}_{j_0} = p_{j_0} \mathcal{I}_d$ implies that $\mathcal{S}_L \mathcal{E}_{j_0}$ is invertible, and $\mathcal{L}_{j_0}/p_{j_0}$ is its inverse. Using this fact, one obtains the condition $\mathcal{S}_L \widetilde{\mathcal{E}} = \mathcal{I}_d$, with $\widetilde{\mathcal{E}} := \mathcal{E}_{j_0} \mathcal{L}_{j_0}/p_{j_0}$. Since $\mathcal{S}_L$ is trace preserving, the condition $\mathcal{S}_L \widetilde{\mathcal{E}} = \mathcal{I}_d$ implies that, for every matrix ρ, one has $\mathrm{Tr}[\rho] = \mathrm{Tr}[\mathcal{S}_L \widetilde{\mathcal{E}}(\rho)] = \mathrm{Tr}[\widetilde{\mathcal{E}}(\rho)]$. Hence, the map $\widetilde{\mathcal{E}}$ is trace preserving. Since $\mathcal{E}$ is also completely positive, it is a quantum channel. The condition $\mathcal{S}_L \widetilde{\mathcal{E}} = \mathcal{I}_d$ shows that there exists an encoding channel $\widetilde{\mathcal{E}}$ that can be used to transmit a d-dimensional quantum system through channel $\mathcal{S}_L$. Hence, channel $\mathcal{S}_L$ has a capacity of at least $\log d$. ∎

Proof of Theorem 2. Suppose that there exists a general LOCC protocol for random-receiver quantum communication using n entanglement-breaking channels $(\mathcal{C}_i)_{i=1}^n$ and n side channels $(\mathcal{S}_i)_{i=1}^n$ with d-dimensional outputs. Let $\mathcal{E}: L(\mathbb{C}^d) \to L(\mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_n)$ be the encoding channel used in the protocol, with $\mathcal{H}_i := \mathcal{H}_{B_i} \otimes \mathcal{H}_{S_i}$, where $\mathcal{H}_{B_i}$ is the input of channel $\mathcal{C}_i$ and $\mathcal{H}_{S_i}$ is the input of the side channel $\mathcal{S}_i$.

For every $x \in \{1, \ldots, n\}$, the protocol should accomplish the transmission of a d-dimensional quantum system to the xth receiver using a LOCC decoding protocol. Explicitly, one must have

$$\mathcal{D}_x(\mathcal{C}_1 \otimes \mathcal{S}_1 \otimes \mathcal{C}_2 \otimes \mathcal{S}_2 \otimes \cdots \otimes \mathcal{C}_n \otimes \mathcal{S}_n)\mathcal{E} = \mathcal{I}_x, \quad (B2)$$

where $\mathcal{I}_x$ denotes the identity channel from the initial d-dimensional system to another d-dimensional system $\mathcal{K}_x$ in the laboratory of the xth receiver, and $\mathcal{D}_x$ is a separable decoding channel, of the form

$$\mathcal{D}_x = \sum_j \mathcal{D}_{x,1,j} \otimes \mathcal{D}_{x,2,j} \otimes \cdots \otimes \mathcal{D}_{x,n,j}. \qquad (B3)$$

Here, the map $\mathcal{D}_{x,i,j}$ has input $\mathcal{H}'_i := \mathcal{H}_{B'_i} \otimes \mathcal{H}_{S'_i}$, equal to the tensor product of the output of channel $\mathcal{C}_i$ with the output of channel $\mathcal{S}_i$, denoted by B'_i and S'_i, respectively. The output of the map $\mathcal{D}_{x,i,j}$ is $\mathcal{K}_x$ for $i = x$, and the trivial system for $i \neq x$.

We now apply Proposition 2 with systems $L := S_x$, $L' := S'_x$, and $R := B_x \otimes [\bigotimes_{y \neq x}(B'_y \otimes S'_y)]$, and with channels $\mathcal{S}_L := \mathcal{S}_x$ and $\mathcal{E}_{LR} := (\mathcal{F}_1 \otimes \cdots \otimes \mathcal{F}_n)\mathcal{E}$ with $\mathcal{F}_y := \mathcal{C}_y \otimes \mathcal{S}_j$ for $y \neq x$ and $\mathcal{F}_x := \mathcal{I}_{B_x} \otimes \mathcal{I}_{S_x}$.

The original LOCC protocol can be regarded as a special case of the separable protocol with respect to the bipartition (L, R). To see that, we write down the entanglement-breaking channel $\mathcal{C}_x$ as $\mathcal{C}_x = \sum_t \mathcal{P}_{x,t} \mathcal{M}_{x,t}$, where each

$\mathcal{M}_{x,t}: L(\mathcal{H}_{B_x}) \to \mathbb{C}$ corresponds to an outcome of a measurement, and each map $\mathcal{P}_{x,t}: \mathbb{C} \mapsto L(\mathcal{H}_{B'_x})$ represents the preparation of a quantum state, conditional on the outcome of the measurement. Hence, the quantum channel $\mathcal{D}_x(\mathcal{C}_x \otimes \mathcal{I}_{S'_x})$ has the separable form $\mathcal{D}_x(\mathcal{C}_x \otimes \mathcal{I}_{S'_x}) = \sum_t \mathcal{M}_{x,t} \otimes [\mathcal{C}_x(\mathcal{P}_{x,t} \otimes \mathcal{I}_{S'_x})]$, where the first factor acts on system B_x (which is part of system R) and the second factor acts on system S'_x (which is system L'). Then, substituting the explicit form (B3) for the LOCC decoding $\mathcal{D}_x$ into Eq. (B2), we obtain

$$\begin{aligned}
\mathcal{I}_x &= \mathcal{D}_x(\mathcal{C}_1 \otimes \mathcal{S}_1 \otimes \mathcal{C}_2 \otimes \mathcal{S}_2 \otimes \cdots \otimes \mathcal{C}_n \otimes \mathcal{S}_n)\mathcal{E} \\
&= \sum_{j,t}\{(\mathcal{D}_{x,1,j}\mathcal{F}_1) \otimes (\mathcal{D}_{x,2,j}\mathcal{F}_2) \otimes \cdots \otimes (\mathcal{D}_{x,x-1,j}\mathcal{F}_{x-1}) \\
&\quad \otimes [\mathcal{D}_{x,x,j}(\mathcal{P}_{x,t}\mathcal{M}_{x,t} \otimes \mathcal{S}_x)] \otimes (\mathcal{D}_{x,x+1,j}\mathcal{F}_{x+1}) \\
&\quad \otimes \cdots \otimes (\mathcal{D}_{x,n,j}\mathcal{F}_n)\}\mathcal{E} \\
&= \mathcal{D}_{LR}(\mathcal{S}_x \otimes \mathcal{I}_R)\mathcal{E}_{LR}, \tag{B4}
\end{aligned}$$

having defined

$$\begin{aligned}
\mathcal{D}_{LR} := \sum_j &\underbrace{\mathcal{M}_{x,t} \otimes \mathcal{D}_{x,1,j} \otimes \mathcal{D}_{x,2,j} \otimes \cdots \otimes \mathcal{D}_{x,x-1,j}}_{\text{acting on part of } R} \\
&\otimes \underbrace{\mathcal{D}_{x,x,j}(\mathcal{P}_{x,t} \otimes \mathcal{I}_{S'_x})}_{\text{acting on } L'} \otimes \underbrace{\mathcal{D}_{x,x+1,j} \otimes \cdots \otimes \mathcal{D}_{x,n,j}}_{\text{acting on part of } R}.
\end{aligned}$$
$$\tag{B5}$$

Note that $\mathcal{D}_{LR}$ is a separable channel with respect to the partition L/R. Indeed, since the channel $\mathcal{C}_x$ is entanglement breaking, its action on a generic state can be expressed as $\mathcal{C}_x(\rho) = \sum_k \rho_{x,k} \text{Tr}[P_{x,k}\rho]$, and therefore the map $\mathcal{D}_{x,x,j}(\mathcal{C}_x \otimes \mathcal{I}_{S'_x})$ has the separable form $\mathcal{D}_{x,x,j}(\mathcal{C}_x \otimes \mathcal{I}_{S'_x}) = \sum_k \mathcal{A}_{x,k} \otimes \mathcal{B}_{x,k}$, with $\mathcal{A}_{x,k}(\rho) := \text{Tr}[P_{x,k}\rho]$ and $\mathcal{B}_{x,k}(\rho) := \mathcal{D}_{x,x,j}(\rho_x \otimes \mathcal{I}_{S'_x})$.

Applying Proposition 1, we then find that channel $\mathcal{S}_x$ must have a capacity of at least $\log d$ qubits. Since x is an arbitrary element of $\{1, \dots, n\}$, every channel in the set $(\mathcal{S}_i)_{i=1}^n$ must have a capacity of at least $\log d$ qubits. ∎

APPENDIX C: SWITCHING PRODUCTS OF PAULI CHANNELS

Let $\mathcal{E} := \bigotimes_{k=1}^2 \mathcal{E}_k$ be the product of two Pauli channels, given by $\mathcal{E}_1 \equiv \{p_0\mathbb{I}, p_1 X, p_2 Y, p_3 Z\}$ and $\mathcal{E}_2 \equiv \{q_0\mathbb{I}, q_1 X, q_2 Y, q_3 Z\}$, $\sum_{l=0}^3 p_l^2 = \sum_{l=0}^3 q_l^2 = 1$, respectively, where X, Y, Z are Pauli matrices. If two instances of the quantum channel $\mathcal{E}$ are combined through the quantum SWITCH, the resulting channel is

$$\begin{aligned}
&\mathcal{S}_{\omega_c}^{(2)}(\mathcal{E}, \mathcal{E})[\rho_{B_1 \cdots B_n}] \\
&\quad = \mathcal{C}_+(\rho_{B_1 \cdots B_n}) \otimes \omega_c + \mathcal{C}_-(\rho_{B_1 \cdots B_n}) \otimes Z\omega_c Z, \tag{C1}
\end{aligned}$$

where

$$\begin{aligned}
\mathcal{C}_+(\rho_{B_1 B_2}) = &\left(\sum_{l=0}^3 p_l^2 q_l^2 + p_0^2(1 - q_0^2) + p_1^2(1 - q_1^2) + p_2^2(1 - q_2^2) + p_3^2(1 - q_3^2)\right)[\rho_{B_1 B_2}] \\
&+ 2q_0 \sum_{l=0}^3 p_l^2 \{q_1(\mathbf{I} \otimes X)[\rho_{B_1 B_2}](\mathbf{I} \otimes X) + q_2(\mathbf{I} \otimes Y)[\rho_{B_1 B_2}](\mathbf{I} \otimes Y) + q_3(\mathbf{I} \otimes Z)[\rho_{B_1 B_2}](\mathbf{I} \otimes Z)\} \\
&+ 2p_0 \sum_{l=0}^3 q_l^2 \{p_1(X \otimes \mathbf{I})[\rho_{B_1 B_2}](X \otimes \mathbf{I}) + p_2(Y \otimes \mathbf{I})[\rho_{B_1 B_2}](Y \otimes \mathbf{I}) + p_3(Z \otimes \mathbf{I})[\rho_{B_1 B_2}](\mathbf{I} \otimes Z)\} \\
&+ 4(p_0 p_1 q_0 q_1 + p_2 p_3 q_2 q_3)(X \otimes X)[\rho_{B_1 B_2}](X \otimes X) + 4(p_0 p_2 q_0 q_2 + p_1 p_3 q_1 q_3)(Y \otimes Y)[\rho_{B_1 B_2}](Y \otimes Y) \\
&+ 4(p_0 p_3 q_0 q_3 + p_2 p_1 q_2 q_1)(Z \otimes Z)[\rho_{B_1 B_2}](Z \otimes Z) + 4(p_0 p_1 q_0 q_2 + p_2 p_3 q_1 q_3)(X \otimes Y)[\rho_{B_1 B_2}](X \otimes Y) \\
&+ 4(p_0 p_1 q_0 q_3 + p_2 p_3 q_1 q_2)(X \otimes Z)[\rho_{B_1 B_2}](X \otimes Z) + 4(p_0 p_2 q_0 q_1 + p_1 p_3 q_2 q_3)(Y \otimes X)[\rho_{B_1 B_2}](Y \otimes X) \\
&+ 4(p_0 p_2 q_0 q_3 + p_1 p_3 q_1 q_2)(Y \otimes Z)[\rho_{B_1 B_2}](Y \otimes Z) + 4(p_0 p_3 q_0 q_1 + p_2 p_1 q_2 q_3)(Z \otimes X)[\rho_{B_1 B_2}](Z \otimes X) \\
&+ 4(p_0 p_3 q_0 q_2 + p_1 p_2 q_1 q_3)(Z \otimes Y)[\rho_{B_1 B_2}](Z \otimes Y), \tag{C2}
\end{aligned}$$

$$\begin{aligned}
\mathcal{C}_-(\rho_{B_1 B_2}) = &2\sum_{l=0}^3 p_l^2 \{q_1 q_2(\mathbf{I} \otimes Z)[\rho_{B_1 B_2}](\mathbf{I} \otimes Z) + q_2 q_3(\mathbf{I} \otimes X)[\rho_{B_1 B_2}](\mathbf{I} \otimes X) + q_3 q_1(\mathbf{I} \otimes Y)[\rho_{B_1 B_2}](\mathbf{I} \otimes Y)) \\
&+ 2\sum_{l=0}^3 q_l^2 \{p_1 p_2(Z \otimes \mathbf{I})[\rho_{B_1 B_2}](Z \otimes \mathbf{I}) + p_2 p_3(X \otimes \mathbf{I})[\rho_{B_1 B_2}](X \otimes \mathbf{I}) + p_3 p_1(Y \otimes \mathbf{I})[\rho_{B_1 B_2}](Y \otimes \mathbf{I})\}
\end{aligned}$$

$$+ 4(p_2 p_3 q_0 q_1 + p_0 p_1 q_2 q_3)(X \otimes X)[\rho_{B_1 B_2}](X \otimes X) + 4(p_1 p_3 q_0 q_2 + p_0 p_2 q_1 q_3)(Y \otimes Y)[\rho_{B_1 B_2}](Y \otimes Y)$$

$$+ 4(p_1 p_2 q_0 q_3 + p_0 p_3 q_1 q_2)(Z \otimes Z)[\rho_{B_1 B_2}](Z \otimes Z) + 4(p_0 p_1 q_1 q_2 + p_2 p_3 q_0 q_3)(X \otimes Z)[\rho_{B_1 B_2}](X \otimes Z)$$

$$+ 4(p_0 p_1 q_1 q_3 + p_2 p_3 q_0 q_2)(X \otimes Y)[\rho_{B_1 B_2}](X \otimes Y) + 4(p_1 p_3 q_0 q_1 + p_0 p_2 q_2 q_3)(Y \otimes X)[\rho_{B_1 B_2}](Y \otimes X)$$

$$+ 4(p_1 p_3 q_0 q_3 + p_0 p_2 q_1 q_2)(Y \otimes Z)[\rho_{B_1 B_2}](Y \otimes Z) + 4(p_1 p_2 q_0 q_1 + p_0 p_3 q_2 q_3)(Z \otimes X)[\rho_{B_1 B_2}](Z \otimes X)$$

$$+ 4(p_1 p_2 q_0 q_2 + p_0 p_3 q_1 q_3)(Z \otimes Y)[\rho_{B_1 B_2}](Z \otimes Y). \tag{C3}$$

For $\mathcal{E}_1 = \mathcal{E}_1 = \mathcal{N}_{XY}$, substituting $p_0 = p_3 = q_0 = q_3 = 0$ and $p_1 = p_2 = q_1 = q_2 = 1/\sqrt{2}$ in Eqs. (C2)–(C3) we obtain

$$\mathcal{C}_+(\rho_{B_1 B_2}) = \rho_{B_1 B_2} + Z \otimes Z(\rho_{B_1 B_2})Z \otimes Z, \tag{C4}$$

$$\mathcal{C}_-(\rho_{B_1 B_2}) = \mathbb{I} \otimes Z(\rho_{B_1 B_2})\mathbb{I} \otimes Z + Z \otimes \mathbb{I}(\rho_{B_1 B_2})Z \otimes \mathbb{I}. \tag{C5}$$

Now considering $\omega_c = |+\rangle_c \langle +|$, after proper normalization, Eq. (C1) becomes

$$\mathcal{S}^{(2)}_{|+\rangle_c}(\mathcal{E}, \mathcal{E})[\rho_{B_1 B_2}]$$
$$= \tfrac{1}{4}[\mathbb{I} \otimes Z(\rho_{B_1 B_2})\mathbb{I} \otimes Z + Z \otimes \mathbb{I}(\rho_{B_1 B_2})Z \otimes \mathbb{I}] \otimes \mathbb{P}^{|-\rangle}_c$$
$$+ \tfrac{1}{4}[\rho_{B_1 B_2} + Z \otimes Z(\rho_{B_1 B_2})Z \otimes Z] \otimes \mathbb{P}^{|+\rangle}_c, \tag{C6}$$

where $\mathbb{P}^{|\pm\rangle} := |\pm\rangle \langle\pm|$. Upon measuring the order system in the $\{\mathbb{P}^{|\pm\rangle}\}$ basis, the conditional states of $B_1 B_2$ read

" $- 1$"outcome
$$\rightarrow \tfrac{1}{2}[\mathbb{I} \otimes Z(\rho_{B_1 B_2})\mathbb{I} \otimes Z + Z \otimes \mathbb{I}(\rho_{B_1 B_2})Z \otimes \mathbb{I}],$$

" $+ 1$"outcome
$$\rightarrow \tfrac{1}{2}[\rho_{B_1 B_2} + Z \otimes Z(\rho_{B_1 B_2})Z \otimes Z]. \tag{C7}$$

APPENDIX D: RANDOM-RECEIVER QUANTUM COMMUNICATION FOR N RECEIVERS

When $\mathcal{E} = \mathcal{F} := \bigotimes_{k=1}^n \mathcal{N}_{XY}$, where $\mathcal{N}_{XY}(\rho) = \tfrac{1}{2}(X\rho X + Y\rho Y)$, the switched quantum distribution channel from Alice to n Bobs reads

$$\mathcal{S}^{(n)}_{\omega_c}[\rho_{B_1 \cdots B_n}]$$
$$:= \sum_{i_1, j_1, \ldots, i_n, j_n = 0}^{1} G_{i_1 j_1 \cdots i_n j_n}(\rho_{B_1 \cdots B_n} \otimes \omega_c)G^\dagger_{i_1 j_1 \cdots i_n j_n}, \tag{D1}$$

where the Kraus operators

$$G_{i_1 j_1 \cdots i_n j_n} := \bigotimes_{k=1}^n E_{i_k} F_{j_k} \otimes |0\rangle_c \langle 0| + \bigotimes_{k=1}^n F_{j_k} E_{i_k} \otimes |1\rangle_c \langle 1|$$

with $E_{0_k} = F_{0_k} = X/\sqrt{2}$ and $E_{1_k} = F_{1_k} = Y/\sqrt{2}$ the Kraus operators of $\mathcal{N}_{XY}$ on the kth transmission line. Consider now an individual term in the summation on the right-hand side of Eq. (D1). The sign of the coherence term of the order qubit will be flipped, i.e., $\omega_c \rightarrow Z\omega_c Z$ if $\bigoplus_{k=1}^n (i_k \oplus j_k) = 1$, and whenever $\bigoplus_{k=1}^n (i_k \oplus j_k) = 0$, it will remain invariant, i.e., $\omega_c \rightarrow \omega_c$. Furthermore, we use the facts that $XX = YY = \mathbb{I}$ and $XY = iZ$ and $YX = -iZ$ in the following analysis.

Case I: order bit invariant terms $[\bigoplus_{k=1}^n (i_k \oplus j_k) = 0]$. In this case we have the following terms.

(i) For all k, $i_k = j_k$, which will result in the term $G_{i_1 j_1 \cdots i_n j_n}$ having the form $\mathbb{I}_{B_1 \cdots B_n} \otimes (|0\rangle_c \langle 0| + |1\rangle_c \langle 1|)$ on the right-hand side of Eq. (D1).

(ii) For an even number of cases (say $2m$), the i_k indices are different from the corresponding j_k, and for the other cases, they are equal. For a given $m \in \{0, 1, \ldots, [n/2]\}$, this will result in terms $G_{i_1 j_1 \cdots i_n j_n}$ of the form $(-1)^m(Z_1, \ldots, Z_{2m}, \mathbb{I}_{2m+1}, \ldots, \mathbb{I}_n) \otimes (|0\rangle_c \langle 0| + |1\rangle_c \langle 1|)$, where $(Z_1, \ldots, Z_p, \mathbb{I}_{p+1}, \ldots, \mathbb{I}_q)$ denotes the term with Z acting on p among q numbers of state and the identity acting on rest. There are $\binom{q}{p} = q!/[p!\,(q-p)!]$ such terms.

Case II: order bit flipped terms $[\bigoplus_{k=1}^n (i_k \oplus j_k) = 1]$. In this case we have the following terms.

(i) For an odd number of cases (say $2m + 1$), the i_k indices and the corresponding j_k indices are $i_k = \bar{j}_k = 0$, and for the other cases, they are equal. For a given $m \in \{0, 1, \ldots, [(n-1)/2]\}$, this will result in terms $G_{i_1 j_1 \cdots i_n j_n}$ of the form $i \times (-1)^m(Z_1, \ldots, Z_{2m+1}, \mathbb{I}_{2m+2}, \ldots, \mathbb{I}_n) \otimes (|0\rangle_c \langle 0| - |1\rangle_c \langle 1|)$.

(ii) For $2m + 1$ cases, $i_k = \bar{j}_k = 1$, with all other cases equal. For a given $m \in \{0, 1, \ldots, [(n-1)/2]\}$, this will result in terms $G_{i_1 j_1 \cdots i_n j_n}$ of the form $-i \times (-1)^m(Z_1, \ldots, Z_{2m+1}, \mathbb{I}_{2m+2}, \ldots, \mathbb{I}_n) \otimes (|0\rangle_c \langle 0| - |1\rangle_c \langle 1|)$.

Combining these together we finally have

$$
\mathcal{S}_{\omega_c}^{(n)}[\rho_{B_1 \cdots B_n}]
$$

$$
:= \frac{1}{2^n} \sum_{m=0}^{[n/2]} [(Z_1, \ldots, Z_{2m}, \mathbb{I}_{2m+1}, \ldots, \mathbb{I}_n) \rho_{B_1 B_2 \cdots B_n}
$$

$$
\times (Z_1, \ldots, Z_{2m}, \mathbb{I}_{2m+1}, \ldots, \mathbb{I}_n)] \otimes \omega_c
$$

$$
+ \frac{1}{2^n} \sum_{m=0}^{[(n-1)/2]} [(Z_1, \ldots, Z_{2m+1}, \mathbb{I}_{2m+2}, \ldots, \mathbb{I}_n) \rho_{B_1 B_2 \cdots B_n}
$$

$$
\times (Z_1, \ldots, Z_{2m+1}, \mathbb{I}_{2m+2}, \ldots, \mathbb{I}_n)] \otimes Z \omega_c Z. \quad \text{(D2)}
$$

Suppose that initial state of the order system is $\omega_c = |+\rangle \langle +|$. Then, after evolution of the switched channel, depending on the outcome of the Pauli X measurement on the order system, if one of the receivers applies a suitable local unitary correction to his subsystem then the final outcome state reads

$$
\frac{1}{2^n} \sum_{m=0}^{[n/2]} [(Z_1, \ldots, Z_{2m}, \mathbb{I}_{2m+1}, \ldots, \mathbb{I}_n) \rho_{B_1 B_2 \cdots B_n}
$$

$$
\times (Z_1, \ldots, Z_{2m}, \mathbb{I}_{2m+1}, \ldots, \mathbb{I}_n)]. \quad \text{(D3)}
$$

In the present context the input state is the generalized GHZ state $|\psi\rangle_{B_1 \cdots B_n} = \alpha |0 \cdots 0\rangle_{B_1 \cdots B_n} + \beta |1 \cdots 1\rangle_{B_1 \cdots B_n}$, which is invariant under a local unitary Z operation by any even number of parties. Thus, the state gets distributed perfectly among n receivers.

To reproduce the qubit information at one of the receivers' labs, they will follow a LOCC protocol. Suppose that the qubit state needs to be reproduced at ith receiver. All other receivers will perform a Pauli X measurement on their respective subsystems and inform the measurement results $x_k \in \{+1, -1\}$ for all $k \in \{1, \ldots, n\}$, $k \neq i$. Depending on this information, ith receiver will apply a Z unitary correction on their part if $\Pi_{k \neq i} x_k$ is -1; otherwise, they does nothing.

APPENDIX E: RANDOM-RECEIVER QUANTUM COMMUNICATION WITH CONTROLLED OPERATIONS IN A DEFINITE ORDER

In this section we discuss the use of controlled operations in a definite causal order for random-receiver quantum communication. First, we show that, if arbitrary controlled operations are allowed, it is easy to construct protocols that achieve random-receiver quantum communication through entanglement-breaking channels. This is because (i) controlled operations before transmission can transfer information to the control system, thus bypassing the noisy channels, and (2) controlled operations after transmission allow one to generate entanglement between the control system and all the systems at the receivers'

locations, thus evading the LOCC constraint. Then, we show that if the controlled operations are restricted to permutations then random-receiver quantum communication cannot be achieved for any odd n.

1. Protocol for random-receiver quantum communication using arbitrary controlled operations

The following protocol permits random-receiver quantum communication through the channels $\mathcal{A} = \mathcal{B} = \mathcal{N}_{XY}^{\otimes n}$. The protocol starts with the message encoded in the state of the first of the n qubits. First, the sender applies a CNOT gate to the message and the control qubit, initialized in the state $|+\rangle$. As a result, the message and the control qubit end up in the state $[|0\rangle(\alpha|0\rangle + \beta|1\rangle) + |1\rangle(\alpha|1\rangle + \beta|0\rangle)]/\sqrt{2}$. Second, the sender prepares $n - 1$ qubits in the state $|0\rangle$. The sender sends the message and the other $n - 1$ qubits through the channel $\mathcal{AB} = (\mathcal{N}_{XY}^2)^{\otimes n}$, which collapses the overall state to a classical mixture of the states $|0\rangle|0\rangle^{\otimes(n-1)}(\alpha|0\rangle + \beta|1\rangle)$ and $|1\rangle|0\rangle^{\otimes(n-1)}(\alpha|1\rangle + \beta|0\rangle)$. Third, CNOT gates are applied to the control qubit and to the additional $n - 1$ qubits, producing either the state $|0\rangle(\alpha|0\rangle^{\otimes n} + \beta|1\rangle^{\otimes n})$ or the state $|1\rangle(\alpha|1\rangle^{\otimes n} + \beta|0\rangle^{\otimes n})$. Finally, the first receiver measures the first qubit in the computational basis, and, if the outcome is 1, all the other receivers perform the bit flip operation $X = |0\rangle\langle 1| + |1\rangle\langle 0|$ on the remaining qubits and on the control qubit. In this way, the remaining qubits end up in the generalized GHZ state $\alpha|0\rangle^{\otimes n} + \beta|1\rangle^{\otimes n}$, and random-receiver quantum communication can be achieved as in the noiseless protocol presented in the Introduction.

Note that this protocol uses the control qubit to bypass the noisy channels $\mathcal{A}$ and $\mathcal{B}$, as one can see from the fact that, after the channels $\mathcal{A}$ and $\mathcal{B}$ have acted, all the information about the message is on the control qubit. In addition, the protocol freely generates entanglement between the n receivers after the channels $\mathcal{A}$ and $\mathcal{B}$ have acted. The entanglement generation is achieved by the $n - 1$ CNOT gates applied in the last step of the protocol. In general, these CNOT gates cannot be implemented by the receivers, due to their spatial separation. Hence, they must be regarded as performed by a third party other than the receivers.

Note that the presence of entangling operations between the control and each receiver is essential in the above protocol. More generally, entangling operations are necessary in any protocol that achieves random-receiver quantum communication through entanglement-breaking channels in a definite order. Any such protocol needs to bypass the entanglement-breaking channels by encoding quantum information in the control qubit. An equivalent condition can be obtained by introducing an additional reference system at the receiver's end: in order to achieve perfect quantum communication, the protocol must transform a maximally entangled state of the input and the reference

into a maximally entangled state of the control and the reference. After the action of an entanglement-breaking channel, the control and the reference have no correlation with the qubits at the receivers' locations. Hence, no quantum information can be transferred back from the control to the receivers without the use of entangling operations.

2. No random-receiver quantum communication with controlled permutations in a fixed order

Arbitrary controlled operations appear to be a too broad set for the problem of random-receiver quantum communication, in that they allow a complete transfer of information to the control qubit and violate the locality restrictions among the receivers. On the other hand, the quantum SWITCH can be regarded as a controlled SWAP operation *in time*: it swaps the order of quantum systems appearing in a given time sequence, putting the inputs and outputs of channel $\mathcal{A}$ either before or after the inputs and outputs of channel $\mathcal{B}$. One may then ask if controlled SWAP operations *in space* can reproduce the same features when the channels $\mathcal{A}$ and $\mathcal{B}$ are arranged in a fixed sequential order, say with $\mathcal{A}$ acting before $\mathcal{B}$.

Here we show that the answer is negative, in the following sense: suppose that the quantum channels $\mathcal{A}$ and $\mathcal{B}$ are placed in a fixed order, and that their inputs and outputs undergo arbitrary controlled permutations, as in Fig. 4. For odd n, we show that, no matter which controlled permutations are chosen, one of the receivers will remain in a fixed state, independent of the quantum message from the sender.
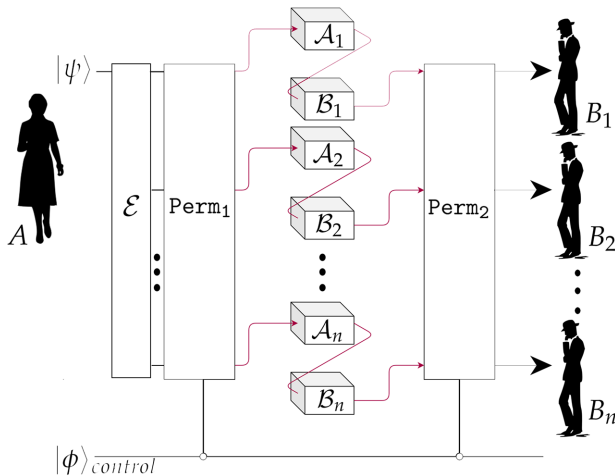
The argument is simple. The output of channel $\mathcal{N}_{XY}^{\otimes n}$ is a mixture of states in the computational basis, of the form $\bigotimes_{j=1}^{n} |b_j\rangle$, with $b_j \in \{0, 1\}$ for every j. Perfect quantum communication through this entanglement-breaking channel is possible only if, for every state appearing in the mixture, the initial message has been perfectly transferred to the control qubit (note that this argument applies in general, even if the operations before the action of the channel $\mathcal{N}_{XY}^{\otimes n}$ are arbitrary global operations).

Now, let us focus on one specific state in the mixture, say $|\mathbf{b}\rangle = \bigotimes_{j=1}^{n} |b_j\rangle$ for some bit string $\mathbf{b} = (b_i)_{i=1}^n$. Let us denote by $|\psi'\rangle = \alpha'|0\rangle + \beta'|1\rangle$ the state of the control qubit conditional to the state $\bigotimes_{j=1}^{n} |b_j\rangle$. The state $|\mathbf{b}\rangle|\psi'\rangle$ then undergoes a controlled permutation W, becoming the state $W|\mathbf{b}\rangle|\psi'\rangle = \alpha'\bigotimes_{j=1}^{n} |b_{\pi(j)}\rangle \otimes |0\rangle + \beta'\bigotimes_{j=1}^{n} |b_{\sigma(j)}\rangle \otimes |1\rangle$, where π and σ are two permutations. Equivalently, the state can be rewritten as $W|\mathbf{b}\rangle|\psi'\rangle = \alpha'\bigotimes_{j=1}^{n} |c_j\rangle \otimes |0\rangle + \beta'\bigotimes_{j=1}^{n} |c_{\tau(j)}\rangle \otimes |1\rangle$, where $\mathbf{c} = (c_j)_{j=1}^n$ is a suitable bit string and τ is a permutation. Now, recall that $\mathbf{c}$ is a string of length n consisting of zeros and ones. When n is odd, there exists at least one value of j such that $c_j = \tau(c_j)$. Hence, the jth system ends up in the state $|c_j\rangle$, which has no dependence on the coefficients α' and β', and therefore on the initial message.

In summary, the n output systems and the control end up in a mixture of pure states, one of which is a product between a fixed state of system j and the remaining systems. Hence, the quantum message cannot be transferred perfectly to the jth receiver, since with some nonzero probability, the state of the jth system will be independent of the message.

FIG. 4. Random-receiver quantum communication task with controlled permutations *in space*. A control qubit, initially in the state $|\phi\rangle$, controls the choice of a permutation Perm$_1$ acting on the input systems. Then, the input systems are sent through the noisy channels, with system i passing through channels $\mathcal{A}_i$ and $\mathcal{B}_i$ in a definite order. Finally, a permutation Perm$_2$ is applied to the outputs of the channels, with the choice of permutation depending on the state of the control qubit.

[1] A. M. Childs, Secure assisted quantum computation, Quantum Inf. Comput. **5**, 456 (2005).

[2] Pablo Arrighi and Louis Salvail, Blind quantum computation, Int. J. Quantum Inf. **04**, 883 (2006).

[3] Joseph F. Fitzsimons, Private quantum computation: An introduction to blind quantum computing and related protocols, Npj Quantum Inf. **3**, 23 (2017).

[4] Vedran Dunjko, Joseph F. Fitzsimons, Christopher Portmann, and Renato Renner, in *Lecture Notes in Computer Science* (Springer Berlin Heidelberg, 2014), p. 406.

[5] Scott Aaronson, Alexandru Cojocaru, Alexandru Gheorghiu, and Elham Kashefi, Complexity-theoretic limitations on blind delegated quantum computation, (2019).

[6] William K. Wootters and Wojciech H. Zurek, A single quantum cannot be cloned, Nature **299**, 802 (1982).

[7] D. G. B. J. Dieks, Communication by epr devices, Phys. Lett. A **92**, 271 (1982).

[8] Adrian Kent, A no-summoning theorem in relativistic quantum theory, Quantum Inf. Process. **12**, 1023 (2013).

[9] Adrian Kent, Quantum tasks in minkowski space, Classical Quantum Gravity **29**, 224013 (2012).

[10] Patrick Hayden and Alex May, Summoning information in spacetime, or where and when can a qubit be?, J. Phys. A: Math. Theor. **49**, 175304 (2016).

[11] Emily Adlam and Adrian Kent, Quantum paradox of choice: More freedom makes summoning a quantum state harder, Phys. Rev. A **93**, 062327 (2016).

[12] Adrian Kent, Unconstrained summoning for relativistic quantum information processing, Phys. Rev. A **98**, 062332 (2018).

[13] Ya-Dong Wu, and Abdullah Khalid, and Barry C. Sanders, Efficient code for relativistic quantum summoning, New J. Phys. **20**, 063052 (2018).

[14] Lucien Hardy, Towards quantum gravity: A framework for probabilistic theories with non-fixed causal structure, J. Phys. A: Math. Theor. **40**, 3081 (2007).

[15] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Beyond quantum computers, arXiv:0912.0195 (2009).

[16] O. Oreshkov, F. Costa, and Č. Brukner, Quantum correlations with no causal order, Nat. Commun. **3**, 1092 (2012).

[17] G. Chiribella, G. M. D'Ariano, P. Perinotti, and B. Valiron, Quantum computations without definite causal structure, Phys. Rev. A **88**, 022318 (2013).

[18] Alessandro Bisio and Paolo Perinotti, Theoretical framework for higher-order quantum theory, Proc. R. Soc. A **475**, 20180706 (2019).

[19] Michael Horodecki, Peter W. Shor, and Mary Beth Ruskai, Entanglement breaking channels, Rev. Math. Phys. **15**, 629 (2003).

[20] A. S. Holevo, Entanglement-breaking channels in infinite dimensions, Probl. Inf. Transm. **44**, 171 (2008).

[21] A. S. Holevo, Quantum coding theorems, Russian Math. Surveys **53**, 1295 (1998).

[22] Giulio Chiribella, Manik Banik, Some Sankar Bhattacharya, Tamal Guha, Mir Alimuddin, Arup Roy, Sutapa Saha, Sristy Agrawal, and Guruprasad Kar, Indefinite causal order enables perfect quantum communication with zero capacity channels, New J. Phys. **23**, 033039 (2021).

[23] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, Teleporting an Unknown Quantum State via Dual Classical and Einstein-Podolsky-Rosen Channels, Phys. Rev. Lett. **70**, 1895 (1993).

[24] Lev Vaidman, Instantaneous Measurement of Nonlocal Variables, Phys. Rev. Lett. **90**, 010402 (2003).

[25] Salman Beigi and Robert König, Simplified instantaneous non-local quantum computation with applications to position-based cryptography, New J. Phys. **13**, 093036 (2011).

[26] A. Gonzales and E. Chitambar, Bounds on instantaneous nonlocal quantum computation, IEEE Trans. Inf. Theory **66**, 2951 (2020).

[27] M. Gregoratti and R. F. Werner, Quantum lost and found, J. Mod. Opt. **50**, 915 (2003).

[28] M. Gregoratti and R. F. Werner, On quantum error-correction by classical feedback in discrete time, J. Math. Phys. **45**, 2600 (2004).

[29] P. Hayden and C. King, Correcting quantum channels by measuring the environment, Quan. Inf. Comp. **5**, 156 (2005).

[30] J. A. Smolin, F. Verstraete, and A. Winter, Entanglement of assistance and multipartite state distillation, Phys. Rev. A **72**, 052317 (2005).

[31] A. Guérin, G. Rubino, and Č. Brukner, Communication through quantum-controlled noise, Phys. Rev. A **99**, 062317 (2019).

[32] G. Chiribella and H. Kristjánsson, Quantum shannon theory with superpositions of trajectories, Proc. R. Soc. A **475**, 20180903 (2019).

[33] Hlér Kristjánsson, Giulio Chiribella, Sina Salek, Daniel Ebler, and Matthew Wilson, Resource theories of communication, New J. Phys. **22**, 073014 (2020).

[34] L. M. Procopio *et al.*, Experimental superposition of orders of quantum gates, Nat. Commun. **6**, 7913 (2015).

[35] G. Rubino *et al.*, Experimental verification of an indefinite causal order, Sci. Adv. **3**, e1602589 (2017).

[36] K. Goswami, C. Giarmatzi, M. Kewming, F. Costa, C. Branciard, J. Romero, and A. G. White, Indefinite Causal Order in a Quantum Switch, Phys. Rev. Lett. **121**, 090503 (2018).

[37] Y. Guo, X.-M. Hu, Z.-B. Hou, H. Cao, J.-M. Cui, B.-H. Liu, Y.-F. Huang, C.-F. Li, G.-C. Guo, and G. Chiribella, Experimental Transmission of Quantum Information Using a Superposition of Causal Orders, Phys. Rev. Lett. **124**, 030502 (2020).

[38] K. Goswami and J. Romero, Experiments on quantum causality, AVS Quantum Sci. **2**, 037101 (2020).

[39] Giulia Rubino, Lee A. Rozema, Daniel Ebler, Hlér Kristjánsson, Sina Salek, Philippe Allard Guérin, Alastair A. Abbott, Cyril Branciard, Časlav Brukner, and Giulio Chiribella *et al.*, Experimental quantum communication enhancement by superposing trajectories, Phys. Rev. Res. **3**, 013093 (2021).

[40] V. Parigi *et al.*, Storage and retrieval of vector beams of light in a multiple-degree-of-freedom quantum memory, Nat. Commun. **6**, 7706 (2015).

[41] Xi-Lin Wang *et al.*, Quantum teleportation of multiple degrees of freedom of a single photon, Nature **518**, 516 (2015).

[42] Fu-Guo Deng, Bao-Cang Ren, and Xi-Han Li, Quantum hyperentanglement and its applications in quantum information processing, Sci. Bull. **62**, 46 (2017).

[43] Ming-Xing Luo, Hui-Ran Li, Hong Lai, and Xiaojun Wang, Quantum computation based on photons with three degrees of freedom, Sci. Rep. **6**, 25977 (2016).

[44] D. Ebler, S. Salek, and G. Chiribella, Enhanced Communication with the Assistance of Indefinite Causal Order, Phys. Rev. Lett. **120**, 120502 (2018).

[45] S. Salek, D. Ebler, and G. Chiribella, Quantum communication in a superposition of causal orders, arXiv:1809.06655.

[46] K. Goswami, Y. Cao, G. A. Paz-Silva, J. Romero, and A. G. White, Increasing communication capacity via superposition of order, Phys. Rev. Res. **2**, 033292 (2020).

[47] M. Caleffi and A. S. Cacciapuoti, Quantum switch for the quantum internet: Noiseless communications through noisy channels, IEEE J. Sel. Areas Commun. **38**, 575 (2020).

[48] Alastair A. Abbott, Julian Wechs, Dominic Horsman, Mehdi Mhalla, and Cyril Branciard, Communication

through coherent control of quantum channels, Quantum **4**, 333 (2020).

[49] Dirk Bouwmeester, Artur Ekert, Anton Zeilinger, eds. *The Physics of Quantum Information* (Springer, Berlin, Heidelberg, 2000).

[50] J. I. Cirac, P. Zoller, H. J. Kimble, and H. Mabuchi, Quantum State Transfer and Entanglement Distribution among Distant Nodes in a Quantum Network, Phys. Rev. Lett. **78**, 3221 (1997).

[51] H. J. Kimble, The quantum internet, Nature **453**, 1023 (2008).

[52] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Science **362**, 9288 (2018).