Quantum Electronics **50** (5) 461–468 (2020)

https://doi.org/10.1070/QEL17200

Role of collective preparation and measurement of states in some quantum communication protocols

D.A. Kronberg

Abstract. **We consider related problems in quantum communications: distribution of information and a secret key between a sender and several receivers. We study the gain of participants of communication protocols both from the use of collective measurements and from collective actions at the transmitter's side related to the employment of entangled states and various actions on them.**

Keywords: *quantum information, classically quantum communication channel, communication protocol, superadditivity, entangled state, secret key.*

1. Introduction

An important object of research in quantum information is an ensemble of two nonorthogonal states, for which the following properties of quantum mechanics are essential:

(i) cloning is impossible for such states [1], and when trying to perform approximate cloning, the output states will differ from the initial ones [2];

(ii) broadcasting of such states is unavailable [3], that is, it is impossible to distribute the initial states to several participants (with admissible entanglement between them) so that the partial state of each participant coincides with the initial one;

(iii) transmitting information with the help of such states is superadditive [4, 5], that is, collective measurements over the entire transmitted sequence give more information than individual measurements with subsequent classical processing of the results; and

(iv) distributing the secret key according to the B92 quantum key distribution protocol is possible [6].

These phenomena arise from the impossibility of a reliable discrimination between nonorthogonal quantum states: If it were possible, then, in particular, one could prepare a copy of the initial state, and the eavesdropper in quantum cryptography could unnoticeably make such a copy for himself/herself. At the same time, quantum mechanics makes it possible to partially circumvent the prohibition of a reliable discrimination between nonorthogonal states, both with the help of error-free measurement, which is used in quantum cryptography and capable of giving complete information about the signal with some probability of success, and with the help of collective measurements, which is capable of giving more information compared with individual measurements, which is the essence of the phenomenon of superadditivity.

A quantitative description of the relationship of these phenomena with the characteristics of an ensemble of quantum states is an important scientific problem to which, as far as we know, a complete solution has not yet been obtained, despite a number of important results, such as the introduction of quantum discord as a measure of the 'quantumness' of correlations that are not always related with entanglement. The original definition of discord [7] is related to the phenomenon of quantum superadditivity, since it considers the difference between the maximum of achievable information and the maximum of information achievable in individual measurements. Later, other approaches to the definition of discord were proposed [8], for example, related to various metrics on a set of quantum states, but the question of the possibility of a quantitative description of many quantum phenomena through discord is still open.

The phenomenon of superadditivity is associated with the ability to apply collective measurements, while an ensemble of states is a separable product [9]. Of interest is the situation when entangled states are also applied to the channel input. An important result is that coding using entangled states in the general case can give an increase in mutual information [10], but it is achieved under rather difficult conditions.

In this paper, we consider simpler situations in which entangled states are used to communicate with several receivers, and entanglement makes it possible to overcome the limitations caused by the independent work of the receivers, as well as by their possible mistrust of each other when distributing secret keys. For various situations we obtained estimates for the total public mutual information between a sender and several receivers, as well as for the total length of the secret key in the case of an ideal channel between the sender and receivers.

Section 2 introduces the basic concepts, as well as describes the phenomenon of superadditivity and considers the gain from the use of collective observables for one of the simple situations, that is, the use of the repetition code. In Section 3, we consider the problems of distributing public information and a secret key between several users, in which the use of the repetition code is related to the problem of approximate clon-

D.A. Kronberg Steklov Mathematical Institute, Russian Academy of Sciences, ul. Gubkina 8, 119991 Moscow, Russia; Russian Quantum Center, Skolkovskoe sh. 45, 121353 Moscow, Russia; Moscow Institute of Physics and Technology (National Research University), Institutskii per. 9, 141701 Dolgoprudnyi, Moscow region, Russia; e-mail: dmitry.kronberg@gmail.com

Received 15 November 2019
Kvantovaya Elektronika **50** (5) 461–468 (2020)
Translated by I.A. Ulitkin

ing of quantum states. Section 4 is devoted to the same problems, but using entangled states instead of separable ones, which corresponds to the approximate broadcasting, and Section 5 discusses the use of entanglement distillation to produce independent ensembles for each participant. The Conclusion contains the main results of the work.

2. Gain from using collective observables

Consider a simple binary classically quantum (c-q) channel, that is, a channel with quantum states $\{|\psi_0\rangle, |\psi_1\rangle\}$ at the output, corresponding to the input classical signals 0 and 1, with the output states being nonorthogonal and noncoincident: $\langle \psi_0 | \psi_1 \rangle = \kappa \in (0,1)$. The sender selects the signals, and the receiver performs a measurement and concludes what state was sent. The observable Π in quantum mechanics is described by a set of nonnegative Hermitian operators summing up into the identity: $\Pi = \{M_i\}_i$: $M_i = M_i^* \geqslant 0$, $\sum_i M_i = I$. The probability of the outcome i when measuring the state ρ of the observable Π is defined as $p(i) = \mathrm{Tr}(\rho M_i)$.

In transmitting information, the key task is to maximise the mutual information between the sender and receiver under conditions of multiple transmission of states, where the use of codewords becomes important (see [9]). In binary coding, the classical codeword is $w = (x_1, \ldots, x_N)$, where $x_i \in (0,1)$ is mapped to the product state $S_w = |\psi_{x_1}\rangle \otimes \ldots \otimes |\psi_{x_N}\rangle$. A code (W, M) is a set of K classical codewords $\{w^{(i)}\}$ of length N and an observable M with $K + 1$ outcomes $\{0, 1, \ldots, K\}$, where outcome 0 corresponds to avoidance of decision-making. The code rate R is defined as

$$R = \frac{\log K}{N}.$$

The mutual information between the input and output when using codewords of length N is set by

$$I_N(\{\hat{p}_i\}, M) = \sum_i \hat{p}_i \sum_k p_N(k|i) \times [\log p_N(k|i) - \log \sum_{i'} p_N(k|i')\hat{p}_{i'}], \quad (1)$$

where $p_N(k|i) = \mathrm{Tr} S_{w^{(i)}} M_k$ is the probability of receiving the kth outcome when sending the ith codeword, and $\hat{p}_i$ is the probability of sending the ith codeword. We can determine the capacity when use is made of codewords of length N as a maximum of mutual information upon employment of the best code and measurement:

$$C_N = \max_{\{\hat{p}_i\}, M} I_N(\{\hat{p}_i\}, M). \quad (2)$$

If, for the classical case, $C_N = NC_1$ is always fulfilled, then for the quantum case, the phenomenon of superadditivity is possible: $C_N > NC_1$. This phenomenon consists in the fact that the capacity of c-q channels can increase when using collective measurements over the entire sequence, which is not achievable in the classical case. An important role is played by the quantity C_1, that is, the maximum mutual information achievable in individual measurements and called one-shot capacity.

A simple example of a situation where the above c-q channel demonstrates superadditivity is presented in [11]: a specific code was constructed with $K = 4$ codewords of length $N = 3$, for which $I_3 > 3C_1$, that is, mutual information in the collective measurement of such codewords exceeds by more than three times the one-shot capacity.

The quantity $C = \lim_{N\to\infty} N^{-1} C_N$ is called the capacity of a classical quantum communication channel. The quantum coding theorem [4, 5] states that this quantity is equal to the maximum of the Holevo value (or χ value), which in the general case of an ensemble $(\{\rho_i\}, \{p_i\})$, where each state ρ_i has a probability p_i, takes the form

$$\chi(\{\rho_i\}, \{p_i\}) = S\Big(\sum_i p_i \rho_i\Big) - \sum_i p_i S(\rho_i). \quad (3)$$

Here $S(\rho)$ is the von Neumann entropy of a quantum state.

For two pure equiprobable states $\{|\psi_0\rangle, |\psi_1\rangle\}$, the Holevo value is written as

$$\chi\Big(\{|\psi_0\rangle, |\psi_1\rangle\}, \Big\{\frac{1}{2}, \frac{1}{2}\Big\}\Big) = S\Big(\frac{1}{2}(|\psi_0\rangle\langle\psi_0| + |\psi_1\rangle\langle\psi_1|)\Big) = h_2\Big(\frac{1-\kappa}{2}\Big), \quad (4)$$

where $h_2(x) = -(1-x)\log(1-x) - x\log x$ is the Shannon binary entropy.

For superadditivity, both collective measurements and codewords are important, which do not fall into the use of codes with a shorter codeword length [12]. The task of constructing ‘good’ codes in the classical coding theory is very nontrivial, an so it makes sense to separately consider the phenomenon of increasing mutual information when using the collective observable. We will do this by the example of a simple code, that is, a repetition code. This code contains two codewords

$$W = \{|w_0\rangle, |w_1\rangle\} = \{|\psi_0\rangle^{\otimes N}, |\psi_1\rangle^{\otimes N}\}; \quad (5)$$

for these words, $\langle w_0 | w_1 \rangle = \kappa^N$. The states $|w_0\rangle$ and $|w_1\rangle$ are still nonorthogonal quantum states, and it is easy to find the observable of optimal distinction between them.

We will use the observable obtained from the square root of the Gram operator [13]. The Gram operator of an ensemble of equiprobable states $\{|w_0\rangle, |w_1\rangle\}$

$$G = \frac{1}{2}(|w_0\rangle\langle w_0| + |w_1\rangle\langle w_1|),$$

and its normalised eigenvectors have the form

$$|\lambda_0\rangle = \frac{1}{\sqrt{2}\sqrt{1+\kappa^N}}(|\psi_0\rangle^{\otimes N} + |\psi_1\rangle^{\otimes N}),$$

$$|\lambda_1\rangle = \frac{1}{\sqrt{2}\sqrt{1-\kappa^N}}(|\psi_0\rangle^{\otimes N} - |\psi_1\rangle^{\otimes N}),$$

with corresponding eigenvalues $\frac{1}{2}(1 \pm \kappa^N)$. Therefore,

$$G^{-1/2} = \frac{1}{\sqrt{2}\sqrt{1+\kappa^N}} |\lambda_0\rangle\langle\lambda_0| + \frac{1}{\sqrt{2}\sqrt{1-\kappa^N}} |\lambda_1\rangle\langle\lambda_1|,$$

and the measuring basis is given by vectors

$$\begin{aligned}|e_0\rangle &= \frac{1}{\sqrt{2}}G^{-1/2}|w_0\rangle = \frac{1}{\sqrt{2}}\big(|\lambda_0\rangle + |\lambda_1\rangle\big),\\ |e_1\rangle &= \frac{1}{\sqrt{2}}G^{-1/2}|w_1\rangle = \frac{1}{\sqrt{2}}\big(|\lambda_0\rangle - |\lambda_1\rangle\big),\end{aligned} \qquad (6)$$

where the factor $1/\sqrt{2}$ is the square root of the state probability.

It is easy to see that with such coding, the error probability is

$$\begin{aligned}Q &= |\langle\psi_0|^{\otimes N}|e_1\rangle|^2 = \frac{1}{2}\left(\sqrt{\frac{1+\kappa^N}{2}} - \sqrt{\frac{1-\kappa^N}{2}}\right)^2\\ &= \frac{1}{2}\big(1 - \sqrt{1-\kappa^{2N}}\big). \qquad (7)\end{aligned}$$

For mutual information in collective measurements, we have

$$\begin{aligned}I_{N,\mathrm{col}}(A,B) &= 1 - h_2(Q)\\ &= 1 - h_2\Big(\frac{1}{2}(1-\sqrt{1-\kappa^{2N}})\Big). \qquad (8)\end{aligned}$$

Using similar actions, we can calculate the probability of error q with an individual decoding of the states $\{|\psi_0\rangle,|\psi_1\rangle\}$ in each position:

$$q = \frac{1}{2}\big(1 - \sqrt{1-\kappa^2}\big);$$

the calculation of mutual information, taking into account the uneven probability distribution of the output signals, is less trivial, that is, for $N = 2$, mutual information is expressed as

$$\begin{aligned}I_{2,\mathrm{ind}}(A,B) &= H(Y) - H(Y|X) = 1 + h_2(2q(1-q))\\ &- 2h_2(q) = 1 + h_2\left(\frac{\kappa^2}{2}\right) - 2h_2\left(\frac{1-\sqrt{1-\kappa^2}}{2}\right). \qquad (9)\end{aligned}$$

One can easily see from (8) and (9) that $I_{2,\mathrm{col}}(A, B) > I_{2,\mathrm{ind}}(A, B)$, that is, when use is made of the same codewords, collective measurements give a gain in mutual information, while a repetition code in this case does not make it possible to achieve general superadditivity [$I_{2,\mathrm{col}}(A, B) > 2C_1$]; more complex codes are needed [11, 12]. In the following sections, we will consider the use of repetition code for the transmission of information to several users and for distributing a secret key and will show that its use may be more justified.

Of interest is the entanglement measure of the measurement vectors (6), since the presence of the vectors that do not fall into individual measurements makes it possible to obtain more information during the measurement. In a many-particle system, the definition of the entanglement measure is ambiguous [14]; therefore, we consider the case $N = 2$. The entanglement measure is the same for both states $|e_0\rangle$ and $|e_1\rangle$, and therefore we consider one of them:

$$\begin{aligned}|e_0\rangle = \frac{1}{2}\bigg[&\left(\frac{1}{\sqrt{1+\kappa^2}} + \frac{1}{\sqrt{1-\kappa^2}}\right)|\psi_0\rangle|\psi_0\rangle\\ &+\left(\frac{1}{\sqrt{1+\kappa^2}} - \frac{1}{\sqrt{1-\kappa^2}}\right)|\psi_1\rangle|\psi_1\rangle\bigg];\end{aligned}$$

the partial state of the first subsystem has the form

$$A = \mathrm{Tr}_2\,|e_0\rangle\langle e_0| = \frac{1}{2}\begin{pmatrix} 1 + \dfrac{1}{\sqrt{1+\kappa^2}} & \dfrac{\kappa}{\sqrt{1+\kappa^2}}\\ \dfrac{\kappa}{\sqrt{1+\kappa^2}} & 1 - \dfrac{1}{\sqrt{1+\kappa^2}}\end{pmatrix}.$$

The entanglement measure of this state is determined by the von Neumann entropy of the state of the subsystem and is equal to

$$h_2\left[\frac{1}{2}\left(1 - \frac{\sqrt{1+2\kappa^2}}{1+\kappa^2}\right)\right]. \qquad (10)$$

This measure is the greater, the greater the κ, that is, the less distinguishable the states $\{|\psi_0\rangle,|\psi_1\rangle\}$. From the point of view of expressions for mutual information (8) and (9), the entanglement measure can have the following meaning: the terms $h_2(Q)$ and $2h_2(q)$ in expressions for collective and individual mutual information mean a measure of entanglement of the system and the environment after taking the measurement, and this measure turns out to be smaller in the case of collective measurements. The calculations show that the entanglement measure of vector measurement is a monotonic function of the difference $2h_2(q) - h_2(Q)$, and vice versa: the indicated difference is a monotonic function of entanglement. This speaks in favour of the fact that the entanglement of the operators of the observable helps reduce the error, that is, the entanglement of the state and the environment after the measurement. This phenomenon is of interest for further studies.

3. Cloning problem and distribution of information between multiple receivers

The repetition code is also notable for the fact that when it is used, the sender operates with two quantum states $|\psi_0\rangle^{\otimes N}$ and $|\psi_1\rangle^{\otimes N}$ (hereinafter it is assumed that $N \geqslant 2$), and they can be considered to be an action of transformation

$$\begin{aligned}&|\Phi_0\rangle \to |\psi_0\rangle^{\otimes N},\\ &|\Phi_1\rangle \to |\psi_1\rangle^{\otimes N}\end{aligned} \qquad (11)$$

to the original vectors $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ in a two-dimensional space, where $\langle\Phi_0|\Phi_1\rangle = \alpha$. Operation (11) is an operation of approximate cloning of states $\{|\Phi_0\rangle,|\Phi_1\rangle\}$. As is known, nonorthogonal quantum states cannot be cloned [1], but approximate cloning is possible [2]. In this case, an important limitation is the unitarity condition for operation (11), which implies the relation between the scalar products, $\alpha = \kappa^N$.

We can describe at the application of the repetition code as follows: the sender has the states $\{|\Phi_0\rangle,|\Phi_1\rangle\}$, but decides to send them not in the original form. By performing approximate cloning of the states, which divides them into several parts, he sends these parts one by one. The collective measurement by the receiver can be interpreted as the fulfilment of the inverse transformation, in which the receiver collects the partial states together. At the same time, in individual measurements, the receiver has many ‘extra’ outcomes that reduce his information.

This approach allows us to consider the task of sending states $\{|\Phi_0\rangle, |\Phi_1\rangle\}$ to several receivers; in this case, each receiver can perform his own measurement, including collective one, but the receivers act independently of each other, and the reverse operation of ‘assembling’ the states $\{|\Phi_0\rangle, |\Phi_1\rangle\}$ is not available to them. It is easy to determine the Holevo value of the states of each receiver in such a situation:

$$\chi_{\text{part}} = \chi(\{|\psi_0\rangle, |\psi_1\rangle\}) = h_2\left(\frac{1-\kappa}{2}\right)$$
$$= h_2\left(\frac{1-\sqrt[N]{\alpha}}{2}\right). \quad (12)$$

It can be seen that for a fixed α, with increasing number N of receivers the maximum information of each of them tends to zero, while the general transmitted information specified by the sum of the pieces of information of the receivers is, for $\alpha \in (0, 1)$ and sufficiently large N, a superadditive quantity:

$$N\chi_{\text{part}} > \chi(\{|\psi_0\rangle, |\psi_1\rangle\}). \quad (13)$$

Receivers, however, cannot unite after the measurement and take joint actions (for example, processing the results of their measurements) to obtain information that exceeds the initial value of the Holevo states $\{|\Phi_0\rangle, |\Phi_1\rangle\}$, because their measurement results will be duplicated.

The operation of approximate cloning of states for sending to multiple users is also of interest from the point of view of cryptography. In fact, we can set a task of creating a secret key between the sender and several receivers, when the sender simultaneously sends nonorthogonal states to several receivers, and the result is that each participant receives his key. In this case, a similarity of the B92 protocol [6] arises between the sender and each of the receivers, in which each receiver measures the state using an error-free measurement defined by the observable:

$$M_0 = \frac{I - |\psi_1\rangle\langle\psi_1|}{1+\kappa}, \; M_1 = \frac{I - |\psi_0\rangle\langle\psi_0|}{1+\kappa},$$
$$M_? = I - M_0 - M_1. \quad (14)$$

Such a measurement either gives complete information about the state with probability $p_{\text{conc}} = 1 - \kappa$ (the outcome 0 or 1 is called conclusive), or with probability $p_? = \kappa$ (an inconclusive outcome), which indicates that it was not possible to extract the information.

Further actions of the participants are as follows: each receiver informs the sender of the position in which he received a conclusive result. If in this position only one receiver was able to receive information, he uses this value as a bit of a ‘raw’ key; in the case of conclusive results for several receivers, the sender randomly decides which of the receivers uses this bit value, and the rest do not use it and delete it out from their memory. This scheme of actions requires trust between the receivers that they all behave according to the protocol and, in particular, really ‘forget’ the values of the common bits.

With full trust between the participants and in the absence of errors and attenuation in the channel, all users receive independent keys. The length of the secret key of each participant is determined by the probability of obtaining complete information and the probability of collision with other participants when they also received conclusive results. The probability of receiving a key in this position by one of the participants in the case of complete trust is equal to the probability that at least one of the participants will receive a conclusive outcome:

$$l_{\text{key,all}} = 1 - p_?^N = 1 - \kappa^N = 1 - \alpha. \quad (15)$$

This probability is equal to the probability of obtaining a conclusive result when sending the states $\{|\Phi_0\rangle, |\Phi_1\rangle\}$ to one sender. It follows that with full trust and an ideal channel, the sum of the lengths of the secret keys of the participants is exactly equal to the length of the key of one participant, as if he had received all the states.

At the same time, if one of the recipients suspects that part of the other receivers does not follow the protocol, then in the absence of an error, he should assume that the eavesdropper has partial information about the key, specified by the Holevo value of states of unscrupulous participants (it is more profitable for them to unite together and use common measurements over their subsystems). Then the total length of the key transmitted to all trusted users in the presence of F untrusted users and with an ideal channel satisfies the inequality

$$l_{\text{key,trusted}} \geqslant (1 - p_?^{N-F})p_?^F\{1 - h_2[\tfrac{1}{2}(1-\kappa^F)]\}. \quad (16)$$

This probability includes the probability of obtaining a conclusive outcome for at least one of the $N-F$ trusted users, the absence of a conclusive outcome for F untrusted users, and the exclusion of information that untrusted users could receive with the best measurement. Expression (16) gives a conservative estimate: If part of the users decided to perform the optimal collective measurement to obtain the Holevo value equal to $1 - h_2[\frac{1}{2}(1-\kappa^F)]$, then they already cannot perform an error-free measurement of their states and either cannot signal the sender about a conclusive outcome in the expected number of positions, or they will reveal themselves by the erroneous value of these bits at the stage of disclosing part of the sequence. Note that in the presence of an error between some users, estimate (16) is no longer correct, since introducing an error gives unscrupulous participants new opportunities: In particular, they can perform measurements with error-free state discrimination and, conversely, signal a conclusive result, when the result was inconclusive to exclude such positions from the key. Also, the probability of attenuation in the channel and how it can be used by the interceptor [15] were not taken into account, since there is no attenuation for an ideal channel. A detailed analysis of such a system, taking into account the possibility of introducing errors and blocking some of the states, may be the topic of future research; in this paper, of essence is the general principle which states: when use is made of such a scheme, a large number of trusted users can increase the length of the key received by each of them.

Note also that in the scheme in question, the sender does not know which of the receivers acts unscrupulously, and is not able to not send states to these participants. At the same time, for each receiver, the set of untrusted participants can be different, including generally speaking their number, and the key length of each user depends only on the number of such participants.

We should also mention similar problems associated with the cryptographic protocols of several participants: distribution of a shared secret key between a group of remote users [16, 17], as well as sharing a secret message between several participants, in which they can read the message together, but any subset of them will have no access to a secret [18].

4. Problem of broadcasting quantum states and using entangled states in a channel

If the goal is to distribute the maximum public information among unrelated users in the presence of the initial states $\{|\Phi_0\rangle, |\Phi_1\rangle\}$ at the sender's disposal, then we can see that the approximate cloning transformation (11) is not optimal. Consider a broadcasting operation in which the output states can be entangled:

$$|\Phi_0\rangle \to \sqrt{1-p}|\varphi_0\rangle^{\otimes N} + \sqrt{p}|\varphi_0^{\perp}\rangle^{\otimes N},$$
$$|\Phi_1\rangle \to \sqrt{1-p}|\varphi_1\rangle^{\otimes N} + \sqrt{p}|\varphi_1^{\perp}\rangle^{\otimes N}, \quad (17)$$

where $0 \leqslant p < 1$, and from considerations of unitarity it follows

$$\alpha = (1-p)\langle\varphi_0|\varphi_1\rangle^N + p\langle\varphi_0^{\perp}|\varphi_1^{\perp}\rangle^N$$
$$+ \sqrt{p}\sqrt{1-p}(\langle\varphi_0|\varphi_1^{\perp}\rangle^N + \langle\varphi_0^{\perp}|\varphi_1\rangle^N), \quad (18)$$

which gives other scalar relations for vectors $|\varphi_i\rangle$ with respect to the vectors $|\psi_i\rangle$ corresponding to the approximate cloning operation (11).

The quantum broadcasting problem generalizes the cloning problem, since the latter does not allow the entanglement of output states. For two noncommuting density matrices, broadcasting is also prohibited [3], that is, the obtained partial states

$$\rho_0 = (1-p)|\varphi_0\rangle\langle\varphi_0| + p\,|\varphi_0^{\perp}\rangle\langle\varphi_0^{\perp}|,$$
$$\rho_1 = (1-p)|\varphi_1\rangle\langle\varphi_1| + p\,|\varphi_1^{\perp}\rangle\langle\varphi_1^{\perp}| \quad (19)$$

of each participant will necessarily differ from the initial states $\{|\Phi_0\rangle\langle\Phi_0|, |\Phi_1\rangle\langle\Phi_1|\}$.

For partial states (19), it is important that their Holevo value no longer tends to zero with an increase in the number of receivers. In fact, there is an individual measurement of states $\{|\Phi_0\rangle, |\Phi_1\rangle\}$, which distinguishes them with the probability of error

$$Q = \frac{1}{2}(1 - \sqrt{1-\alpha^2}),$$

coinciding with (7). After such a measurement by copying the classical mutually orthogonal states $\{|e_0\rangle, |e_1\rangle\}$, corresponding to the measurement results 0 and 1, we can obtain the states

$$|\Phi_0\rangle \to \sqrt{1-Q}|e_0\rangle^{\otimes N} + \sqrt{Q}|e_1\rangle^{\otimes N},$$
$$|\Phi_1\rangle \to \sqrt{1-Q}|e_1\rangle^{\otimes N} + \sqrt{Q}|e_0\rangle^{\otimes N} \quad (20)$$

for arbitrary N.

Thus, the Holevo value of each participant after transformation (17) can be made no less than the amount of mutual information in an individual measurement of the states $\{|\Phi_0\rangle, |\Phi_1\rangle\}$:

$$\chi(\{\rho_0, \rho_1\}) \geqslant 1 - h_2(Q).$$

It makes sense to consider the problem of maximising information $\chi(\{\rho_0, \rho_1\})$, which can be distributed between the sender and each of the independent receivers, under conditions of unitarity of (18). The prohibition of full broadcasting indicates that for $\alpha \in (0, 1)$ it is less than the initial χ value:

$$\chi(\{\rho_0, \rho_1\}) < \chi(\{|\Phi_0\rangle, |\Phi_1\rangle\}).$$

This phenomenon can be called prohibition of information broadcasting: it is impossible to use the available quantum states to transmit information to an arbitrary number of users without losing information. This prohibition can be considered as a dual phenomenon to the superadditivity of the classical capacity of the c-q channel. If superadditivity is associated with the ability to make collective measurements over the entire transmitted sequence, the prohibition of information broadcasting is associated with the inability of several users to perform a joint collective measurement, while each of them performs collective measurements over his sequence of states obtained in several communication sessions, which allows the χ value of partial states to be employed to evaluate the participant information.

With approximate broadcasting, the problem of distributing public information is well solved; however, such a transformation, as is easy to see, is poorly suited for distributing keys, because receivers due to their entanglement will receive a matching key, and the distribution of independent keys is extremely inefficient. This can be interpreted as follows: the low quantumness of ensembles of states that each participant receives makes the distribution of keys poorly implemented.

Consider also the situation where the sender performed transformation (17), but after that sent all the states to one receiver. Then, due to the unitarity relation (18), the mutual information between the sender and the receiver during collective measurements of the latter over all N states is unchanged and is equal to the one-shot capacity for the states $\{|\Phi_0\rangle, |\Phi_1\rangle\}$:

$$I_{\text{col}}(A, B) = C_1(\{|\Phi_0\rangle, |\Phi_1\rangle\}) = 1 - h_2(Q)$$
$$= 1 - h_2\left(\frac{1 - \sqrt{1-\alpha^2}}{2}\right),$$

which coincides with (8). In individual measurements, the mutual information is higher than cloning allows [see (9)], and is defined as

$$I_{\text{ind}}(A, B) = C_1(\{\rho_0, \rho_1\}).$$

If we set the maximisation problem $I_{\text{ind}}(A, B)$, then it is easy to see that the maximum is achieved by measuring the states $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ and preparing several copies (20) and does not differ from the capacity $I_{\text{ind}}(A, B)$ in the collective measurement of the receiver over N messages. Thus, there is no gain in using collective measurements in this case.

As a result, the entanglement between the states of different participants acts both constructively (for the task of information broadcasting and maximisation of the receiver information in individual measurements) and destructively (for the task of distributing independent keys among several users).

5. Entanglement dilution at the transmitter's side

The two previous sections considered the sender's actions, in which he initially has a set of nonorthogonal states $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ and performs actions with them, resulting in states in a new space, generally speaking, of a different dimension. This situation can be generalised to the case when the sender has an entangled state of the system AB

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}\big(|0\rangle_A|\Phi_0\rangle_B + |1\rangle_A|\Phi_1\rangle_B\big) \tag{21}$$

and performs actions over this state. To obtain the states $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ in the subsystem B, it suffices to measure the subsystem A in the basis $\{|0\rangle,|1\rangle\}$, but this is not the only possible action.

For state (21), we can write the Schmidt decomposition

$$|\Psi\rangle_{AB} = \sqrt{\frac{1+\alpha}{2}}\,|\bar{0}\rangle_A|\bar{0}\rangle_B + \sqrt{\frac{1-\alpha}{2}}\,|\bar{1}\rangle_A|\bar{1}\rangle_B, \tag{22}$$

where, as before, $\alpha = \{|\Phi_0\rangle,|\Phi_1\rangle\}$, and the Schmidt basis is given by vectors

$$|\bar{0}\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A + |1\rangle_A), \qquad |\bar{1}\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle_A - |1\rangle_A),$$

$$|\bar{0}\rangle_B = \frac{1}{\sqrt{2(1+\alpha)}}(|\Phi_0\rangle_B + |\Phi_1\rangle_B), \quad |\bar{1}\rangle_B = \frac{1}{\sqrt{2(1-\alpha)}}(|\Phi_0\rangle_B - |\Phi_1\rangle_B).$$

A measure of entanglement of the two-particle state (21) is the entropy of the squares of Schmidt coefficients

$$E(|\Psi\rangle_{AB}) = H\Big(\Big\{\frac{1+\alpha}{2},\frac{1-\alpha}{2}\Big\}\Big) = h_2\Big(\frac{1-\alpha}{2}\Big) = \mu_\alpha. \tag{23}$$

Important operations in quantum information are concentration (the terms distillation and purification are also used) and entanglement dilution [14, 19]. Concentration of entanglement allows a smaller number of fully entangled states to be obtained from a large number of partially entangled states, while entanglement dilution is the inverse operation, which allows a larger number of partially entangled states to be obtained from a small number of fully entangled states.

The entanglement measure of state (21) is equal to μ_α, and this means that one can obtain from it N states $|\Psi'\rangle_{AB}$, with the entanglement measure of each being equal to μ_α/N:

$$|\Psi\rangle_{AB} \to |\Psi'\rangle_{AB}^{\otimes N}. \tag{24}$$

Consider the situation when the sender performs such dilution and then measures the subsystem A of each of the states $|\Psi'\rangle_{AB}$ in the basis $\{|0\rangle,|1\rangle\}$, after which N independent ensembles of states $\{|\omega_0\rangle,|\omega_1\rangle\}$, are formed in the system B for which $\langle\omega_0|\omega_1\rangle$ is determined from the equation

$$h_2\Big(\frac{1-\alpha}{2}\Big) = Nh_2\Big(\frac{1-\langle\omega_0|\omega_1\rangle}{2}\Big).$$

Note again that the scalar relations between $|\omega_i\rangle$ differ from the relations between $|\psi_i\rangle$ and $|\varphi_i\rangle$ introduced for approximate cloning and broadcasting operations, respectively. Also note that states $|\omega_i\rangle$ are different from codewords $|w_i\rangle$ (5) considered in Section 2.

From the point of view of distributing public information, this approach is worse than those described above, since the total Holevo value of the ensembles $\{|\omega_0\rangle,|\omega_1\rangle\}$ is equal to the value of the Holevo values of the states $\{|\Phi_0\rangle,|\Phi_1\rangle\}$ and it turns out to be less than the same sum for other cases.

At the same time, this situation is well suited for distributing keys among several recipients in the absence of trust between them, since they receive independent keys about which other participants do not have information, regardless of their good faith. If there is no error, the length of the secret key of each participant is expressed as

$$l_{\text{key, part}} = 1 - \langle\omega_0|\omega_1\rangle. \tag{25}$$

The sum of keys of participants will be slightly lower than the sum of keys with approximate cloning of states and the presence of a sufficient number of trusted participants, but higher than with a small number of untrusted users.

Figure 1 shows the key generation rate during the entanglement dilution and during the operation of approximate cloning in the case of a different number of trusted users. It can be seen that with a large number of receivers, the entanglement dilution ensures a key generation rate comparable to that for approximate cloning and half of trusted users.

Of interest is the situation when all N states are sent to one receiver. If the receiver is not able to perform collective measurements over the entire sequence that would give the Holevo value of the states $\{|\Phi_0\rangle,|\Phi_1\rangle\}$, , then it does not make sense for him to take collective measurements over words of length N, because, due to independence, the general ensemble quantum states breaks up into N ensembles of the states $\{|\omega_0\rangle,|\omega_1\rangle\}$ related to the subsystems, and, as noted above, the collective measurement does not give a gain in comparison with the individual measurement of each state [12]. Note that with increasing N, the difference between the information available in collective and individual measurements increases, while measurements over all N states do not give a gain compared to individual measurements. For future studies, it is of interest to study relation of this fall in information with the characteristics of the observable over the states $|\Psi'\rangle_{AB}^{\otimes N}$ after entanglement dilution, since, as was noted in [20], the coherence (which can serve as a measure of quan-

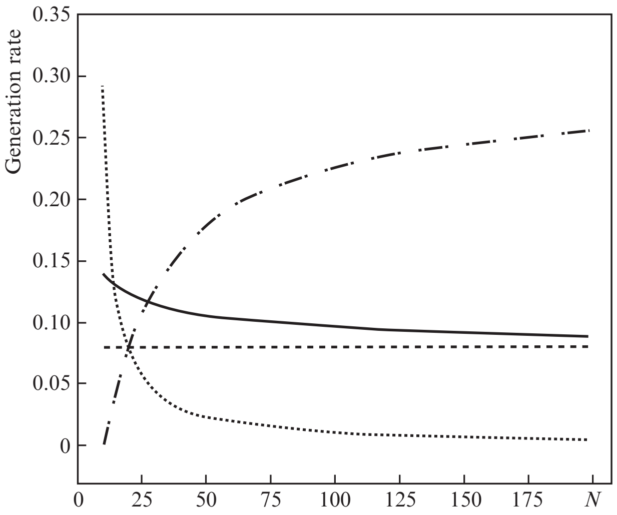

Figure 1. Secret key generation rate per message bit as a function of the number N of receivers during the approximate cloning and entanglement dilution operations. The solid curve shows the sum of the user keys for the case of entanglement dilution, when the key length of each participant is given by formula (25). Other curves correspond to the approximate cloning operation and are calculated according to (16): the dotted curve is calculated for 10 trusted users; the dashed curve, for half the trusted users; and dot-and-dash curve, for 10 untrusted users. The initial measure of entanglement of the sender's states is $h_2[0.5(1-1/\sqrt{2})]$, which corresponds to $\langle\Phi_0|\Phi_1\rangle = \cos(\pi/4)$.

tumness) of the ensemble obtained by measuring part of the entangled state depends on the degree of uncertainty used in the observable.

6. Conclusions

We have discussed the situations of public data transmission and secret key distribution with a fixed resource between remote users. As a resource we use a measure of the entanglement of the sender's state, from which one can obtain an ensemble of states or several independent ensembles. Three main directions are considered when working with the obtained ensemble: the preparation of several pure states (approximate cloning), the preparation of mixed states (broadcasting) and the entanglement dilution with the preparation of independent ensembles. For each situation, we have studied the problem of transmitting public information to one or several users and the problem of distributing the secret key.

When all states are transmitted to one participant and it is possible to perform collective measurements, the method of data transmission does not play any role, since the maximum mutual information is given by the Holevo value of the initial states $\{|\Phi_0\rangle, |\Phi_1\rangle\}$ or, equivalently, by the measure of state entanglement $|\Psi\rangle_{AB}$.. However, if it is possible to perform measurements over N states for the three situations considered, the results are different. With the approximate cloning of states, a gain arises from collective measurements, which is equivalent to a gain in applying a repetition code in a c-q channel. In the case of approximate broadcasting, the gain from measurements over N states is small, and with sufficient entanglement between the states, it turns out to be zero. When an entangled state is diluted with its subsequent measurement, the gain from measuring all N states is absent.

If we set the task of transmitting public information to several participants making independent measurements, then approximate broadcasting copes with this task best; nevertheless, finding the optimal transformation (information broadcasting) over an arbitrary initial ensemble is a nontrivial problem, which lacks a general solution. If participants are limited to individual measurements, then this problem is solved by optimally measuring the initial state and preparing classical states based on the measurement results.

When distributing independent keys between N receivers, the approximate broadcasting operation is poorly suited due to signal duplication caused by state entanglement. It is logical to make use of entanglement dilution as the main transformation, which will allow an independent key to be generated for each participant. However, an interesting situation arises in the case of approximate cloning: the key distribution rate with each participant depends on the trust between the participants. The more the trusted users with whom the participant is confident that they are behaving according to the protocol, the higher the key distribution rate for this participant.

In our opinion, it makes sense to take these situations into account in the quantitative description of the phenomena of quantum physics and the work of quantum communication protocols. It is also worth paying attention to a number of related problems: the study of the influence of entanglement on the gain from collective measurements, finding the optimal transformation of information broadcasting to transmit the maximum of public information to several recipients with given initial quantum states and a strict estimate of the length of the secret key when it is distributed between the sender and multiple receivers, depending on the number of trusted receivers, including those with an imperfect channel and errors.

Acknowledgements. The author thanks A.N. Pechen for fruitful discussions.

The work is supported by the Russian Science Foundation under Grant No. 17-11-01388-P and performed at the Steklov Mathematical Institute of the Russian Academy of Sciences.

References

1. Wootters W.K., Zurek W.H. *Nature*, **299** (5886), 802 (1982).
2. Scarani V., Iblisdir S., Gisin N., Acin A. *Rev. Mod. Phys.*, **77** (4), 1225 (2005).
3. Barnum H., Caves C.M., Fuchs C.A., Jozsa R., Schumacher B. *Phys. Rev. Lett.*, **76** (15), 2818 (1996).
4. Holevo A.S. *IEEE Trans. Inform. Theory*, **44** (1), 269 (1998).
5. Schumacher B., Westmoreland M.D. *Phys. Rev. A*, **56** (1), 131 (1997).
6. Bennett C.H. *Phys. Rev. Lett. A*, **68**, 3121 (1992).
7. Ollivier H., Zurek W.H. *Phys. Rev. Lett.*, **88** (1), 017901 (2001).
8. Bera A., Das T., Sadhukhan D., Roy S.S., De A.S., Sen U. *Rep. Prog. Phys.*, **81** (2), 024001 (2017).
9. Holevo A.S. *Quantum Systems, Channels and Information: A Mathematical Introduction* (Berlin: De Gruyter, 2012; Moscow: MTsNMO, 2010).
10. Hastings M.B. *Nature Phys.*, **5** (4), 255 (2009).
11. Sasaki M., Kato K., Izutsu M., Hirota O. *Phys. Lett. A*, **236**, 1 (1997).
12. Sasaki M., Kato K., Izutsu M., Hirota O. *Phys. Rev. A*, **58** (1), 146 (1998).
13. Hausladen P., Jozsa R., Schumacher B., Westmoreland M., Wootters W.K. *Phys. Rev. A*, **54** (3), 1869 (1996).
14. Bennett C.H., Popescu S., Rohrlich D., Smolin J.A., Thapliyal A.V. *Phys. Rev. A*, **63** (1), 012307 (2000).

15. Kronberg D.A., Kurochkin Yu.V. *Quantum Electron.*, **48** (9), 843 (2018) [*Kvantovaya Elektron.*, **48** (9), 843 (2018)].
16. Bose S., Vedral V., Knight P.L. *Phys. Rev. A*, **57** (2), 822 (1998).
17. Chen K., Lo H.K. arXiv preprint quant-ph/0404133 (2004).
18. Hillery M., Bužek V., Berthiaume A. *Phys. Rev. A*, **59** (3), 1829 (1999).
19. Bennett C.H., Bernstein H.J., Popescu S., Schumacher B. *Phys. Rev. A*, **53** (4), 2046 (1996).
20. Kronberg D.A. *Lobachevskii J. Mathematics*, **40** (10), 1507 (2019).