# Private Quantum Coding for Quantum Relay Networks

Laszlo Gyongyosi, Sándor Imre



# Private Quantum Coding for Quantum Relay Networks

Laszlo Gyongyosi[1], Sandor Imre[1]

[1]Quantum Technologies Laboratory, Department of Telecommunications
Budapest University of Technology and Economics
Budapest, Hungary
gyongyosi@hit.bme.hu

**Abstract.** The relay encoder is an unreliable probabilistic device which is aimed at helping the communication between the sender and the receiver. In this work we show that in the quantum setting the probabilistic behavior can be completely eliminated. We also show how to combine quantum polar encoding with superactivation-assistance in order to achieve private communication over noisy quantum relay channels.

**Keywords:** Quantum communications, private quantum channel, quantum polar encoding.

## 1 Introduction

The relay encoding scheme for classical communication channels was introduced by Cover and Gamal [1]. The relay encoding with classical polar coding was studied by Andersson et al. [2], using their nested polar relay channel codes. Here we show that relay encoding can also be used in the quantum setting to achieve enhanced private communication [11] between the sender and receiver. Our two main goals can be summarized as follows: First, by constructing capacity-achieving quantum polar codes we would like to maximize the transmittable private classical information over the quantum relay channel. Second, we would like to prove that using superactivation-assistance [5] the reliability of the quantum relay encoder can be maximized and the probabilistic behavior can be completely eliminated.

This paper is organized as follows: In Section 2 we discuss the proposed encoding scheme. In Section 3 we show the quantum relay encoder. In Section 4 we present the theorems and proofs. Finally, in Section 5, we conclude our results.

## 2 Our Private Encoding Scheme

The channel polarization scheme introduced by Arikan [3] makes it possible to achieve the symmetric capacity of a noisy communication channel. The symmetric capacity is the highest rate at which the channel can be used for communication if the

probability of the input letters is equal [3-5]. The polar coding technique was extended to secure communication over classical channels by Mahdavifar and Vardy [4]. The quantum polar coding scheme was studied by Wilde and Guha [6] and by Renes et al. [7]. Later, the results of [7] were extended by Wilde and Renes [13], [21] for arbitrary quantum channels. Gyongyosi and Imre have given a solution for the polaractivation of private classical capacity of noisy quantum channels [12,16]. The *superactivation* is an extreme violation of the additivity of quantum channel capacities and enables the use of zero-capacity quantum channels for communication [5],[14], [17-19]. In this work we show, that this effect can also be exploited. The relay encoder is placed between the Alice and Bob and intended to help Bob receiving messages from Alice [1].

The channel which contains an $\mathcal{E}_2$ relay encoder between Alice and Bob is called the *relay channel* [1]. In case of a degraded relay channel, the relay receiver $\mathcal{E}_2$ works better than Bob's receiver $\mathcal{D}$ and the relay encoder can cooperate with original encoder $\mathcal{E}_1$ to help to decode the message on Bob's side [1], [2]. In our scheme we use polar encoding to achieve the private classical capacity.

For a quantum channel $\mathcal{N}$ the *symmetric* classical capacity is equal to the quantum mutual information $I(A:B)$ [10], [15], [20],

$$C_{sym}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max I(A:B)^{\otimes n}, \tag{1}$$

where $\otimes n$ denotes the $n$ channel uses, and the probability distribution of the input states is assumed to be *uniform* [3], [6]. The symmetric *private* classical capacity [11], [15] can be expressed as follows:

$$P_{sym}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max \left( I(A:B) - I(A:E) \right)^{\otimes n}, \tag{2}$$

where $I(A:E)$ is the quantum mutual information function assuming a symmetric channel between Alice and Eve.

In Fig. 1, we depict our encoding scheme [12]. Alice encodes her private message $M$ into the phase using the $X$ basis and then into the amplitude using the $Z$ basis [12]. The phase carries the *data*, while the amplitude is the *key* for the encryption i.e., in our scheme Alice first encodes the phase (data) and then the amplitude (key). Bob applies it in the reverse direction using his successive and coherent decoder, and finally gets $M'$ as follows [7], [8]: he first decodes the *amplitude* (key) information in the $Z$ basis [10]. Then Bob continues the decoding with the *phase* information, in the $X$ basis [10]. According to our encoding scheme, the *symmetric private classical capacity* $P_{sym}$ is defined as

$$\begin{aligned} P_{sym}(\mathcal{N}_1) &= \lim_{n\to\infty} \frac{1}{n} \max \left( I_{sym.}^{phase}(A:B) - I(A:E) \right)^{\otimes n} \\ &= \lim_{n\to\infty} \frac{1}{n} \max \begin{pmatrix} \mathrm{S}\left( \left( \sigma_0^{phase} + \sigma_1^{phase} \right) / 2 \right) - \mathrm{S}\left( \sigma_0^{phase} / 2 \right) \\ -\mathrm{S}\left( \sigma_1^{phase} / 2 \right) - I(A:E) \end{pmatrix}^{\otimes n}, \end{aligned} \tag{3}$$

where $\mathrm{S}(\cdot)$ is the von Neumann entropy function, while $I(A:E)=\mathrm{S}(A)+\mathrm{S}(E)-H(AE)$ stands for the mutual information function between Alice and Eve, and $I_{sym.}^{phase}(A:B)$ is the symmetric mutual information that can be achieved by the phase information between Alice and Bob [3], [12], [15].

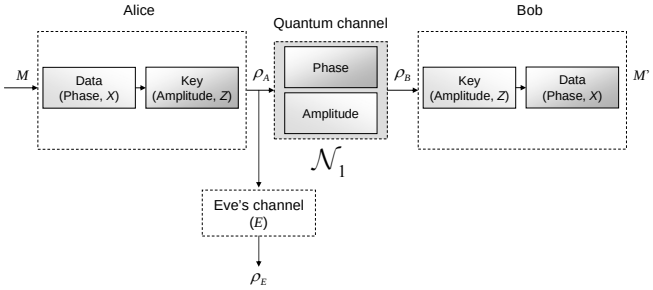


**Fig. 1**. Private communication of Alice and Bob over a quantum channel in presence of an eavesdropper Eve. The quantum channel has positive private classical capacity if it can send both phase and amplitude.

To construct the input polar codeword sets, we use the notation of 'good' $\mathcal{G}(\mathcal{N},\beta)$ and 'bad' $\mathcal{B}(\mathcal{N},\beta)$, where $\beta<0.5$ [3] channels for the transmission of phase and amplitude. The $S_{in}$ set of polar codewords which can transmit private information (both amplitude and phase) is denoted by:

$$S_{in}=\mathcal{G}\left(\mathcal{N}_{amp},\beta\right)\cap\mathcal{G}\left(\mathcal{N}_{phase},\beta\right). \tag{4}$$

All of other input codewords cannot transmit private classical information, however some of them can be used to transmit non private classical information. These codewords are defined by the set $S_{bad}$ as follows:

$$\begin{aligned} S_{bad}=&\left(\mathcal{G}\left(\mathcal{N}_{amp},\beta\right)\cap\mathcal{B}\left(\mathcal{N}_{phase},\beta\right)\right)\cup\\ &\left(\mathcal{B}\left(\mathcal{N}_{amp},\beta\right)\cap\mathcal{G}\left(\mathcal{N}_{phase},\beta\right)\right)\cup\\ &\left(\mathcal{B}\left(\mathcal{N}_{amp},\beta\right)\cap\mathcal{B}\left(\mathcal{N}_{phase},\beta\right)\right). \end{aligned} \tag{5}$$

From set $S_{bad}$, we define the completely useless codewords which cannot transmit any classical information as

$$\mathcal{B}=\mathcal{B}\left(\mathcal{N}_{amp},\beta\right)\cap\mathcal{B}\left(\mathcal{N}_{phase},\beta\right), \tag{6}$$

while the 'partly good' (i.e., can be used for non private classical communication) input codewords will be denoted by

$$\mathcal{P}_1=\mathcal{G}\left(\mathcal{N}_{amp},\beta\right)\cap\mathcal{B}\left(\mathcal{N}_{phase},\beta\right) \tag{7}$$

and

$$\mathcal{P}_2=\mathcal{B}\left(\mathcal{N}_{amp},\beta\right)\cap\mathcal{G}\left(\mathcal{N}_{phase},\beta\right), \tag{8}$$

where $\beta<0.5$ is a fixed constant [3]. The working process of the polar-encoding based quantum relay encoder $\mathcal{E}_2$ can be summarized as follows: The first encoder $\mathcal{E}_1$

encodes the *phase* information into the codeword *A* and then sends it to $\mathcal{E}_2$, using set $\mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)$. In the next step, the quantum relay encoder $\mathcal{E}_2$ with probability $p_{\mathcal{E}_2}$ adds the *amplitude* information to the phase information, using polar codes from the set $\mathcal{G}\left(\mathcal{N}_{phase}, \beta\right) \setminus \mathcal{P}_2$, and then sends it to Bob. Otherwise, with probability $\left(1 - p_{\mathcal{E}_2}\right)$ it leaves unchanged $\mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)$ and transmits to Bob. The problem with the quantum relay encoder $\mathcal{E}_2$ is that it is unreliable since it works in a probabilistic way, which also makes the channel $\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$ too noisy.

## 3 Our Quantum Relay Encoder

Our proposed quantum relay encoder $\mathcal{E}_2$ is depicted in Fig. 2. Alice would like to send her *l*-length private message *M* to Bob. The first encoder $\mathcal{E}_1$ can encode only phase information, while the quantum relay encoder $\mathcal{E}_2$ can encode only amplitude information. The quantum relay encoder $\mathcal{E}_2$ can add the amplitude information to the message *A* received from $\mathcal{E}_1$ only with success probability $0 < p_{\mathcal{E}_2} < 1$. In the first step, her encoder $\mathcal{E}_1$ outputs the *n*-length *phase* encoded message *A*. The second encoder $\mathcal{E}_2$ gets input on the channel output $B'$, which will be amended with *amplitude* information. The relay quantum encoder $\mathcal{E}_2$ outputs $A'$ to the channel, and Bob will receive message *B*. The goal of the whole structure is to help Bob's encoder $\mathcal{D}$, by the quantum relay encoder $\mathcal{E}_2$ to cooperate with $\mathcal{E}_1$, to send the private message *M* from Alice to Bob. The quantum relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$, which includes Alice's first encoder $\mathcal{E}_1$ and the relay encoder $\mathcal{E}_2$ is defined as $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}} = \mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$, where $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}$ is the quantum channel between encoder $\mathcal{E}_1$ and the quantum relay encoder $\mathcal{E}_2$, while $\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$ is the quantum channel between the quantum relay encoder $\mathcal{E}_2$ and Bob's decoder $\mathcal{D}$.

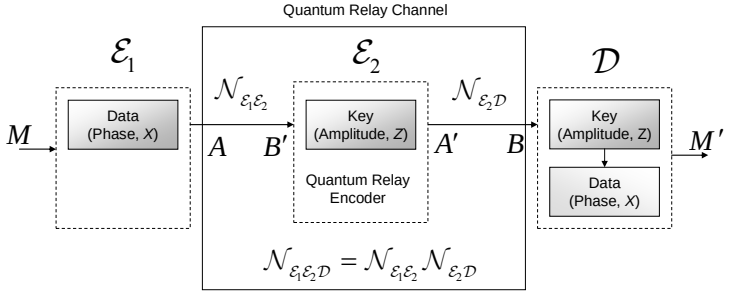


**Fig. 2.** The quantum relay channel with the relay encoder. The first encoder encodes only phase information, the second adds only the amplitude information. The quantum relay encoder is not reliable, it works with success probability $0 < p_{\mathcal{E}_2} < 1$.

For a degradable quantum relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$, the channel $\mathcal{N}_{\mathcal{E}_1\mathcal{D}}$ is noisier than $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}} = \mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$. The $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ quantum relay channel is noisy due to the unreliable quantum relay encoder $\mathcal{E}_2$. Using our quantum polar codeword sets from (4), (6), (7) and (8) the *security* of the scheme is guaranteed, since the transmitted codewords on channels $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}$ and $\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$ are:

$$\begin{aligned} &\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2} : \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right) = \mathcal{P}_2 \cup S_{in}, \\ &\mathcal{N}_{\mathcal{E}_2\mathcal{D}} : \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right) = S_{in}. \end{aligned} \tag{9}$$

which means, that the outputs of $\mathcal{E}_1$ and $\mathcal{E}_2$ are those polar codewords which will be completely useless for Eve. From the polar scheme $\left|\mathcal{P}_2\right| = 0$ [7], [13], while the polar set $S_{in}$ is also useless for Eve, which trivially follows from (6). Assuming a degraded quantum relay encoder $\mathcal{E}_2$, the following probabilities hold for the relay quantum channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$:

$$p\left(B, B' \middle| A, A'\right) = p\left(B' \middle| A, A'\right) p\left(B \middle| B', A'\right), \tag{10}$$

where $A \to \left(A'B'\right) \to B$ is a Markov chain and $p\left(B \middle| B', A, A'\right) = p\left(B \middle| B', A'\right)$. The symmetric classical capacity of quantum relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$, assuming encoders $\mathcal{E}_1$ and $\mathcal{E}_2$, and decoder $\mathcal{D}$ can be expressed as

$$\begin{aligned} C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) &= \max_{p(A,A')} \min\left\{I\left(A, A' : B\right), I\left(A : B' \middle| A'\right)\right\} \\ &= I\left(A : B, B' \middle| A'\right) = I\left(A : B' \middle| A'\right), \end{aligned} \tag{11}$$

which is equivalent to the following definition. Let be the classical capacity of the channel between encoder $\mathcal{E}_1$ and quantum relay encoder $\mathcal{E}_2$ is $C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\right)$, while between $\mathcal{E}_1$ and $\mathcal{D}$ without quantum relay encoder $\mathcal{E}_2$ is $C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{D}}\right)$ and between $\mathcal{E}_2$ and $\mathcal{D}$ is $C_{sym}\left(\mathcal{N}_{\mathcal{E}_2\mathcal{D}}\right)$. Using these channels, the capacity $C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$ of $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ can be calculated as

$$C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) = \min\left\{C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\right), \left(C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{D}}\right) + C_{sym}\left(\mathcal{N}_{\mathcal{E}_2\mathcal{D}}\right)\right)\right\}. \tag{12}$$

Our quantum relay encoder differs from the classical relay encoder scheme of [1], [2]. The $\mathcal{E}_2$ quantum relay encoder outputs codeword

$$B = p_{\mathcal{E}_2}\left(\mathcal{G}\left(\mathcal{N}_{phase}, \beta\right) \setminus \mathcal{P}_2\right) + \left(1 - p_{\mathcal{E}_2}\right)\mathcal{G}\left(\mathcal{N}_{phase}, \beta\right), \tag{13}$$

with $\left|B\right| = p_{\mathcal{E}_2}\left|\left(\mathcal{G}\left(\mathcal{N}_{phase}, \beta\right) \setminus \mathcal{P}_2\right)\right|$ or $\left|B\right| = \left(1 - p_{\mathcal{E}_2}\right)\left|\mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)\right|$, where $p_{\mathcal{E}_2}$ is the success probability of the quantum relay encoder $\mathcal{E}_2$. Finally, Bob decodes the message using set $\mathcal{G}\left(\mathcal{N}_{phase}, \beta\right) \setminus \mathcal{P}_2$. If Bob received $B = \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)$ from the quantum relay encoder $\mathcal{E}_2$, then the decoding process fails—this occurs with

probability $\left(1-p_{\varepsilon_2}\right)$. As we will prove, using superactivation-assistance in the relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$, the reliability of $\mathcal{E}_2$ will be $p_{\varepsilon_2}=1$; however, the rate of private communication will be lower, which will result in the codeword

$$B^*=\mathcal{G}\left(\mathcal{N}_{phase},\beta\right)\setminus\mathcal{P}_2. \tag{14}$$

with $\left|B^*\right|=\frac{1}{2}\left|\left(\mathcal{G}\left(\mathcal{N}_{phase},\beta\right)\setminus\mathcal{P}_2\right)\right|$. For the *rate* of private communication, any benefits from the superactivation-assistance can be exploited if and only if $0<p_{\varepsilon_2}<0.5$, since in that case $\left|B^*\right|>\left|B\right|$. As follows, we will assume an unreliable quantum relay encoder with success probability $0<p_{\varepsilon_2}<0.5$. The achievable symmetric classical capacities can be summarized as follows: The symmetric classical capacity between Alice and the quantum relay encoder $\mathcal{E}_2$ is $C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\right)=\lim_{n\to\infty}\frac{1}{n}\left|\mathcal{G}\left(\mathcal{N}_{phase},\beta\right)\right|$. The symmetric classical capacity between Alice and Bob with no relay encoder $\mathcal{E}_2$ assistance is $C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{D}}\right)=\lim_{n\to\infty}\frac{1}{n}\left(\left|\mathcal{P}_2\right|\right)$. From these results follows that the symmetric private capacity $P_{sym}\left(\mathcal{N}_{\mathcal{E}_2\mathcal{D}}\right)$ can be expressed as

$$P_{sym}\left(\mathcal{N}_{\mathcal{E}_2\mathcal{D}}\right)=C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\right)-C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{D}}\right), \tag{15}$$

thus for the channel between the quantum relay encoder $\mathcal{E}_2$ and Bob, the achievable symmetric private classical capacity is

$$P_{sym}\left(\mathcal{N}_{\mathcal{E}_2\mathcal{D}}\right)=\lim_{n\to\infty}\frac{1}{n}\left(\left|\mathcal{G}\left(\mathcal{N}_{phase},\beta\right)\right|-\left|\mathcal{P}_2\right|\right), \tag{16}$$

which is equal to

$$P_{sym}\left(\mathcal{N}_{\mathcal{E}_2\mathcal{D}}\right)=\lim_{n\to\infty}\frac{1}{n}\left|\left(\mathcal{G}\left(\mathcal{N}_{phase},\beta\right)\right)\cap\left(\mathcal{G}\left(\mathcal{N}_{amp.},\beta\right)\right)\right|=\lim_{n\to\infty}\frac{1}{n}\left|S_{in}\right|. \tag{17}$$

The private capacity which can be achieved over the quantum relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ with the combination of the *superactivation-assistance* and *polar encoding* will be referred to as $P^*_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$. Using the first encoder $\mathcal{E}_1$, we will get $C_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\right)>0$, however $P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\right)=0$, since $\mathcal{E}_1$ can encode only *phase* information. The relay encoder $\mathcal{E}_2$ adds *amplitude* information to the *phase* information, thus $C_{sym}\left(\mathcal{N}_{\mathcal{E}_2\mathcal{D}}\right)>0$. Since for any input *A* received from $\mathcal{E}_1$ the channel $\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$ also has positive private capacity $P_{sym}\left(\mathcal{N}_{\mathcal{E}_2\mathcal{D}}\right)>0$, which can be achieved only with success probability $p_{\varepsilon_2}>0$.

## 4 Theorems and Proofs

In this section we present the theorems and give the proofs. Our result on the reliability of the proposed quantum relay encoder is summarized in Theorem 1.

**Theorem 1.** Using the unreliable quantum relay encoder $\mathcal{E}_2$ with $0 < p_{\mathcal{E}_2} < 0.5$, the superactivation-assisted private classical capacity $P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$ of the quantum relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ will be positive and the reliability of the quantum relay encoder equals to $p_{\mathcal{E}_2} = 1$.

*Proof*: First, Alice generates codeword *A* with $\mathcal{E}_1$. In the next step, she transmits it over $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}$ and feeds $B'$ into $\mathcal{E}_2$, which will result in $A'$. It will be transmitted over $\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$, which will result in Bob's input *B*. For positive private classical capacity $P_{sym} > 0$, both the phase and the amplitude have to be transmitted; however, the encoders $\mathcal{E}_1$ and $\mathcal{E}_2$ individually cannot encode both of them. Using channel $\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$ between $\mathcal{E}_2$ and $\mathcal{D}$, for the superactivation of we define the following channel $\mathcal{M}$

$$\mathcal{M} = p\mathcal{N}_{\mathcal{E}_2\mathcal{D}} \otimes |0\rangle\langle 0| + (1-p)\mathcal{A}_e \otimes |1\rangle\langle 1|, \tag{18}$$

where $0 \le p \le 1$ and $\mathcal{A}_e$ is the 50% erasure channel [5]. The channel $\mathcal{M}$ with probability $p$ is a $\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$ channel (i.e., an $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}} = \mathcal{N}_{\mathcal{E}_1\mathcal{E}_2}\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$ channel, since the encoder $\mathcal{E}_1$ is applied before channel $\mathcal{N}_{\mathcal{E}_2\mathcal{D}}$), otherwise, with probability $(1-p)$, it is an 50% erasure channel, which also has zero private capacity, i.e., $P(\mathcal{A}_e) = 0$. To superactivate the joint construction of $\mathcal{M}_1 \otimes \mathcal{M}_2$, Alice will feed the following entangled system to the inputs (denoted by *A* and *C*) of the joint channel [5]:

$$\rho_{AC} = \frac{1}{2}\left(|0\rangle\langle 0|_{A_1} \otimes |0\rangle\langle 0|_{C_1} + |0\rangle\langle 0|_{A_1} \otimes |0\rangle\langle 0|_{C_1}\right) \otimes |\Psi_+\rangle\langle\Psi_+|, \tag{19}$$

where $|\Psi_+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right)$ is a Bell-state. The $I_{coh}$ quantum coherent information of $\mathcal{M}_1 \otimes \mathcal{M}_2$ for the input system $\rho_{AC}$ is $I_{coh}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) = 2p(1-p)I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$ [5], from which follows that for the private classical capacity of $\mathcal{M}_1 \otimes \mathcal{M}_2$, $P_{sym}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) \ge 2p(1-p)P\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$, where $I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$ is the coherent information of channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$, and $0 < p < 1$. The lower bound on the achievable superactivated symmetric private classical capacity of $\mathcal{M}_1 \otimes \mathcal{M}_2$ is $P_{sym}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) \ge \frac{1}{2} I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$. Using $P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) = I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$, we get the following lower bound for the *P* symmetric private classical capacity of $\mathcal{M}_1 \otimes \mathcal{M}_2$:

$$P_{sym}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) \geq \frac{1}{2} P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right), \tag{20}$$

thus for our encoding scheme $P_{sym}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) = \frac{1}{2} P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$. The required condition $I_{sym.}^{amp.}\left(A:B\right) > 0$ for the positive private capacity $P\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$ of the relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ is also satisfied. Finally, the superactivation-assisted private classical capacity $P\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right)$ of $\mathcal{M}_1 \otimes \mathcal{M}_2$ is evaluated as follows:

$$\begin{aligned} &P_{sym}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) = \frac{1}{2}\left(I_{sym.}^{phase}\left(A:B\right) - I\left(A:E\right)\right) = \\ &\frac{1}{2}\begin{pmatrix} \mathrm{S}\left(\left(\sigma_0^{phase} + \sigma_1^{phase}\right)/2\right) - \mathrm{S}\left(\sigma_0^{phase}/2\right) \\ -\mathrm{S}\left(\sigma_1^{phase}/2\right) - I\left(A:E\right) \end{pmatrix}, \end{aligned} \tag{21}$$

which is the half of the private classical capacity $P\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$, that can be achieved over $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ if $p_{\mathcal{E}_2} = 1$. The following result concludes our proof, since $p_{\mathcal{E}_2} P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) < \frac{1}{2} P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$, if the $p_{\mathcal{E}_2}$ initial success probability of encoder $\mathcal{E}_2$ was between $0 < p_{\mathcal{E}_2} < 0.5$.

■

In case of $0 < p_{\mathcal{E}_2} < 0.5$ then the superactivation-assistance of $\mathcal{E}_2$ can enhance the *reliability* the private classical communication over $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ using the quantum relay encoder $\mathcal{E}_2$. Assuming asymptotic limit with $n \to \infty$, for the superactivation-assisted private classical capacity of $\mathcal{M}_1 \otimes \mathcal{M}_2$ the following relation holds:

$$P_{sym}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right)^{\otimes n} \geq P_{sym}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right). \tag{22}$$

Next we show that with the help of the combination of quantum polar encoding and superactivation-assistance the private capacity of $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ can be achieved. The joint channel construction $\mathcal{M}_1 \otimes \mathcal{M}_2$ realizes the quantum relay encoder $\mathcal{E}_2$ with $p_{\mathcal{E}_2} = 1$. Using this scheme, the rate of private communication between Alice and Bob can be increased if initially the $p_{\mathcal{E}_2}$ success probability of $\mathcal{E}_2$ was $0 < p_{\mathcal{E}_2} < 0.5$, while the reliability of the quantum relay encoder can be maximized to the $p_{\mathcal{E}_2} = 1$. We use the same channel $\mathcal{M}$ as defined in (18), but in this case, instead of applying $\rho_{AC}$ in (19) Alice feeds to the inputs of $\mathcal{M}_1 \otimes \mathcal{M}_2$ an arbitrary quantum system $\rho \in \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)$ (assumed being symmetric in *A* and *C*, which will result in $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}} \otimes \mathcal{A}_e = \mathcal{A}_e \otimes \mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$). Using our polar set construction the result of Theorem 2 is satisfied for the quantum relay encoder.

**Theorem 2.** Using superactivation-assisted polar coding and a degraded quantum relay encoder $\mathcal{E}_2$ with $0 < p_{\mathcal{E}_2} < 0.5$ and input $\rho \in \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)$, for the superactivation-assisted private capacity $P_{sym}^{*}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$ and the symmetric private classical capacity $P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$ hold that $\frac{1}{2}P_{sym}^{*}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) > \frac{1}{2}P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$.

*Proof*: For the input system, the quantum coherent information of $\mathcal{M}_1 \otimes \mathcal{M}_2$ is evaluated as follows:

$$\begin{aligned} & I_{coh}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) = p^2 I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}} \otimes \mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) \\ & + p(1-p) I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) + p(1-p) I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) \\ & + p(1-p) I_{coh}\left(\mathcal{A}_e \otimes \mathcal{A}_e\right), \end{aligned} \tag{23}$$

where $I_{coh}\left(\mathcal{A}_e \otimes \mathcal{A}_e\right) = 0$ and $I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}} \otimes \mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) = 0$, since $\mathcal{A}_e \otimes \mathcal{A}_e$ is a symmetric channel [5], while $I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}} \otimes \mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) = 0$, since quantum relay encoder $\mathcal{E}_2$ can add the amplitude information to the phase information received from $\mathcal{E}_1$ in message $A$ only with probability $0 < p_{\mathcal{E}_2} < 0.5$. (The relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ can transmit quantum information only with probability $p_{\mathcal{E}_2}$; otherwise it produces an output $\sigma$, which will result in zero quantum coherent information.) It trivially leads to zero quantum capacity $Q\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}} \otimes \mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) = 0$, since to achieve positive quantum capacity $p_{\mathcal{E}_2} > 0.5$ is required.

■

The main result on the combination of superactivation-assistance and our quantum polar coding scheme is summarized in Theorem 3.

**Theorem 3.** Using the superactivation-assisted quantum relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$, the reliability of any $\mathcal{E}_2$ will be the maximal $p_{\mathcal{E}_2} = 1$ and the symmetric private classical capacity will be lower bounded by $P_{sym}^{*}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) \geq \lim_{n\to\infty}\frac{1}{n}\left(\frac{1}{2}\left|S_{in}\right|\right)$.

*Proof*: Assuming a quantum relay encoder $\mathcal{E}_2$ with reliability $p_{\mathcal{E}_2}$, this result reduces to $p_{\mathcal{E}_2} P_{sym}\left(\mathcal{N}_{\mathcal{E}_2\mathcal{D}}\right)$. Using the channel structure $\mathcal{M}_1 \otimes \mathcal{M}_2$ constructed for the superactivation of quantum relay encoder $\mathcal{E}_2$, using the result obtained in (23),

$$I_{coh}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) = 2p(1-p) I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) \tag{24}$$

where $0 < p < 1$ and $I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) > 0$, combining with

$$P_{sym}^{*}\left(\mathcal{M}_1 \otimes \mathcal{M}_2\right) \geq \frac{1}{2}P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right) \tag{25}$$

and using $P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)=I_{coh}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$, lead us to the following result regarding the symmetric private classical capacity of superactivation-assisted polar encoding-based quantum relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$: $P_{sym}^{*}\left(\mathcal{M}_1\otimes\mathcal{M}_2\right)\geq\frac{1}{2}P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$. In the asymptotic limit with $n\to\infty$, the following lower bound holds:

$$P_{sym}^{*}\left(\mathcal{M}_1\otimes\mathcal{M}_2\right)^{\otimes n}\geq P_{sym}^{*}\left(\mathcal{M}_1\otimes\mathcal{M}_2\right)\geq\lim_{n\to\infty}\frac{1}{n}\left(\frac{1}{2}\left|S_{in}\right|\right). \tag{26}$$

For the polar-coding based superactivation of relay encoder $\mathcal{E}_2$ our proof is concluded as follows:

$$\begin{aligned}&P_{sym}^{*}\left(\mathcal{M}_1\otimes\mathcal{M}_2\right)\geq\lim_{n\to\infty}\frac{1}{n}\left(\frac{1}{2}\left|\left(\mathcal{G}\left(\mathcal{N}_{phase},\beta\right)\right)\cap\left(\mathcal{G}\left(\mathcal{N}_{amp.},\beta\right)\right)\right|\right),\\&P_{sym}^{*}\left(\mathcal{M}_1\otimes\mathcal{M}_2\right)\geq P_{sym}^{*}\left(\mathcal{M}_1\otimes\mathcal{M}_2\right)\geq\lim_{n\to\infty}\frac{1}{n}\left(\frac{1}{2}\left|S_{in}\right|\right),\end{aligned} \tag{27}$$

where $\lim_{n\to\infty}\frac{1}{n}\left|S_{in}\right|\geq P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$, since the maximum of the rate of any private communication over the relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ cannot exceed $\lim_{n\to\infty}\frac{1}{n}\left|S_{in}\right|$, which concludes our proof. For the output $B^{*}$ of the superactivation-assisted quantum relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$:

$$\left|B^{*}\right|=\frac{1}{2}\left(\left|\mathcal{G}\left(\mathcal{N}_{phase},\beta\right)\setminus\mathcal{P}_2\right|\right)=\frac{1}{2}\left|S_{in}\right|>\left|B\right|=p_{\mathcal{E}_2}\left|S_{in}\right|, \tag{28}$$

i.e., if $0<p_{\mathcal{E}_2}<0.5$ the $P_{sym}\left(\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}\right)$ private capacity of $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$ can be achieved by the combination of the proposed polar coding scheme and the superactivated relay channel $\mathcal{N}_{\mathcal{E}_1\mathcal{E}_2\mathcal{D}}$.

■

## 5 Conclusion

In this paper we have shown that by combining the polar coding with superactivation-assistance, the reliability of the quantum relay encoder can be increased and the rate of the private communication over the superactivation-assisted relay quantum channel can be maximized at the same time. The proposed encoding scheme can be a useful tool in private quantum communications.

## Acknowledgment

The results discussed above are supported by the grant TAMOP-4.2.1/B-09/1/KMR-2010-0002, 4.2.2.B-10/1--2010-0009 and COST Action MP1006.

## References


1. T. Cover and A. Gamal, “Capacity theorems for the relay channel,” IEEE Transactions on Information Theory, vol. 25, no. 5, pp. 572 – 584, Sep. 1979.
2. M. Andersson, V. Rathi, R. Thobaben, J. Kliewer, and M. Skoglund, “Nested Polar Codes for Wiretap and Relay Channels”, IEEE Communications Letters, 2010, arXiv:1006.3573v1 [cs.IT] 17 Jun 2010.
3. E. Arikan. Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels. IEEE Transactions on Information Theory, 55(7):3051–3073, July 2009. arXiv:0807.3917.
4. H. Mahdavifar and A. Vardy. Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes. arXiv:1001.0210v2 [cs.IT], April 2010.
5. G. Smith, J. Yard, Quantum Communication with Zero-capacity Channels. Science 321, 1812-1815 (2008).
6. M. M. Wilde and S. Guha. Polar codes for classical-quantum channels. arXiv:1109.2591v1 [quant-ph], September 2011.
7. J. M. Renes, Frederic Dupuis, and Renato Renner, Efficient Quantum Polar Coding, arXiv:1109.3195v1 [quant-ph] 14 Sep 2011
8. J.-C. Boileau, J. M. Renes, Optimal State Merging Without Decoupling, arXiv:0905.1324v1 [quant-ph] 8 May 2009.
9. M. Christandl, A. Winter, Uncertainty, Monogamy, and Locking of Quantum Correlations, IEEE Trans Inf Theory, vol 51, no 9, pp 3159-3165 (2005).
10. S. Imre, F. Balázs: Quantum Computing and Communications – An Engineering Approach, Published by John Wiley and Sons Ltd, (2005).
11. I. Devetak, “The private classical capacity and quantum capacity of a quantum channel,” IEEE Trans. Inf. Theory, vol. 51, pp. 44–55, quant-ph/0304127, (2005).
12. L. Gyongyosi, S. Imre, “Quantum Polar Coding for Noisy Optical Quantum Channels,” APS DAMOP 2012 Meeting, The 43rd Annual Meeting of the APS Division of Atomic, Molecular, and Optical Physics, Jun. 2012, Anaheim, California, USA.
13. M. M. Wilde, J. Renes, “Quantum polar codes for arbitrary channels”, arXiv:1201.2906v1 [quant-ph] 13 Jan 2012.
14. L. Gyongyosi, S. Imre: Algorithmic Superactivation of Asymptotic Quantum Capacity of Zero-Capacity Quantum Channels, Information Sciences, ELSEVIER, 2011.
15. S. Imre, L. Gyongyosi: Advanced Quantum Communications - An Engineering Approach, Publisher: Wiley-IEEE Press (New Jersey, USA), John Wiley & Sons, Inc., The Institute of Electrical and Electronics Engineers. (2012)
16. L. Gyongyosi, S. Imre: “Private Classical Communication over Zero-Capacity Quantum Channels Using Quantum Polar Codes,” The 7th Conference on Theory of Quantum Computation, Communication, and Cryptography (TQC 2012), Jun. 2012.
17. F. Brandao and J. Oppenheim, “Public Quantum Communication and Superactivation,” arXiv:1005.1975. (2010).
18. F. Brandao, J. Oppenheim and S. Strelchuk, "When does noise increase the quantum capacity?", arXiv:1107.4385v1 [quant-ph] (2011)
19. S. Imre, L. Gyongyosi: Quantum-assisted and Quantum-based Solutions in Wireless Systems, with L. Hanzo, H. Haas, D. O’Brien and M. Rupp, in: "Wireless Myths, Realities and Futures: From 3G/4G to Optical and Quantum Wireless", Proceedings of the IEEE, Volume: 100, pp. 1853-1888, Issue: Special Centennial Issue, ISSN: 0018-9219, 2012.
20. K. Bradler, P. Hayden, D. Touchette, and M. M. Wilde, Trade-off capacities of the quantum Hadamard channels, arXiv:1001.1732v2, (2010).
21. M. M. Wilde, J. Renes, “Polar codes for private classical communication”, arXiv:1203.5794.