

Quantum Advantage in Communication Networks

Aditi Sen(De) and Ujjwal Sen

Quantum channels are known to provide qualitatively better information transfer capacities over their classical counterparts. Examples include quantum cryptography, quantum dense coding, and quantum teleportation. This is a short review on paradigmatic quantum communication protocols in both bipartite as well as multipartite scenarios.

I. INTRODUCTION

Communication is a process by which information is transferred from a sender to a receiver. Information transmission networks have revolutionized our lives – telephone, radio, television, internet, and other forms of communication, have become a necessity for most of us. Such transmission channels can be broadly classified into two categories – ones without a security aspect, and ones with it.

Information transmission without a security feature can range from an examination result on the internet to a radio message from the meteorological office to warn about an impending storm or a telephone call from a relative. In such channels, there is either no a priori precaution taken to protect the message against potential eavesdroppers (as in telephone conversations) or it is the intention of the sender that the message is obtained by as many receivers as possible (as in messages from the meteorological office). However, one often requires *secure* communication protocols, and their applications range from day-to-day use e.g. in internet banking, to national security (e.g. for communication between the security forces).

All the currently existing practical communication networks deal with classical messages sent over classical channels. By a classical message, we shall mean any information that can be expressed as an array of 0s and 1s, where 0 and 1 denote two distinguishable objects. Such distinguishable objects can be a black ball and a white ball, or two distinguishable signals sent over an optical fibre. A classical channel is any transmission channel that carries such messages, and is governed by the laws of classical mechanics. Mathematically, it is an operator that acts on arrays of 0s and 1s to produce similar arrays or probabilistic mixtures of them.

Over the past few years, it has been realized that the performance of communication can be enhanced, sometimes even qualitatively, by using channels that observe quantum mechanical laws [1–4]. After the theoretical proposals, the successful journey of quantum communication has begun from the experimental achievements starting in the late 1990s with photons [5]. But several other physical systems including ions [6], atoms in optical lattices [7], nuclear magnetic resonance [8], Josephson junctions [9], and atoms and photons in a cavity [10], have also been used for implementing quantum information processing tasks. While photonic devices and channels still remain the trusted vehicle for long distance quantum communication, experiments involving quantum communication via massive particles and those that involve atom-photon systems may turn out to be important for quantum computational applications.

In quantum communication protocols that does not involve a security aspect, quantum correlations, aka entanglement [11] has turned out to be an essential ingredient – it is the *resource* that runs the protocols. The quintessential quantum communication channels without a security feature are quantum states used as quantum dense coding [3] and quantum teleportation [4] channels. They are channels respectively for transmitting classical and quantum information, and form the basis of most quantum channels without a security angle. The advantage of both the protocols – dense coding and teleportation – over their classical counterparts, depend on the use of shared entangled quantum states. Before we present the communication schemes in further detail, we will give a formal definition of entanglement in Sec. II.

Classical information sent via quantum states will be discussed in Sec. III. In 1992, C.H. Bennett and S.J. Wiesner invented a protocol – called quantum dense coding [3] – for sending classical messages by using a maximally entangled quantum state shared between a sender and a receiver. The information transmission capacity of this quantum channel is double of that of the corresponding classical channel. Along with this initial protocol, we will also discuss the case when the shared quantum state may not be maximally entangled. A communication channel with a single sender and a single receiver has limited commercial use, and in Sec. III, we will consider classical information transfer over quantum communication networks involving multiple senders and receivers.

While quantum dense coding involves sending classical information over a quantum channel, “quantum teleportation” [4] – introduced in 1993 – involves quantum information transfer over a quantum channel. It was shown that a maximally entangled quantum state between the sender and the receiver, along with two bits of classical communication from the sender to the receiver, is sufficient to exactly transfer the state of a two-dimensional quantum system (qubit). In the absence of the shared quantum state, the same transfer will take an infinite amount of classical communication. Therefore, while quantum dense coding results in a doubling of the capacity of information transfer as compared to the corresponding classical protocol, quantum teleportation leads to an infinite resource reduction

over its classical counterpart. These concepts will be discussed in Sec. V. Other similar protocols involving multiple senders and multiple receivers will also be discussed in that section.

Sending secret messages has probably been around from the dawns of civilization. There has of course been huge advances in recent times, and e.g. currently we use the internet for secure monetary transactions with a considerable amount of reliability. However, all such practical classical cryptographic protocols depend for its security on unproven premises of the hardness of certain mathematical computations on classical computers. [A classical computer is a device for performing mathematical operations, and which follows laws of classical mechanics for its functioning. Commercially available desktops, notebooks, etc. fall in this category. They are different from a quantum computer – a device that performs mathematical operations, and follows laws of quantum mechanics for its functioning. Although a realistic quantum computer has as yet not been built, small-scale ones are being built in several laboratories around the globe. See e.g. [6, 7, 12]] Most practical classical cryptographic schemes depend for their security on the unproven premise that it is hard to factorize an integer into its prime factors on a classical computer [13]. A twist to the story is that it is *easy* to factorize an integer into its prime factors on a *quantum* computer [14, 15]. In 1984, in a conference of (mostly classical!) computer scientists in Bengaluru, C.H. Bennett and G. Brassard introduced a protocol – quantum cryptography [1] – for sending secret classical messages, where the security is guaranteed by the laws of quantum mechanics. In particular, such protocols remain secure even if the potential eavesdropper has a quantum computer to work with. Interestingly, the protocol did not require any shared entanglement. The existence of nonorthogonal quantum states in quantum mechanics provided the security. Later on, in 1991, A. Ekert proposed a quantum cryptographic scheme which involved shared entangled states [2]. From the perspective of security, both the protocols turn out to be equivalent [16]. We discuss about these protocols in Sec. VI, along with generalizations to the case of multiple senders and receivers. In particular, we discuss a case of a single sender and two receivers where entanglement in the encoding states provide a higher level of security than in the case when there is no entanglement, thus demonstrating that entanglement is also an essential ingredient in *secure* quantum communication.

II. ENTANGLEMENT

Consider a situation where there are two observers who are situated in two distant locations. It is usual to call them Alice and Bob. A cartoon of the situation is depicted in Fig. 1. Below, unless mentioned to the contrary, a suffix A in the notation for a state or a Hilbert space will imply that it is in possession of the observer Alice. And similarly B for Bob. Now suppose that Alice has a physical system, corresponding to which the quantum mechanical Hilbert space is \mathcal{H}_A , and prepares it in the quantum state $|\psi\rangle_A$. Similarly, Bob prepares the quantum state $|\phi\rangle_B$ in \mathcal{H}_B . Then their joint state, $|\Psi\rangle_{AB} = |\psi\rangle_A \otimes |\phi\rangle_B$, in $\mathcal{H}_A \otimes \mathcal{H}_B$, is said to be a (pure) product state. Note that the preparation of the joint state did not require any communication, classical or quantum, between the observers. Suppose now that the observers are allowed to communicate over a classical channel, say a phone line. In that case, the two observers can (classically) correlate their preparation procedures, and produce mixtures of product states, and the most general state that can be prepared in that way is of the form [17]

$$\rho_{AB} = \sum_i p_i (|\psi_i\rangle\langle\psi_i|)_A \otimes (|\phi_i\rangle\langle\phi_i|)_B.$$

Here $\{p_i\}$ forms a probability distribution, so that $p_i \geq 0$, and $\sum_i p_i = 1$. This is therefore the most general shared quantum state of two parties that can be prepared by Alice and Bob, if they act locally in their distant laboratories with quantum operations and communicate over a classical channel. These set of operations is called “LOCC”, standing for “local (quantum) operations and classical communication.” And the bipartite (i.e. two-party) quantum states whose production is possible by LOCC are called separable states. Similar definitions are possible for multiparty (i.e. more than two parties) quantum states.

Quantum states that cannot be prepared by LOCC are called entangled. Quantum theory allows the existence of such states (see [11] for a review), and have actually been prepared in the lab (see e.g. [5–7]). The preparation of such states necessarily requires an interaction between the two physical systems of Alice and Bob. An example of an entangled state is the well-known singlet,

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \quad (1)$$

where $|0\rangle$ and $|1\rangle$ denote two orthonormal states of a qubit. They could e.g. be the spin-up and spin-down states in the z -direction of the spin degree of freedom of a spin-1/2 particle, or the horizontal and vertical polarizations of a photon. As we will see in the subsequent sections, the singlet state is a useful resource in quantum communication protocols. For this and other reasons, the singlet state (and any other state that is local unitarily equivalent to it)

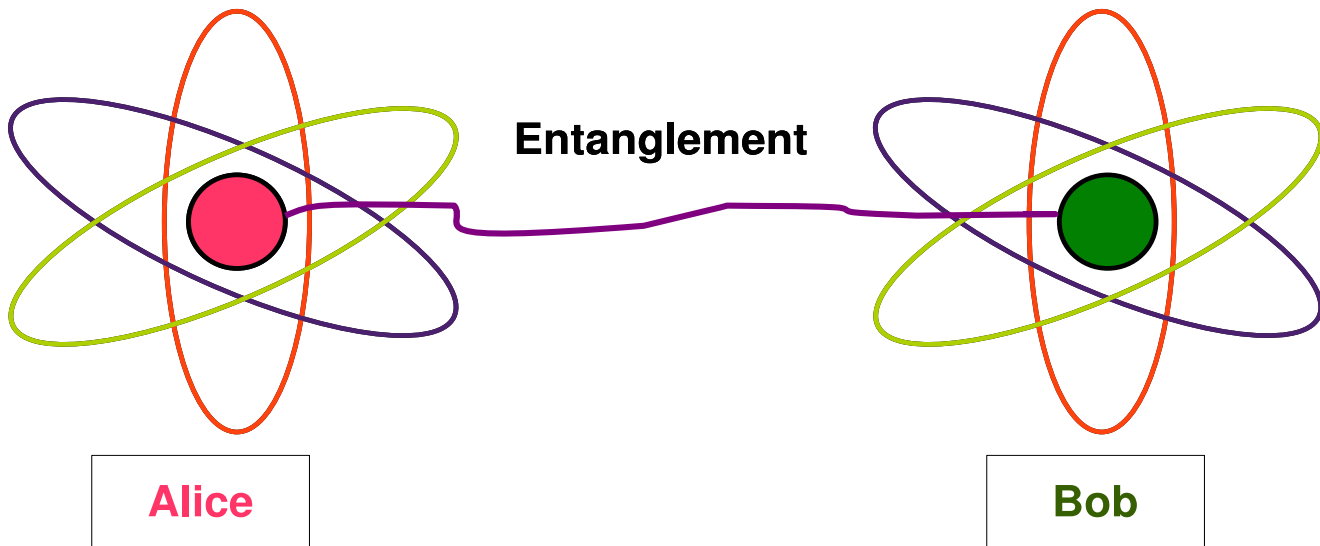


FIG. 1: Two separated observers – Alice and Bob – share an entangled state.

is called a maximally entangled state. An equivalent definition of a maximally entangled (bipartite) state is a *pure* bipartite quantum state whose local states are completely unpolarized – a bipartite quantum state of which we have the complete information globally (as the von Neumann entropy of the total state is vanishing) while no information locally (as the von Neumann entropies of the local states are maximal).

III. CLASSICAL INFORMATION TRANSMISSION VIA QUANTUM STATES: DENSE CODING

We will start by discussing the original quantum dense coding protocol [3] by using a maximally entangled state – the singlet. Before proceeding to the quantum protocol, let us note that classically, to send two bits of classical information (i.e. four independent messages), one needs a four-dimensional system, i.e. four orthogonal states, which could e.g. be four differently coloured balls. The protocol goes as follows. Suppose that Alice and Bob are together in Delhi today. Tomorrow, Alice will be in Mumbai, and Bob in Chennai. Suppose that after reaching Mumbai, Alice needs to send the information about the weather of the city to Bob. She is allowed to send only four independent messages (i.e. one option out of only four), and so while in Delhi they decide the following encoding:

- Red ball : Windy and raining,
- Blue ball : Windy but not raining,
- Green ball : Not windy but raining,
- Pink ball : Not windy and not raining.

Since, the balls are distinguishable, Bob will be able to decode the message sent by Alice. The question is whether using quantum mechanics can help to increase the capacity of such classical information transmission. As we will now find out, the answer is in the affirmative.

Suppose that after Alice and Bob reach Mumbai and Chennai respectively, Alice creates a singlet in her lab in Mumbai, and sends half of it [i.e. one of the particles] to Bob. We assume that the resulting shared state between Alice and Bob is just the singlet state, so that the channel that carries half of the singlet from Alice to Bob is a noiseless quantum channel. This is currently science fiction, as the distance from Mumbai to Chennai is about a thousand kilometres, and the distances between which entangled states can be created are currently about a hundred and fifty kilometres [18]. But not a long time ago, the same was around 10 kilometres [19], and sometime before that, it was about 10 metres [20]! After the singlet is created between Alice and Bob, Alice finds out the weather in Mumbai, and depending on what the weather is, she performs a unitary operation on her part of the shared singlet, according to the following instruction set:

$$\begin{aligned} \text{Windy and raining} & : \mathbb{I}, \\ \text{Windy but not raining} & : \sigma_z, \\ \text{Not windy but raining} & : \sigma_x, \\ \text{Not windy and not raining} & : \sigma_y, \end{aligned}$$

where \mathbb{I} is the identity operation on the qubit Hilbert space, and σ_i , $i = x, y, z$ are the Pauli spin operators. This has the following effect on the shared singlet:

$$\begin{aligned} \mathbb{I} \otimes \mathbb{I} |\psi^-\rangle & = |\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle), \\ \sigma_z \otimes \mathbb{I} |\psi^-\rangle & = |\psi^+\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ \sigma_x \otimes \mathbb{I} |\psi^-\rangle & = -|\phi^-\rangle = \frac{-1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ \sigma_y \otimes \mathbb{I} |\psi^-\rangle & = \iota |\phi^+\rangle = \frac{\iota}{\sqrt{2}}(|00\rangle + |11\rangle), \end{aligned} \tag{2}$$

where $\iota = \sqrt{-1}$, and where we suppose that in Eq. (2), the first particle of the shared state is with Alice and the second is with Bob. Moreover, we assume that here and hereafter, $|0\rangle$ and $|1\rangle$ are eigenvectors of the Pauli σ_z operator, corresponding to the eigenvalues $+1$ and -1 respectively. The states produced are either the singlet or the triplet states (perhaps up to a phase). After the application of the unitary operation, according to the weather report obtained, Alice sends her part of the shared state to Bob, down a noiseless quantum channel, so that now the whole post-operated two-qubit state is with Bob. For the case of the quantum protocol, we assume that while in Delhi, Alice and Bob agree on the following encoding:

$$\begin{aligned} \text{Windy and raining} & : |\psi^-\rangle, \\ \text{Windy but not raining} & : |\psi^+\rangle, \\ \text{Not windy but raining} & : |\phi^-\rangle, \\ \text{Not windy and not raining} & : |\phi^+\rangle. \end{aligned}$$

So e.g. if the state obtained by Bob is $|\phi^+\rangle$ (up to an indeterminate phase), he will infer that the weather in Mumbai is “not windy and not raining”. Since the singlet and the three triplets are mutually orthogonal, it is possible to set up a measurement to distinguish between them. Again this is not a simple matter to actually do that experiment in the lab [21], but is certainly a quantum mechanically allowed measurement. Therefore, after obtaining the second qubit from Alice, Bob measures the two-qubit state in the Bell basis (the two-qubit basis formed by the singlet and the three triplets), and finds out the weather in Mumbai, by looking up the encoding decided upon in Delhi.

Is there an advantage in the quantum protocol over the classical one? The classical protocol uses a four-dimensional physical system (a ball with four possible colours) to send two bits of classical information. In the quantum case, Alice initially sends a qubit (two-dimensional system) to Bob to prepare the shared singlet, and subsequently sends another qubit after her unitary operations. So the total dimension of the physical system sent is again four ($= 2 \times 2$) in the quantum case, and again there are two bits of classical information sent from Alice to Bob. However, in the classical case, the whole four-dimensional state has to be sent after obtaining the news about the weather, while in the quantum protocol, the first two-dimensional system can be sent before any news about the weather is obtained, and only the remaining two-dimensional system is to be sent after the news. It is in this sense that we have an advantage in the

quantum case, and we say that the capacity of classical information transfer is doubled by using quantum mechanics – two bits via a two-dimensional system in the quantum case against two bits via a four-dimensional system in the classical one, counting only the physical system sent after the news is obtained. One envisages a “quantum internet”, where sending qubits is free at night, and costly during the day, so that Alice sends the first qubit at night to prepare the singlet, and sends only the second qubit during the day after the news about the weather is obtained. While this may be still very much inside fiction, quantum dense coding (without such quantum memory effects) have been realized in the lab with several physical systems. See e.g. [22].

A. Towards Quantum Dense Coding Networks

The dense coding protocol described before is for a maximally entangled state of two qubits. It can be easily generalized to the case of a maximally entangled state of higher dimensions, e.g.

$$|\Phi^+\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle,$$

in $\mathcal{H}_A \otimes \mathcal{H}_B$, where $d = \min\{d_A, d_B\}$, $d_A = \dim \mathcal{H}_A$, $d_B = \dim \mathcal{H}_B$, and where $\{|i\rangle\}$ forms a mutually orthonormal set of states, to show that Alice can send $\log_2 d_A + \log_2 d_B$ bits of classical information by sending her part of $|\Phi^+\rangle$ to Bob. Classically, by sending a d_A -dimensional system, Alice can send at most $\log_2 d_A$ bits of classical information.

Experiments often produce quantum states that are nonmaximally entangled and possibly noisy, and before we go over to networks, let us first find whether nonmaximally entangled states can also be used to obtain a quantum advantage in dense coding protocols.

1. Nonmaximally Entangled Bipartite States

Consider therefore a bipartite quantum state (density matrix) ρ_{AB} , defined on the tensor product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, and the question is whether the capacity of classical information transfer, by using the shared quantum state ρ_{AB} , can go beyond the classical limit of $\log_2 d_A$. Suppose that the classical information that Alice wants to send to Bob is i , and that it happens with probability p_i . As in the case of the original protocol of Bennett and Wiesner, Alice performs a unitary operation U_i , if the message that she wants to send is i , on her part of ρ_{AB} . Subsequent to her unitary operation, she sends her part of the post-operated shared state to Bob. Bob then has the ensemble $\{p_i, \rho_i\}$, where

$$\rho_i = U_i \otimes \mathbb{I}_{d_B} \rho_{AB} U_i^\dagger \otimes \mathbb{I}_{d_B},$$

with \mathbb{I}_{d_B} being the identity operator on Bob’s physical system. The task of Bob now is to find as much information as is quantum mechanically possible about i from the ensemble $\{p_i, \rho_i\}$. The procedure is schematically shown in Fig. 2.

To decode the message, Bob performs a quantum measurement on the ensemble $\{p_i, \rho_i\}$, and obtains the result m with probability q_m . Let the corresponding post-measurement ensemble be $\{p_{i|m}, \rho_{i|m}\}$. The information gathered by Bob (about the message i) can be quantified by the classical mutual information between the message i and the measurement outcome m [23]:

$$I(i : m) = H(\{p_i\}) - \sum_m q_m H(\{p_{i|m}\}). \quad (3)$$

Here $H(\{r_x\}) = -\sum_x r_x \log_2 r_x$ is the Shannon entropy of the probability distribution $\{r_x\}$. Note that $H(\{p_i\})$ and $\sum_m q_m H(\{p_{i|m}\})$ respectively quantifies the pre-measurement and average post-measurement ignorance (i.e., lack of information) of Bob, about the message i . The difference $I(i : m)$ therefore quantifies the information gain due to the measurement. Bob’s aim is to obtain as much information as possible about i , and hence he has to perform a measurement that maximizes $I(i : m)$ among all quantum mechanically allowed measurements. This leads us to the concept of accessible information,

$$I_{acc} = \max I(i : m), \quad (4)$$

where the maximization is over all measurement strategies.

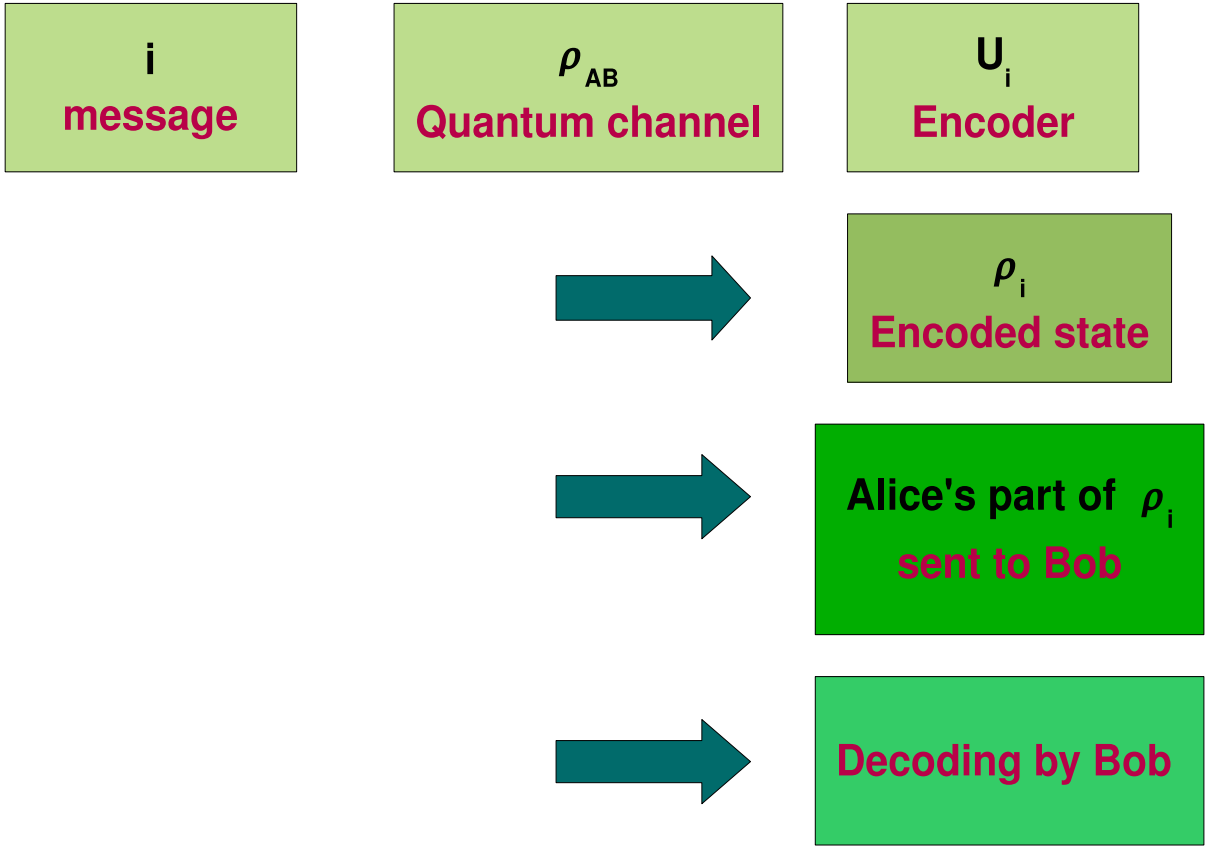


FIG. 2: A flowchart for the quantum dense coding protocol.

However, the maximization over measurements in accessible information is in general hard to compute, and therefore it is important to obtain bounds on I_{acc} [24–26]. A universal upper bound on I_{acc} , called the “Holevo bound” [24], is known for more than 30 years, and is given by

$$I_{acc}(\{p_i, \rho_i\}) \leq \chi(\{p_i, \rho_i\}) \equiv S(\bar{\rho}) - \sum_i p_i S(\rho_i), \quad (5)$$

where $\bar{\rho} = \sum_i p_i \rho_i$ is the average ensemble state, and $S(\varsigma) = -\text{tr}(\varsigma \log_2 \varsigma)$ is the von Neumann entropy of ς .

Since the Holevo bound can be achieved asymptotically [27–30], we define the capacity of dense coding for the state ρ_{AB} as

$$\mathcal{C}(\rho) = \max_{p_i, U_i} \chi(\{p_i, \rho_i\}) \equiv \max_{p_i, U_i} \left(S(\bar{\rho}) - \sum_i p_i S(\rho_i) \right). \quad (6)$$

The maximization involved in the capacity can be performed [31–36] (see also [37]), and we obtain

$$\mathcal{C}(\rho_{AB}) = \log_2 d_A + S(\rho_B) - S(\rho),$$

where $\rho_B = \text{tr}_A \rho_{AB}$ is Bob’s part of the state ρ_{AB} . The classical limit being at $\log_2 d_A$, the bipartite quantum state ρ_{AB} is useful for dense coding if and only if

$$S_{A|B}(\rho_{AB}) = S(\rho) - S(\rho_B) < 0.$$

This reminds us of the classical conditional entropy (using Shannon, instead of von Neumann, entropy). While the classical expression is always positive, the corresponding quantum one (obtained by simply replacing the Shannon entropies by the von Neumann ones) can be negative, and exactly those bipartite quantum states which produce such a negative quantity are the ones which are useful for quantum dense coding (cf. [38, 39], see also [40]). Such states

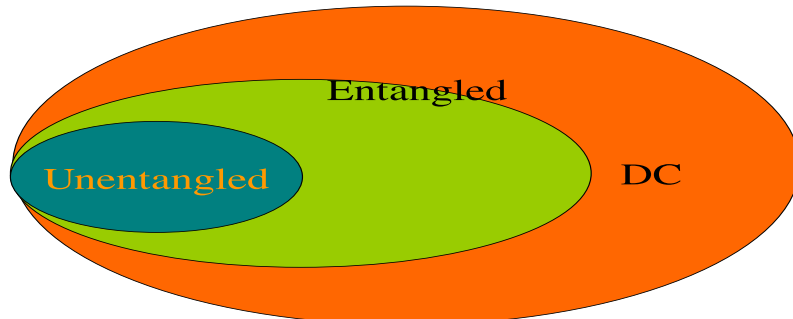


FIG. 3: Classification of bipartite quantum states according to their usefulness in dense coding. The innermost region consists of unentangled (separable) states. The shell surrounding it contains states that are all entangled, but are not useful for dense coding. The outermost shell is that of the dense-codeable states. It can be shown that both separable and non-DC states form convex sets [17, 41].

will be called dense-codeable (DC) states. DC states exist, an example being the singlet state. It can be shown that no separable state can be used for dense coding [42]. Interestingly however, not all entangled states are useful for dense coding: there exist entangled states which have a positive $S_{A|B}$ [43]. This leads us to a classification of bipartite quantum states that is finer than that given by the entanglement-separability paradigm (see Fig. 3.)

2. Beyond the Bipartite Setting: Networks

Let us now briefly consider the relatively uncharted domain of quantum networks and their classical information transfer capabilities. To begin, let us consider a situation where we want to use an N -particle quantum state ρ shared between N distant parties, with each party in possession of one particle in the beginning. Let us further suppose that we consider a situation where, of the N partners in the network, $N - 1$ are to act as senders (call them A_1, A_2, \dots, A_{N-1} , and there is a single receiver (call him Bob (B)). The senders want to send classical information to Bob by using the multiparty quantum state as a channel. It is possible to find the capacity of the multiparty quantum state for this classical communication task [36], and is given by

$$\mathcal{C}_{\{A_i\} \rightarrow B}(\rho_{A_1 \dots A_{N-1} B}) = \mathcal{C}_{\{A_i\} \rightarrow B}^{CL} + S(\rho_B) - S(\rho_{A_1 \dots A_{N-1} B}),$$

where the classical limit in this situation is given by

$$\mathcal{C}_{\{A_i\} \rightarrow B}^{CL} = \log_2 d_{A_1} + \log_2 d_{A_2} + \dots + \log_2 d_{A_{N-1}}.$$

In this case therefore, the state ρ is dense-codeable if and only if

$$S(\rho_{A_1 \dots A_{N-1} B}) - S(\rho_B) < 0,$$

with d_{A_i} being the dimension of the Hilbert space corresponding to the particle in possession of A_i .

The complexity of the encoding-decoding processes increases in the case when there are more than one receivers, and the dense coding network between an arbitrary number of senders and an arbitrary number of receivers is as yet not solved, although some initial attempt was made to obtain the capacity in the case of an arbitrary number of senders and two receivers [36, 44].

Further work on manipulation of classical information in multiparty quantum systems include Ref. [45], where a quantitative connection is established between the amount of lost classical information about a quantum state and the concomitant loss of entanglement, and Ref. [46], where superadditivity of classical capacities of multi-access quantum channels is revealed.

IV. THE QUANTUM NO-CLONING THEOREM

Before proceeding further, we briefly discuss the no-cloning theorem in quantum mechanics. This will be important for our considerations in the succeeding sections, regarding quantum information transmission, as well as secret classical information transmission.

Suppose that a source produces the quantum states $|\psi_0\rangle$ and $|\psi_1\rangle$. And our goal is to prepare two copies of the output. Unitarity of quantum mechanical evolutions makes such a goal impossible, unless $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal [47]. More precisely, we want to have the transformations

$$|\psi_0\rangle|B\rangle|M\rangle \rightarrow |\psi_0\rangle|\psi_0\rangle|M_0\rangle \quad \text{and} \quad |\psi_1\rangle|B\rangle|M\rangle \rightarrow |\psi_1\rangle|\psi_1\rangle|M_1\rangle, \quad (7)$$

by the same quantum mechanical evolution. Here $|B\rangle$ is the blank state on which the copy is to surface. And $|M\rangle$ is the initial state of the copying machine. $|M_0\rangle$ and $|M_1\rangle$ are also machine states. So what we want is to “clone” the given state. Such machines are available to us in the classical world. The photo-copying machine in shops and offices does exactly this job: A paper containing whatsoever information is fed into the machine, along with a blank paper, and we get a copy of the original – plus the original – after the job is completed, and the machine is maybe a bit heated-up after the job. Such clones are also being tried with considerable success in the biological world. A parallel machine does not however exist in the quantum world. One may check that there is no single unitary operator by which both the transformations in (7) is possible, unless $|\psi_0\rangle$ and $|\psi_1\rangle$ are orthogonal.

Although exact cloning is not possible for arbitrary quantum states, it is possible to quantum mechanically clone a given set of states inexactly. This was first considered by Bužek and Hillery [48]. Optimizations were considered by Bruß et al. [49] (see also [50]). Such inexact – but near-optimal – quantum cloners have actually been realized in the laboratory (see e.g. [51]).

No-information leaking: Producing an exact clone of a state of a physical system is an extreme form of information gathering from the system. Is it possible to leak out a small amount of information about the state of a physical system, while still keeping the original state intact? Precisely, we want to have the transformations

$$|\psi_0\rangle_S|E\rangle_E \rightarrow |\psi_0\rangle_S|E_0\rangle_E \quad \text{and} \quad |\psi_1\rangle_S|E\rangle_E \rightarrow |\psi_1\rangle_S|E_1\rangle_E, \quad (8)$$

by the same quantum mechanical evolution. Here the suffixes S and E denote “system” and “environment”. If $|E_0\rangle_E$ and $|E_1\rangle_E$ are different for different $|\psi_0\rangle_S$ and $|\psi_1\rangle_S$, we will have leaked out information about whether the system is in $|\psi_0\rangle_S$ or $|\psi_1\rangle_S$, without disturbing (i.e. changing) the state of the system. However, it is easy to show that again such a transformation is not allowed in the quantum world, unless $|\psi_0\rangle_S$ and $|\psi_1\rangle_S$ are orthogonal.

V. QUANTUM STATE TRANSFER USING ENTANGLED STATES: TELEPORTATION

In Sec. III, we considered transmission of classical information using quantum states. In this section, we will consider transmission of quantum information via quantum states. Just as in Sec. III, we will begin with the case when there is a single sender and a single receiver. The task of the sender, Alice, is to send an arbitrary quantum state to a distant receiver, Bob, with whom she has a previously shared bipartite quantum state. We begin with the case when this shared state is the singlet and when the sent quantum state is a qubit, as was done in the first paper that considered the protocol. The protocol was called quantum teleportation [4]. In addition to the shared bipartite quantum state that is to be used by Alice and Bob as the resource for sending the arbitrary qubit, Alice and Bob are also allowed to use a limited amount of classical communication.

If the qubit is in a known state (known only to the sender, and not the receiver), then the sender may try to send that knowledge to the receiver, classically, say over a phone line. However, this requires an infinite number of bits of classical data transfer, as an arbitrary (pure) qubit can be written as $\cos(\theta/2)|0\rangle + \exp(i\phi)\sin(\theta/2)|1\rangle$ ($\theta \in [0, \pi]$, $\phi \in [0, 2\pi)$), which can be represented as a point on a unit sphere, the “Bloch” or the “Poincaré” sphere. For an arbitrary qubit, Alice needs to send the information about θ and ϕ to Bob, and sending it classically requires an infinite amount of data transfer, as the range of these parameters are continuous infinities. Sending the information over a classical channel is not an option in the case when the qubit is in an unknown state and only a single copy is provided, as it is not possible to find the state of a qubit from a single copy. Since an unknown qubit cannot be cloned, as we saw in the preceding section, it is not possible to produce many copies from the given single copy.

Readers should notice that in quantum state transmission, we use a different set of resources than in classical information transmission, discussed in Sec. III. In the latter case, considering only the situation of a single sender and a single receiver (the other cases being similar), the resources were the entangled shared state between the sender and the receiver, and the noiseless quantum channel from the sender to the receiver. In particular, classical communication, say over a phone line, between the sender and the receiver was forbidden: Sending classical communication is the

Measurement outcome at Alice	State created at Bob
$ \psi^-\rangle$	$ \chi\rangle$
$ \psi^+\rangle$	$\sigma_z \chi\rangle$
$ \phi^-\rangle$	$\sigma_x \chi\rangle$
$ \phi^+\rangle$	$\sigma_y \chi\rangle$

TABLE I: Correlations between measurement results at Alice and the corresponding states at Bob.

task of the protocol. In the quantum case, the resources are the entangled shared state between the sender and the receiver, and a limited amount of classical communication. Quantum communication – say over a noiseless quantum channel – is forbidden: Sending quantum states is in this case the task of the protocol.

We now describe the protocol of quantum mechanically teleporting a qubit from Alice to Bob, where the previously shared quantum state is the singlet. Alice wants to send an arbitrary quantum state $|\chi\rangle = a|0\rangle + b|1\rangle$, where a and b are complex numbers with the normalization $|a|^2 + |b|^2 = 1$. To send the state, Alice performs a measurement in the Bell basis, $\{|\psi^\pm\rangle, |\phi^\pm\rangle\}$, on the four-dimensional space formed by her part of the singlet and the input state $|\chi\rangle$. Depending on the measurement results, there are different states created at Bob’s end, as shown in the following table. This can be easily checked by explicit calculation. For example, if the outcome at Alice’s end is $|\phi^-\rangle$, the state created at Bob is $(\langle\phi^-|)_{1A}(|\chi\rangle_1 \otimes |\psi^-\rangle_{AB})$, which is exactly $\sigma_x|\chi\rangle$, upto a constant multiple. We have ignored multiplicative phases in the above table. We use the suffix “1” to denote the input qubit.

Alice communicates the result of the measurement to Bob over a classical channel. Note that the number of bits that needs to be sent is 2 (corresponding to four outcomes).

Depending on the message received by Bob, he performs one of the unitaries $\{\mathbb{I}, \sigma_i, i = x, y, z\}$ on his particle according to the following instruction set.

Measurement outcome at Alice	Unitary applied by Bob
$ \psi^-\rangle$	\mathbb{I}
$ \psi^+\rangle$	σ_z
$ \phi^-\rangle$	σ_x
$ \phi^+\rangle$	σ_y

After performing the unitary operation, Bob’s state is exactly in the state $|\chi\rangle$, the state used by Alice as the initial state. We have therefore been able to use an entangled quantum state (the singlet) to send an arbitrary qubit from Alice to Bob, without actually sending the qubit down a quantum channel. The protocol is pictorially depicted in Fig. 4.

Can one use the quantum teleportation protocol for (superluminal) signaling? In the protocol as given above, Alice sends the measurement outcome to Bob over a classical channel, which will of course respect special relativity. But what if Alice does not send her message? The states in the right column of Table 1 are still created at Bob’s end. However, without Alice’s message, Bob only knows that a measurement onto the basis $\{|\psi^\pm\rangle, |\phi^\pm\rangle\}$ is performed by Alice, and that any one of the states $\{|\psi^\pm\rangle, |\phi^\pm\rangle\}$ are obtained by her – he does not know which! To find his post-measurement state, Bob must therefore consider a mixture of the states in the right column of Table 1, with the corresponding probabilities – which he can find out by using Born rule. A simple calculation shows that the resulting mixture is the completely unpolarized state, and is equal to his pre-measurement state $\text{tr}_A(|\psi^-\rangle\langle\psi^-|)$. Quantum teleportation therefore does not help us to signal.

The second question is whether one can use quantum teleportation for violating the no-cloning theorem. The answer is again negative. Although an exact copy of the input state is created at Bob’s end, the original copy is completely destroyed. The post-measurement state of Alice does not contain any information whatsoever about the input state $|\chi\rangle$: The output states at Alice are the states of the Bell basis and are independent of a and b . So are the probabilities of their occurrence.

Experimental realization of quantum teleportation has been achieved in many physical systems, like photons, ions, and light-matter interface. See e.g. [52].

A. Teleportation with Nonmaximally Entangled Bipartite States

A shared singlet state, along with limited classical communication, supports an exact transfer of a qubit. Nonmaximally entangled states, however, do not enjoy such a feature. To go further, we have to introduce the concept of

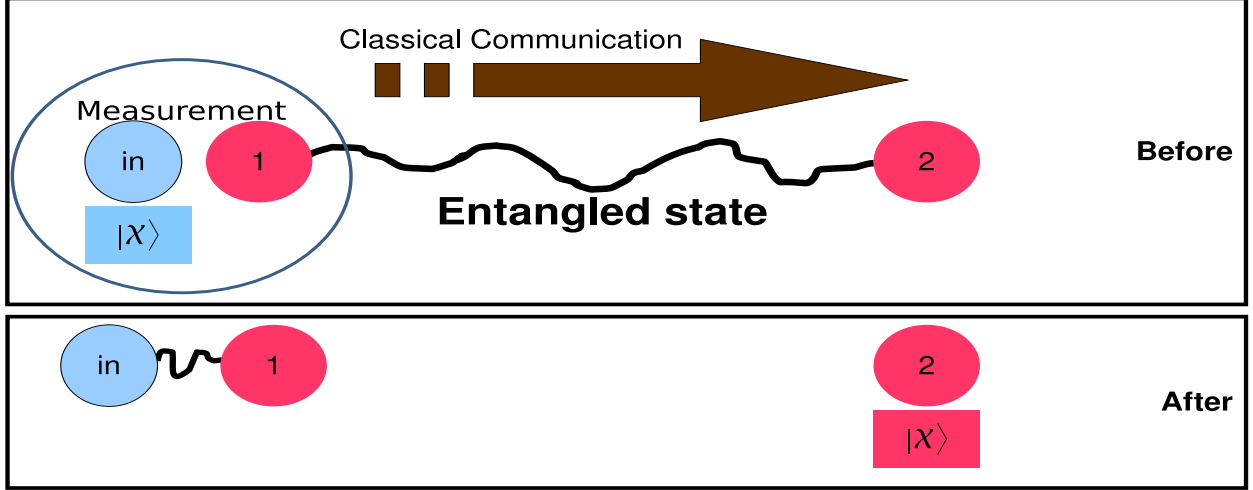


FIG. 4: A pictorial description of the teleportation protocol.

“fidelity”. Suppose that a machine promises to produce a quantum state $|\psi\rangle$. However, it actually produces the state ζ , which may be mixed [53]. We then say that the machine has the fidelity $\langle\psi|\zeta|\psi\rangle$. In case the machine is exact, the fidelity is unity. In connection to quantum teleportation, suppose that Alice and Bob share the quantum state ρ_{AB} , defined on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. For simplicity, we assume that $\dim \mathcal{H}_A = \dim \mathcal{H}_B = d$. The task now is to transfer the state $|\psi\rangle$ of a d -dimensional quantum system from Alice to Bob by using the quantum state ρ_{AB} as a quantum channel. Suppose that the state produced at Bob’s end after the teleportation protocol is $\zeta(\psi)$. Then the fidelity of the teleportation protocol is

$$F = \int \langle\psi|\zeta(\psi)|\psi\rangle d\psi / \int d\psi,$$

where we have included a uniform average over the d -dimensional Hilbert space of the input state.

If Alice and Bob do not share the quantum state ρ , but Alice still wants to send the unknown quantum system $|\psi\rangle$ – of which she has a single copy – to Bob by sending classical information over a classical channel, the fidelity that she can reach is just $2/(d+1)$. The optimal protocol for Alice to follow is to measure the quantum state $|\psi\rangle$ in an arbitrary basis, and send the measurement outcome to Bob, after which Bob prepares a quantum system in that basis state. Let us call the limit $2/(d+1)$ as the classical fidelity [54].

There do exist nonmaximally entangled states that support quantum teleportation with a fidelity that is higher than the classical fidelity. An important result was obtained by the Horodeccy family, where they found a relation between the optimal teleportation fidelity and the singlet fraction (fidelity of a two-party state to the corresponding maximally entangled state) [54] (see also [55]), and ruled out the ability of a large class entangled quantum states to teleport with fidelity beyond the classical limit.

B. Quantum Networks carrying Quantum Information

There are many interesting examples of quantum information transmission in quantum networks, and below we provide a necessarily incomplete selection. The subject is replete with open problems.

1. Entanglement Swapping

Close on the heels of the teleportation paper, came the paper on entanglement swapping [56] (see also [57]), which, along with giving an interesting example of quantum information transmission and a proposal for preparation of bipartite entangled states, also led to a re-thinking of the definition of entangled states. Let us first describe the protocol. Suppose that two distant observers Alice and Bob share the singlet state. Two other observers, Charu and Debu, share another singlet. We assume that Alice and Debu have never met in the past and neither do they have a quantum channel between them – i.e. their particles have never interacted. The particles with Alice and Bob have of course interacted in the past, as otherwise they could not have been in the singlet state. Also Charu’s and Debu’s particles must have interacted in the past. Now suppose that Bob and Charu meet and perform a measurement on the particles that they carry. It turns out that it is now possible for Alice and Debu – whose particles have never interacted in the past – to share an entangled state. There have been several experiments that have realized entanglement swapping [58]. The concept has been found to be useful e.g. for proposals to realize long distance quantum communication via “quantum repeaters” (see e.g. [59, 60]).

2. Quantum Telecloning

Quantum telecloning is a natural generalization of the original teleportation protocol to the case where there is still a single sender, but many receivers [61]. [A similar protocol was previously considered in Ref. [49].] Suppose that Alice is in possession of a qubit in an unknown state $|\psi\rangle$. She wishes to send it to $N - 1$ distant receivers B_1, B_2, \dots, B_{N-1} ($N > 2$). Producing exact copies at all these locations is forbidden by the no-cloning theorem. However, Alice may try to prepare $N - 1$ inexact copies of $|\psi\rangle$ and send it to the $N - 1$ distant locations by using $N - 1$ singlets which she happens to share with the $N - 1$ distant receivers. Murao *et al.* showed that the same result can be obtained if Alice and her $N - 1$ associates share particular multipartite entangled states, in which case only $O(\log_2(N - 1))$ singlets are required. The protocol has been experimentally realized – see [62], and references therein.

3. Multi-access Channels and Multiparty Entanglement

For a pure *bipartite* quantum state, a higher entanglement implies higher capacities for sending both classical and quantum information by using the bipartite state as a quantum channel [3, 4, 31, 32, 34–36, 63, 64]. This relatively simple image in the bipartite domain is not mirrored in the case of many senders and many receivers. More precisely, two types of multi-access quantum channels, motivated by distillation protocols in multiparty quantum networks, were defined in Ref. [65], and it was shown that the capacities of these channels cannot be correlated with *any* multiparty entanglement measure.

VI. QUANTUM CRYPTOGRAPHY

Until now, we have discussed about communication protocols that do not have a security aspect. In this section, we will deal with protocols for sending *secret* classical information over a quantum channel. It is worthwhile to mention here that among the exciting achievements in quantum information science during the last few years, the experimental success of quantum cryptography is one of the foremost [66].

A typical cryptographic scheme consists of a sender, Alice, who wants to send some classical message to a receiver, Bob, secretly. Since all messages can be written as a sequence of binary digits (0’s and 1’s), we suppose that Alice has a sequence P of 0’s and 1’s which she wants to send to Bob. This is known in cryptographic parlance as “plaintext”. If we now suppose that Alice and Bob have a previously shared “secret key” K – a random sequence of 0’s and 1’s that both Alice and Bob know, but nobody else knows it – which is at least as long as the plaintext, then Alice will be able to send her plaintext secretly to Bob, by a protocol known as the “one-time pad”. The protocol can be described as follows. Alice adds (bitwise addition modulo 2) P and K to obtain the “ciphertext” C , and sends it down a classical

channel to Bob. Since K is random, C is also random, and hence it is not possible to get any information from it. So, even if an eavesdropper (it is usual to call her “Eve”) gets hold of C , she is not able to decipher it. However, once it reaches Bob, he again adds K to C , to obtain the original plaintext P . As an illustration, suppose that Alice wants to send some message which is 01010110 – the plaintext. Moreover, Alice has a random sequence of binary digits, 00111001 – the key. Bob has exactly the same random sequence, but nobody else has it. Alice encodes her message by adding the message to the key:

$$\begin{aligned} \text{Plaintext} + \text{key (modulo 2)} &= \text{ciphertext}, \\ \text{i.e. } 01010110 + 00111001 \text{ (modulo 2)} &= 01101111. \end{aligned}$$

After the binary addition, Alice sends the ciphertext to Bob, who after obtaining it goes through the decoding process:

$$\begin{aligned} \text{Ciphertext} + \text{key (modulo 2)} &= \text{plaintext}, \\ \text{i.e. } 01101111 + 00111001 \text{ (modulo 2)} &= 01010110. \end{aligned}$$

This process of sending a secret message is completely secure, provided the key is never re-used. Therefore, having shared secret keys is sufficient to implement cryptography. Generation of such secret keys is trivially possible if Alice and Bob meet before they actually send the encoded message. The question is whether they can generate secret keys without meeting.

The cryptography problem therefore boils down to a key distribution protocol. Generation of such secret keys, without meeting, is possible both in the classical and the quantum worlds. In both cases, the security depends on some unproven premises. In the classical case, the security of practical key distribution protocols depends on the unproven premise of the hardness in solving certain mathematical equations. Discussion of such classical protocols is beyond the scope of this review [13]. In the quantum case, the security of the quantum key distribution protocols depends on the validity of quantum physics.

We will now discuss the protocol of quantum key distribution known as the Bennett-Brassard 1984 (BB84) protocol [1]. Of the striking facts of the protocol is that it does not involve shared entangled states between the sender and the receiver. To begin, the sender, Alice, randomly chooses one of the following two bases:

$$\begin{aligned} \text{Basis } Z &= \{|0\rangle, |1\rangle\}, \\ \text{Basis } X &= \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\}. \end{aligned} \quad (9)$$

As the names suggest, they are formed by respectively the eigenvectors of the Pauli spin matrices σ_z and σ_x . After choosing the basis, she randomly chooses a state from that basis, prepares a qubit in that state, and sends the qubit to Bob over a quantum channel. After obtaining the state, Bob randomly measures in basis Z or basis X . Alice and Bob then publicly declare (e.g. by advertising on a newspaper) their bases – Alice conveys the basis that she chose for preparing the qubit, and Bob discloses the basis in which he measures. They certainly do *not* declare the states – Alice does not announce the state she prepared, and Bob does not reveal the state he obtained as the measurement outcome. They repeat this procedure over many runs. For each run, Alice notes down a 0 if she had chosen an eigenvector corresponding to the eigenvalue +1, i.e. if she had chosen either $|0\rangle$ of basis Z or $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ of basis X . She notes down a 1 otherwise. Similarly, if Bob measures in the basis Z , and gets the outcome $|0\rangle$ (therefore corresponding to eigenvalue +1 of σ_z) or if he measures in the basis X , and gets the outcome $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ (again corresponding to eigenvalue +1, but of σ_x), he notes down a 0. He notes down a 1 otherwise. In this way, they obtain a sequence of 0’s and 1’s. Due to the preparation procedure, at least the sequence at Alice is a random one. The one at Bob may depend on the noise in the quantum channel, which may in principle be due to an eavesdropper who is trying to get information about the sent qubits. After the bases are publicly declared, Alice and Bob remove the entries in their corresponding binary sequences that correspond to runs for which the bases did not match.

At this stage, if there is no noise in the quantum channel, the binary sequences at Alice and Bob should exactly match. Let us consider a few exemplary runs, where for simplicity we suppose that there is no noise in the channel.

	Alice’s state	Alice’s bit	Bob’s basis	Bob’s bit	Decision
Run 1	$ 0\rangle$	0	X	?	⊗
Run 2	$(0\rangle + 1\rangle)/\sqrt{2}$	0	X	0	⊗
Run 3	$ 1\rangle$	1	Z	1	⊗
Run 4	$ 1\rangle$	1	Z	1	⊗
Run 5	$(0\rangle - 1\rangle)/\sqrt{2}$	1	Z	?	⊗

We put a question mark to indicate the runs when Bob’s basis does not match with that of Alice, and therefore although Bob does get a measurement outcome in these cases, the outcome does not have any correlation with the state of Alice. These are exactly the runs (runs 1 and 5) for which Alice and Bob remove the entries in their respective binary digit columns (column 3 for Alice, and column 5 for Bob). Note that the binary sequence with Alice, after removal of the non-matchings, is 011, which is the same as that with Bob.

But what if the eavesdropper Eve is operating on the quantum channel that carries the qubits from Alice to Bob? Since the set of states that Alice sends to Bob contains mutually nonorthogonal states, the no-information leaking theorem (as discussed in Sec. IV) implies that Eve will not be able to obtain any information about the sent qubits without disturbing them. Such disturbance will then show up in the measurement results of Bob: The binary sequence at Alice and that at Bob will not match exactly. Therefore to find whether Eve is operating on the channel (i.e. whether Eve has obtained any information about the sent qubits), Alice now publicly announces some randomly chosen bits of her binary sequence, and Bob publicly declares the bits at exactly those positions in his binary sequence. If there is no mismatch, Alice and Bob can be sure, within statistical uncertainty, that the *rest* of the binary sequences can be used as a shared key. And if there is a mismatch, it implies that Eve has some information about the sent qubits. In that case, they need to start afresh. This is the BB84 protocol, and the security of this key distribution scheme depends on the validity of the statement of the no-information leaking theorem. The theorem is of course valid within the purview of quantum mechanics.

The situation is quite different when the protocol is actually realized. In that case, “Alice” and “Bob” will be using some real quantum channel, which will produce some noise on its own (i.e. even without the presence of Eve). But Alice and Bob have no way but to consider that all the noise have been generated by Eve. Moreover, it may be the case that Eve is always operating on the channel, and therefore there is always a mismatch in the binary sequences at Alice and Bob. Quantum mechanics is able to provide security for keys generated in such scenarios as well. See [66], and references therein for further details.

As mentioned earlier, the BB84 protocol does not involve any entanglement. In 1991, A. Ekert [2] discovered a key distribution protocol that uses entangled states for sharing secret keys. However, one can show that entanglement-based protocols – like the Ekert 1991 (E91) protocol – are equivalent, in principle, to protocols that employ quantum channels but do not require entanglement – like the BB84 protocol [16, 66–68]. This is the status for the case when we are considering security of key distribution protocols involving a single sender and a single receiver. The situation however changes in networks, as we will mention later.

A. Quantum Cryptography in Networks

There are several interesting quantum cryptographic schemes in the multi-user domain (i.e. beyond the single-sender single-receiver scenario). These include secret sharing [69, 70], and the somewhat different Byzantine agreement problem [71]. Below we briefly consider the secret sharing protocols and some of its security aspects.

1. Secret Sharing

Secret sharing [69] (cf. [70]) is a communication task in which a sender, Alice, wants to send a (classical) message to several recipients (called “Bobs” – B_1, B_2, \dots), so that each of the Bobs individually knows nothing about the message, but can recover its content once they cooperate. For simplicity, let us consider the case of two receivers. For transmitting a binary message string $\{a_i\}$, Alice can send a random sequence of bits, $\{b_{1,i}\}$, to B_1 , and the sequence $\{b_{2,i}\} = \{a_i + b_{1,i}\}$ to B_2 , where again we are considering bitwise addition modulo 2. Since $a_i = b_{1,i} + b_{2,i}$, we are assured that the Bobs can recover the message if they cooperate, and yet none of them can learn anything about the message of Alice on his own, since the sequences $\{b_{1,i}\}, \{b_{2,i}\}$ are completely random. In addition to the requirement that the receivers must not learn anything about the message unless they cooperate, it is also demanded that no third (actually fourth (!), assuming that there are two receivers) party learns about the message sent by Alice. The demands can be met by using the single-sender single-receiver quantum cryptography protocols described before (e.g. by the BB84 or the E91 schemes). The procedure goes as follows: Alice establishes secret random keys, independently, with both Bobs, and uses them as one-time pads to securely send bits in the way required by secret sharing. Let us call this the BB84^{⊗2} protocol. However, as argued in [69], a more natural way of using quantum states in secret sharing is to send entangled states to the Bobs, and as a result, avoid establishing random keys with each of the Bobs separately, by combining the quantum and classical parts of secret sharing in a single protocol. The authors of [69] go on to describe a protocol that involves sending four bipartite entangled states by Alice to the two Bobs. Since it uses four entangled states, let us call the protocol as the E4 protocol. The secret sharing protocol has been experimentally realized. See e.g. [72].

Entanglement enhances security in quantum communication: As mentioned before, entanglement has been identified as the essential ingredient in quantum communication without a security aspect, e.g., in quantum dense coding and quantum teleportation. However in secure quantum communication, if we restrict ourselves to the case of a single sender and a single receiver, entanglement-based protocols are equivalent to the product state-based ones. Entanglement is also useful in secure quantum communication, but one has then to go beyond the bipartite case.

Let us again consider the secret sharing scheme described before, and let us begin with the case when the eavesdropper has access to global quantum operations on both the quantum channels – one from Alice to B_1 and another from Alice to B_2 . In this case, the security analyses of the E4 secret sharing protocol and the single-sender single-receiver BB84 cryptographic protocol are isomorphic, as both protocols make use of four nonorthogonal states with the same mutual scalar products. See [69] (cf. [73]). However such “global” eavesdropping attacks are not the most important ones in a cryptographic scenario with separated receivers, as in secret sharing.

Ref. [74] finds optimal eavesdropping attacks, both for E4 and BB84^{⊗2} protocols, that are *local* – there are two eavesdroppers, one acting with local quantum operations on the $A \rightarrow B_1$ quantum channel while the other attacking with the same class of operations on the $A \rightarrow B_2$ one, and they communicate among themselves over a (secure!) classical channel. It turns out that the entanglement-based E4 protocol provides a higher security threshold than the product state-based BB84^{⊗2} one, in terms of what is known as the “tolerable quantum bit error rate”.

VII. IN LIEU OF A CONCLUSION

Being a young subject, there is no dearth of open problems in quantum information in general, and in quantum communication in particular. A criterion to detect entanglement is not known even in the bipartite regime. Characterization and quantification of entanglement is difficult even for pure states in the multiparty case. Many classical and quantum information transmission protocols have been theoretically proposed and several of them have already been realized in the laboratory in different physical systems for the case of a single sender and a single receiver. But quantitative understanding is missing in many cases, and many additivity questions are unanswered. On the experimental front, achieving high fidelities and long distances are some of the main difficulties. The complexity of the multiparty terrain – both on the theoretical and experimental fronts – restricts the study of information transfer in such systems.

However, a lot of progress has been made in the past decade and a half in the understanding of the theoretical aspects of this new science, and experiments realizing quantum communication protocols have in the meanwhile metamorphosed from table-top ones to those between nearby towns and even between nearby islands.

-
- [1] C.H. Bennett and G. Brassard, in *Proceedings of the International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, NY, 1984).
 - [2] A.K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
 - [3] C.H. Bennett and S.J. Wiesner, *Phys. Rev. Lett.* **69**, 2881 (1992).
 - [4] C.H. Bennett, G. Brassard, C. Crépeau, R. Josza, A. Peres, and W.K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
 - [5] J.-W. Pan, Z.-B. Chen, M. Żukowski, H. Weinfurter, and A. Zeilinger, [arXiv:0805.2853](https://arxiv.org/abs/0805.2853) [quant-ph].
 - [6] H. Häffner, C.F. Roos, and R. Blatt, *Phys. Rep.* **469**, 155 (2008); L.-M. Duan and C. Monroe, *Rev. Mod. Phys.* **82**, 1209 (2010); K. Singer, U. Poschinger, M. Murphy, P. Ivanov, F. Ziesel, T. Calarco, and F. Schmidt-Kaler, *Rev. Mod. Phys.* **82**, 2609 (2010).
 - [7] D. Jaksch, *Contemp. Phys.* **45** 367 (2004); D. Jaksch and P. Zoller, *Ann. Phys.* **315** 52 (2005).
 - [8] L.M.K. Vandersypen and I. L. Chuang, *Rev. Mod. Phys.* **76**, 1037 (2005).
 - [9] Y. Makhlin, G. Schön, and A. Shnirman, *Rev. Mod. Phys.* **73**, 357 (2001).
 - [10] J.M. Raimond, M. Brune, and S. Haroche, *Rev. Mod. Phys.* **73**, 565 (2001)
 - [11] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Rev. Mod. Phys.* **81**, 865 (2009).
 - [12] P. Kok, W.J. Munro, K. Nemoto, T.C. Ralph, J.P. Dowling, and G.J. Milburn, *Rev. Mod. Phys.* **79**, 135 (2007).
 - [13] J. Talbot and D. Welsh, *Complexity and Cryptography: An Introduction* (CUP, Cambridge, 2006).
 - [14] See e.g. M.A. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information* (CUP, Cambridge, 2000); *Lectures on Quantum Information*, eds. D. Bruß and G. Leuchs (Wiley, Weinheim, 2006).
 - [15] The terms “easy” and “hard” used here have precise meanings in complexity theory. See e.g. [13].
 - [16] An exception is the scenario of device-independent security proofs. See e.g. Ref. [2], and N. Gisin, S. Pironio, and N. Sangouard, *Phys. Rev. Lett.* **105**, 070501 (2010); K. Horodecki, M. Horodecki, P. Horodecki, R. Horodecki, M. Pawłowski, and M. Bourennane, [arXiv:1006.0468](https://arxiv.org/abs/1006.0468) [quant-ph]; L. Masanes, S. Pironio, and A. Acín, [arXiv:1009.1567](https://arxiv.org/abs/1009.1567) [quant-ph]; E. Hänggi and R. Renner, [arXiv:1009.1833](https://arxiv.org/abs/1009.1833) [quant-ph].
 - [17] R.F. Werner, *Phys. Rev. A* **40**, 4277 (1989).

- [18] R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Oemer, M. Fuerst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, *Nature Phys.* **3**, 481 - 486 (2007).
- [19] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, *Phys. Rev. Lett.* **81**, 3563 (1998).
- [20] A. Aspect, P. Grangier, and G. Roger, *Phys. Rev. Lett.* **47**, 460 (1981).
- [21] N. Lütkenhaus, J. Calsamiglia, and K.-A. Suominen, *Phys. Rev. A* **59** 3295 (1999).
- [22] K. Mattle, H. Weinfurter, P.G. Kwiat, and A. Zeilinger, *Phys. Rev. Lett.* **76**, 4656 (1996); T. Schaetz, M.D. Barrett, D. Leibfried, J. Chiaverini, J. Britton, W.M. Itano, J.D. Jost, C. Langer, and D.J. Wineland, *Phys. Rev. Lett.* **93**, 040505 (2004).
- [23] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley, New York, 1991).
- [24] J.P. Gordon, in *Proc. Int. School Phys. "Enrico Fermi, Course XXXI"*, ed. P.A. Miles, p. 156 (Academic Press, New York, 1964); L.B. Levitin, in *Proc. VI National Conf. Inf. Theory, Tashkent*, p. 111 (1969); A.S. Holevo, *Probl. Pereda. Inf.* **9**, 3 1973 [*Probl. Inf. Transm.* **9**, 110 (1973)].
- [25] R. Josza, D. Robb, and W.K. Wootters, *Phys. Rev. A* **49**, 668 (1994).
- [26] B. Schumacher, M. Westmoreland, and W. K. Wootters, *Phys. Rev. Lett.* **76**, 3452 (1996).
- [27] The Holevo bound is asymptotically achievable in the sense that if the sender Alice is able to wait long enough and send long strings of the input quantum states, then there exists a particular encoding and a decoding scheme that asymptotically attains the bound. Moreover, the encoding consists in collecting certain long and "typical" strings of the input states, and sending them all at once [28, 29]. Note however that the capacity defined here is the so-called "product" capacity, where we assume that during the encoding phase, we do not use entanglement over different uses of the channel. Very recently, it has been shown that using entangled encoding can actually lead to higher, as yet by a small amount, capacities [30].
- [28] B. Schumacher and M.D. Westmoreland, *Phys. Rev. A* **56**, 131 (1997).
- [29] A.S. Holevo, *IEEE Trans. Inf. Theory* **44**, 269 (1998).
- [30] M.B. Hastings, *Nature Phys.* **5**, 255 (2009).
- [31] S. Bose, M.B. Plenio, and V. Vedral, [quant-ph/9810025](https://arxiv.org/abs/quant-ph/9810025).
- [32] T. Hiroshima, *J. Phys. A: Math. Gen.* **34**, 6907 (2001).
- [33] G. Bowen, *Phys. Rev. A* **63**, 022302 (2001)
- [34] M. Horodecki, P. Horodecki, R. Horodecki, D. Leung, and B. Terhal, *Quantum Information and Computation* **1**, 70 (2001).
- [35] M. Ziman and V. Bužek, *Phys. Rev. A* **67**, 042321 (2003).
- [36] D. Bruß, G.M. D'Ariano, M. Lewenstein, C. Macchiavello, A. Sen(De), and U. Sen, *Phys. Rev. Lett.* **93**, 210501 (2004); D. Bruß, M. Lewenstein, A. Sen(De), U. Sen, G.M. D'Ariano, and C. Macchiavello, *Int. J. Quant. Inf.* **4**, 415 (2006).
- [37] X.S. Liu, G.L. Long, D.M. Tong, and F. Li, *Phys. Rev. A* **65**, 022304 (2002).
- [38] L. Henderson and V. Vedral, *J. Phys. A* **34**, 6899 (2001); H. Ollivier and W. H. Zurek, *Phys. Rev. Lett.* **88**, 17901 (2002).
- [39] J. Oppenheim, M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. Lett.* **89**, 180402 (2002); M. Horodecki, K. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De) and U. Sen, *Phys. Rev. Lett.* **90**, 100402 (2003); M. Horodecki, P. Horodecki, R. Horodecki, J. Oppenheim, A. Sen(De), U. Sen and B. Synak-Radtke, *Phys. Rev. A* **71**, 062307 (2005).
- [40] M. Horodecki, J. Oppenheim, and A. Winter, *Nature* **436**, 673 (2005).
- [41] A. Wehrl, *Rev. Mod. Phys.* **50**, 221 (1978).
- [42] R. Horodecki, P. Horodecki, and M. Horodecki, *Phys. Lett. A* **210**, 377 (1996).
- [43] M. Horodecki and P. Horodecki, *Phys. Rev. A* **59**, 4206 (1999); N.J. Cerf, C. Adami, and R.M. Gingrich, *ibid.* **60**, 898 (1999); K.G.H. Vollbrecht and M.M. Wolf, [quant-ph/0202058](https://arxiv.org/abs/quant-ph/0202058); T. Hiroshima, *Phys. Rev. Lett.* **91**, 057902 (2003).
- [44] P. Badziąg, M. Horodecki, A. Sen(De), and U. Sen, *Phys. Rev. Lett.* **91**, 117901 (2003).
- [45] J. Eisert, T. Felbinger, P. Papadopoulos, M.B. Plenio, and M. Wilkens, *Phys. Rev. Lett.* **84**, 1611 (2000).
- [46] L. Czekaj and P. Horodecki, *Phys. Rev. Lett.* **102**, 110505 (2009).
- [47] W.K. Wootters and W.H. Zurek, *Nature* **299**, 802 (1982); D. Dieks, *Phys. Lett. A* **92**, 271 (1982); P.W. Milonni and M.L. Hardies, *Phys. Lett. A* **92**, 321 (1982); H.P. Yuen, *Phys. Lett.* **113A**, 405 (1986).
- [48] V. Bužek and M. Hillery, *Phys. Rev. A* **54**, 1844 (1996).
- [49] D. Bruß, D.P. DiVincenzo, A. Ekert, C.A. Fuchs, C. Macchiavello, and J.A. Smolin, *Phys. Rev. A* **57**, 2368 (1998).
- [50] N. Gisin and S. Massar, *Phys. Rev. Lett.* **79**, 2153 (1997); R.F. Werner, *Phys. Rev. A* **58**, 1827 (1998); M. Keyl and R.F. Werner, *J. Math. Phys.* **40**, 3283 (1999); V. Scarani, S. Iblisdir, N. Gisin, and A. Acín, *Rev. Mod. Phys.* **77**, 1225 (2005).
- [51] A. Lamas-Linares, C. Simon, J.C. Howell, and D. Bouwmeester, *Science* **296**, 712 (2002).
- [52] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eible, H. Weinfurter, and A. Zeilinger, *Nature* **390** 575 (1997); D. Boschi, S. Branca, F. De Martini, L. Hardy, and S. Popescu, *Phys. Rev. Lett.* **80**, 1121 (1998); A. Furusawa, J.L. Sørensen, S.L. Braunstein, C.A. Fuchs, H.J. Kimble, E.S. Polzik, *Science* **282**, 706 (1998); M.A. Nielsen, E. Knill, and R. Laflamme, *Nature* **396**, 52 (1998); I. Marcikic, H. de Riedmatten, W. Tittel, H. Zbinden, and N. Gisin, *Nature* **421**, 509 (2003); M. Riebel, H. Häffner, C.F. Roos, W. Hänsel, J. Benhelm, G.P.T. Lancaster, T.W. Körber, C. Becher, F. Schmidt-Kaler, D.F.V. James and R. Blatt, *Nature* **429**, 734 (2004); M.D. Barrett, J. Chiaverini, T. Schaetz, J. Britton, W.M. Itano, J.D. Jost, E. Knill, C. Langer, D. Leibfried, R. Ozeri and D.J. Wineland, *Nature* **429**, 737 (2004); J. Sherson, H. Krauter, R.K. Olsson, B. Julsgaard, K. Hammerer, J.I. Cirac, and E.S. Polzik, *Nature* **443**, 557 (2006); S. Olmschenk, D. N. Matsukevich, P. Maunz, D. Hayes, L.-M. Duan, C. Monroe, *Science* **323**, 486 (2009).
- [53] We will not have occasion to consider the case when also the input to the machine is mixed.
- [54] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Rev. A* **60**, 1888 (1999).
- [55] See M.A. Nielsen, *Phys. Lett. A* **303** 249 (2002), and references therein.

- [56] M. Żukowski, A. Zeilinger, M.A. Horne, and A.K. Ekert, Phys. Rev. Lett. **71**, 4287 (1993); M. Żukowski, A. Zeilinger, and H. Weinfurter, Ann. N.Y. Acad. Sci. **755**, 91 (1995).
- [57] S. Bose, V. Vedral, and P.L. Knight, Phys. Rev. A **57**, 822 (1998); **60**, 194 (1999).
- [58] See e.g. J.-W. Pan, D. Bouwmeester, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **80**, 3891 (1998); X. Jia, X. Su, Q. Pan, J. Gao, C. Xie, and K. Peng Phys. Rev. Lett. **93**, 250503 (2004); H. de Riedmatten, I. Marcikic, J.A.W. van Houwelingen, W. Tittel, H. Zbinden, and N. Gisin, Phys. Rev. A **71**, 050302(R) (2005).
- [59] W. Dür, H.-J. Briegel, J.I. Cirac, and P. Zoller, Phys. Rev. A **59**, 169 (1999); H.-J. Briegel, W. Dür, J.I. Cirac, and P. Zoller, [quant-ph/9803056](https://arxiv.org/abs/quant-ph/9803056).
- [60] A. Sen(De), U. Sen, and M. Żukowski Phys. Rev. A **68**, 062301 (2003).
- [61] M. Murao, D. Jonathan, M. B. Plenio, and V. Vedral, Phys. Rev. A **59**, 156 (1999).
- [62] Z. Zhao, A.-N. Zhang, X.-Q. Zhou, Y.-A. Chen, C.-Y. Lu, A. Karlsson, and J.-W. Pan, Phys. Rev. Lett. **95**, 030502 (2005); S. Koike, H. Takahashi, H. Yonezawa, N. Takei, S.L. Braunstein, T. Aoki, and A. Furusawa, Phys. Rev. Lett. **96**, 060504 (2006); M. Radmark, M. Żukowski, and M. Bourennane, New J. Phys. **11**, 103016 (2009).
- [63] C.H. Bennett, H.J. Bernstein, S. Popescu, and B. Schumacher, Phys. Rev. A **53**, 2046 (1996).
- [64] P.W. Shor, The Quantum Channel Capacity and Coherent Information, Lecture at MSRI Workshop on quantum computation, 2002; Math. Program. **97**, 311 (2003).
- [65] A. Sen(De) and U. Sen, Phys. Rev. A **81**, 012308 (2010).
- [66] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
- [67] C.H. Bennett, G. Brassard, and N.D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
- [68] D. Bruß, M. Christandl, A.K. Ekert, B.-G. Englert, D. Kaszlikowski, and C. Macchiavello, Phys. Rev. Lett. **91**, 097901 (2003); M. Curty, M. Lewenstein, and N. Lütkenhaus, *ibid.* **92**, 217903 (2004); A. Acín and N. Gisin, *ibid.* **94**, 020501 (2005).
- [69] M. Żukowski, A. Zeilinger, M.A. Horne, and H. Weinfurter, Acta Phys. Pol. **93**, 187 (1998); M. Hillery, V. Bužek, and A. Berthiaume, Phys. Rev. A **59**, 1829 (1999).
- [70] R. Cleve, D. Gottesman, H.-K. Lo, Phys. Rev. Lett. **83**, 648 (1999); A. Karlsson, M. Koashi, and N. Imoto, Phys. Rev. A **59**, 162 (1999); K. Chen and H.-K. Lo, Quant. Inf. Comput. **7**, 689 (2007).
- [71] M. Fitzi, N. Gisin, and U. Maurer, Phys. Rev. Lett. **87**, 217901 (2001).
- [72] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Phys. Rev. Lett. **95**, 230505 (2005).
- [73] V. Scarani and N. Gisin, Phys. Rev. Lett. **87**, 117901 (2001); Phys. Rev. A **65**, 012311 (2002); A. Sen(De), U. Sen, and M. Żukowski, *ibid.* **68**, 032309 (2003).
- [74] R. Demkowicz-Dobrzański, A. Sen(De), U. Sen, and M. Lewenstein, Phys. Rev. A **80**, 012311 (2009).