Secure Communication over Zero Private-Capacity Quantum Channels

Laszlo Gyongyosi[1*] and Sandor Imre[1]
[1]Budapest University of Technology and Economics, Budapest, Hungary
gyongyosi@hit.bme.hu

Abstract

In this work a new phenomenon called polaractivation is introduced. Polaractivation is based on quantum polar encoding and the result is similar to the superactivation effect — positive capacity can be achieved with zero-capacity quantum channels. However, polaractivation has many advantages over the superactivation: it is limited neither by any preliminary conditions on the quantum channel nor on the maps of other channels involved in the joint channel structure. We prove that the polaractivation works for arbitrary zero private-capacity quantum channels and we demonstrate, that the symmetric private classical capacity of arbitrary zero private-capacity quantum channels is polaractive. An immediate practical application of the proposed effect is to private quantum communications, quantum repeater networks and long-distance quantum communications.

1 Introduction

In this work a new phenomenon called *polaractivation* is introduced. The result of our effect is similar to the superactivation effect. The *superactivation* (Smith and Yard, 2008) is an extreme violation of additivity (Hastings, 2009) of quantum channel capacities and enables the use of zero-capacity quantum channels for communication (Brandao et al, 2011). The superactivation effect was discovered by Smith and Yard in 2008 (Smith and Yard, 2008), (Smith et al., 2011), and they have shown this effect works for the quantum capacity. Later, these results were extended to the classical zero-error capacity (Cubitt et al., 2009), (Duan, 2009) and to the quantum zero-error capacity (Cubitt and Smith, 2009). An important difference between superactivation and the polaractivation that polaractivation is *limited neither by* any preliminary conditions on the initial private capacity of the channel nor on the maps of other channels involved to the joint channel structure (Gyongyosi and Imre, 2012a), (Gyongyosi and Imre, 2012b), (Gyongyosi and Imre, 2012c). We present that the proposed polaractivation requires only the quantum polar encoding scheme to activate the *symmetric* private classical capacity of any quantum channel.

The polar coding technique was developed for classical systems to achieve the *symmetric* capacity of a classical 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 (Arikan, 2006), (Arikan, 2009), (Arikan, 2010), (Arikan, 2010a), (Arikan and Telatar, 2009), (Hussami et al, 2009), (Korada et al, 2010), (Mahdavifar and Vardy, 2010), (Mori and Tanaka, 2009), (Sasoglu et al.,2009). The channel polarization scheme introduced by Arikan (Arikan, 2009) for classical channels is a revolutionary encoding and decoding scheme, which makes possible the construction of codewords to achieve the symmetric capacity. Recently, in the quantum setting, the polar coding scheme was studied by Wilde and Guha (Wilde and Guha, 2011), by Renes et al. (Renes et al., 2011), by Wilde and Renes (Wilde and Renes, 2012), (Wilde and Renes, 2012a). As was shown in (Renes et al., 2011) and (Wilde and Renes, 2012) an efficient scheme also can be constructed for the quantum communication channels; however. Here, we show that the quantum

polar coding using the results of (Wilde and Guha, 2011) and (Renes et al., 2011) can be used for the *polaractivation* of private classical capacity.
In this paper we present that the polar coding scheme can be used to transmit classical information privately over noisy quantum channels; however, initially, these channels are so noisy that they cannot transmit any classical information *privately*. We demonstrate that quantum polar coding can be used for the polaractivation of private classical capacity of any quantum channels i.e. the private classical capacity is *polaractive*. Furthermore, due to the proposed polaractivation any quantum channel that had zero private classical capacity initially, can be used for private communication.

This paper is organized as follows: In Section 2, we review the basic definitions of delivering private classical communication over a quantum channel. Section 3 introduces the polar encoding scheme. In Section 4, we interpret our theorems and the proofs regarding the proposed quantum polar codeword construction scheme and the security of the proposed encoding. Finally, in Section 5, we conclude the results.

2 The Symmetric Private Classical Capacity of Quantum Channels

In this section we overview the basic definitions and formulas related to the private classical communication over noisy quantum channels.

2.1 The Classical Capacity

The *classical capacity* $C(\mathcal{N})$ of a quantum channel $\mathcal{N}$ describes the maximum amount of classical information that can be transmitted through the channel. The *Holevo-Schumacher-Westmoreland* (HSW) theorem (Holevo, 1998), (Schumacher and Westmoreland, 1997) defines this quantity for product state input (i.e. entanglement is not allowed between input quantum bits) and single channel use as

$$C^{(1)}(\mathcal{N}) = \max_{all\ p_i,\rho_i} \chi = \max_{all\ p_i,\rho_i} \left(\mathrm{S}\left(\mathcal{N}\left(\sum_i p_i \rho_i \right) \right) - \sum_i p_i \mathrm{S}\left(\mathcal{N}(\rho_i) \right) \right) \tag{1}$$

where $\mathrm{S}(\rho) = -Tr(\rho \log(\rho))$ is the von Neumann entropy, and χ is called the Holevo quantity and the maximum is taken over all $\{p_i, \rho_i\}$ ensembles of input quantum states (Gyongyosi and Imre, 2012), (Imre and Gyongyosi, 2012). The HSW theorem is a generalization of Shannon's the classical noisy channel-coding theorem. However, the HSW theorem raised a lot of questions regarding the transmission of classical information over general quantum channels (Hayashi and Nagaoka, 2003), (Imre and Balazs, 2005), (Imre and Gyongyosi, 2012a), (Gyongyosi and Imre, 2012c), (Gyongyosi and Imre, 2012d). Hastings showed that the entangled inputs can increase the amount of received classical information (Hastings, 2009), and defined as

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} C^{(1)}\left(\mathcal{N}^{\otimes n} \right), \tag{2}$$

where $\mathcal{N}^{\otimes n}$ denotes the *n* uses of the quantum channel $\mathcal{N}$.

2.2 The Private Classical Capacity

The *private classical capacity* $P(\mathcal{N})$ of quantum channel $\mathcal{N}$ describes the maximum rate at which the channel is able to send classical information through the channel between Alice (A) and Bob (B) in *secure* way i.e. without any information leaked about the plain text message to an malicious eavesdropper Eve (E) (Devetak, 2005), (Lloyd, 1997), (Shor, 2002).

The block diagram of a generic private quantum communication system is depicted in Fig. 1. The first output of the channel belongs to Bob and denoted by $\rho_B = \mathcal{N}(\rho_A)$ while the second "receiver" is the environment (i.e., the eavesdropper) *E*, with state $\rho_E = E(\rho_A)$. In Fig. 1, we also depict the encoding scheme. Alice encodes her classical information into the phases of quantum bits using the *X* basis and than into their amplitudes using the *Z* basis. The phase carries the *data* and the amplitude is the *key* for the encryption i.e., Alice first encodes the phase (data) and then the amplitude (key). Bob applies it in the reverse order using his successive and coherent decoder, as was shown by Boileau and Renes in (Boileau and Renes, 2009) and (Renes et al., 2011): he first decodes the *amplitude* (key) information in the *Z* basis. Then Bob continues the decoding with the *phase* information, in the *X* basis.

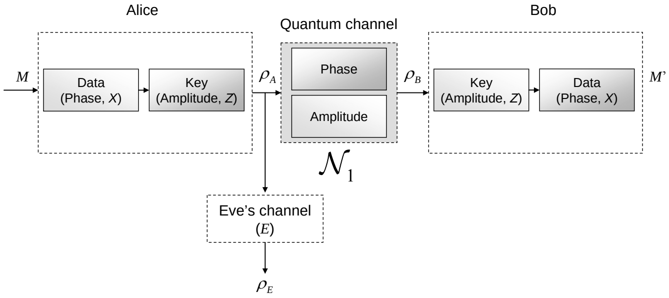

Fig. 1. Private communication of Alice and Bob over a quantum channel in presence of an eavesdropper Eve. The quantum channel has positive private classical capacity if it can send both phase and amplitude.

Based on this model the single-use private classical capacity can be expressed as the maximum of the difference between $I(A:B)$ which measures the classical information transmitted between Alice and Bob, and $I(A:E)$ that represents the information leaked to the eavesdropper (Devetak, 2005)

$$P^{(1)}(\mathcal{N}) = \max_{all\ p_i, \rho_i} \left(I(A:B) - I(A:E) \right). \tag{3}$$

The optimization has to be taken over all possible source distributions and encoding schemes $\{p_i, \rho_i\}$ of Alice $\rho_A \in \{\rho_i\}$.

The corresponding information diagram can be seen in Fig. 2, where conditional entropies are denoted by $H(\cdot|\cdot)$ and *H* is the Shannon entropy (Brandao and Oppenheim, 2010).

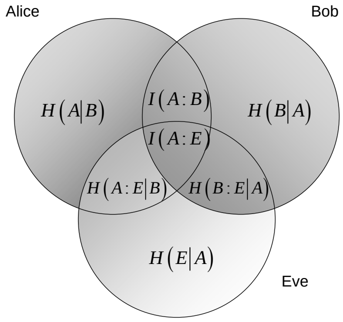

Fig. 2. The private classical information is the difference of two mutual information functions $I(A:B)$ and $I(A:E)$ measured between Alice and Bob and Alice and Eve.

The asymptotic private capacity can be determined from the single-use capacity as (Devetak, 2005)

$$P(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\max_{all\ p_i,\rho_i}\left(I(A:B)-I(A:E)\right)^{\otimes n}. \tag{4}$$

The private capacity can be rewritten using the Holevo quantity as follows (Devetak, 2005), (Schumacher and Westmoreland, 2000):

$$P(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\max_{all\ p_i,\rho_i}\left(\mathcal{X}_{AB}-\mathcal{X}_{AE}\right)^{\otimes n}, \tag{5}$$

where

$$\mathcal{X}_{AB} = \mathrm{S}\left(\mathcal{N}_{AB}(\rho_{AB})\right) - \sum_i p_i \mathrm{S}\left(\mathcal{N}_{AB}(\rho_i)\right) \tag{6}$$

and

$$\mathcal{X}_{AE} = \mathrm{S}\left(\mathcal{N}_{AE}(\rho_{AE})\right) - \sum_i p_i \mathrm{S}\left(\mathcal{N}_{AE}(\rho_i)\right) \tag{7}$$

In case of asymptotic capacity Alice's encoding transformation is amended with

$$\mathcal{E}:\{0,1\}^l \to \{0,1\}^n \tag{8}$$

which takes the *l*-length input *M*, and from this message it constructs an *n*-length classical message before feeding transformation *X* and *Z*. Next, the produced ρ_A quantum codeword having *n* qubit of length is transmitted over the noisy quantum channel by the *n* channel uses.

2.3 The Symmetric Private Classical Capacity

In our scheme, the recursive channel construction is the key ingredient to achieving the polarization effect, which splits the channels into two easily separable sets—one that cannot achieve the symmetric private capacity $P_{sym}(\mathcal{N})$ (i.e., these channels will have $P_{sym}=0$) and a second set, in which the channels almost completely and perfectly can achieve the symmetric private capacity $P_{sym}(\mathcal{N})$. The *symmetric classical capacity* of the quantum channel is defined for *uniform* input distribution. For the symmetric private classical capacity the same condition holds, and it can be expressed as follows (Smith et al., 2011):

$$P_{sym}(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\max_{all\ p_i,\rho_i}\left(I(A:B)-I(A:E)\right)^{\otimes n}, \tag{9}$$

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

According to our encoding scheme, the C_{sym} *symmetric classical* and P_{sym} *symmetric private classical* capacities are defined as the sum of the phase and amplitude channels

$$C_{sym}\left(\mathcal{N}_1\right)=\lim_{n\to\infty}\frac{1}{n}\max_{all\ p_i,\rho_i}\left(I_{sym.}^{phase}\left(A:B\right)+I_{sym.}^{ampl.}\left(A:B\right)\right)^{\otimes n}, \tag{10}$$

and

$$\begin{aligned}P_{sym}\left(\mathcal{N}_1\right)&=\lim_{n\to\infty}\frac{1}{n}\max_{all\ p_i,\rho_i}\left(I_{sym.}^{phase}\left(A:B\right)-I\left(A:E\right)\right)^{\otimes n}=\\&=\lim_{n\to\infty}\frac{1}{n}\max_{all\ p_i,\rho_i}\begin{pmatrix}S\left(\left(\sigma_0^{phase}+\sigma_1^{phase}\right)/2\right)-S\left(\sigma_0^{phase}/2\right)\\-S\left(\sigma_1^{phase}/2\right)-I\left(A:E\right)\end{pmatrix}^{\otimes n},\end{aligned} \tag{11}$$

where $I\left(A:E\right)=S\left(A\right)+S\left(E\right)-H\left(AE\right)$ stand for the mutual information function between Alice and Eve, while $I_{sym.}^{phase}\left(A:B\right)$ and $I_{sym.}^{ampl.}\left(A:B\right)$ are the symmetric mutual information that can be achieved by the phase and amplitude information between Alice and Bob.

2.4 Degraded and Non-degradable Quantum Channel

The main channel between Alice and Bob is defined by $\mathcal{N}_{Bob}\left(B\middle|A\right)$, while Eve's channel is

$$\mathcal{N}_{Eve}\left(E\middle|A\right)=\sum_B\mathcal{N}_{Bob}\left(B\middle|A\right)\circ\mathcal{N}_d\left(E\middle|B\right), \tag{12}$$

where $\mathcal{N}_d\left(E\middle|B\right)$ is the *degradation channel*, $\circ$ is the channel concatenation, while y and z denote Bob's and Eve's output. If Eve's channel is *degradable*, then her channel $\mathcal{N}_{Eve}\left(E\middle|A\right)$ can be expressed as the cascade of Bob's channel $\mathcal{N}_{Bob}\left(B\middle|A\right)$ and the prefix degradation channel $\mathcal{N}_d\left(E\middle|B\right)$. For the error probabilities of the degraded quantum channel $\mathcal{N}_{Eve}$, the relation $p_{Eve}\geq p_{Bob}$ holds. For a *non-degraded* quantum channel $\mathcal{N}_{Eve}$, $p_{Eve}<p_{Bob}$. In the proposed scheme it is assumed that Eve's channel is symmetric; however, if Eve's channel is *not symmetric*, a *prefix* channel can be used to have this property (Koyluoglu and El Gamal, 2010).

3 Quantum Polar Coding

Polar codes belong to the group of error-correcting codes (Arikan, 2009). They introduce no redundancy only operate on codewords of *n* qubit of length. They can be used to achieve the symmetric capacity of classical discrete memoryless channels (DMCs). The basic idea behind the construction of polar codes is channel selection called polarization: assuming *n* identical DMCs we can create two sets by means of an encoder. "Good" channels are nearly noiseless while "bad" channels have nearly zero capacity. Furthermore, for large enough *n*, the fraction of good channels approaches the symmetric capacity of the original DMC. The polarization effect is represented by means of generator matrix G_k having $k\times k$ of size (Arikan, 2009) calculated in a recursive way

$$G_k=\left(I_{k/2}\otimes G_2\right)R_k\left(I_2\otimes G_{k/2}\right), \tag{13}$$

where $G_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ and $I_{k/2}$ is the $\frac{k}{2} \times \frac{k}{2}$ identity matrix and R_k is the $k \times k$ permutation operator. Now we present how matrix *G* is related to the polarization effect. For an input message *M* having $n = 2^k$ length, the encoded codeword ρ_A is

$$\rho_A = f(M) = G_k M \,, \tag{14}$$

i.e., if $k = 2$, then

$$G \begin{pmatrix} M_1 \\ M_2 \end{pmatrix} = \begin{pmatrix} M_1 \oplus M_2 \\ M_2 \end{pmatrix}. \tag{15}$$

The difference between the two channels is the knowledge of input u_1 on Bob's side. For the 'bad' channel $\mathcal{B}$ the input u_1 is unknown. The recursion can be repeated over *k* levels, with $n = 2^k$ channel uses. The two independent $\mathcal{N}_2$ channels are combined into a higher-level channel, denoted by $\mathcal{N}_4$. The 'bad' and 'good' channels from are defined as follows:

$$\begin{aligned} \mathcal{G} &\equiv \mathcal{N}_2\left(y_1, y_2 | u_1\right) = \frac{1}{2} \sum_{u_2 \in \{0,1\}} \mathcal{N}_1\left(y_1 | u_1 \oplus u_2\right) \mathcal{N}_1\left(y_2 | u_2\right), \\ \mathcal{B} &\equiv \mathcal{N}_2\left(u_1, y_1, y_2 | u_2\right) = \frac{1}{2} \mathcal{N}_1\left(y_1 | u_1 \oplus u_2\right) \mathcal{N}_1\left(y_2 | u_2\right). \end{aligned} \tag{16}$$

Using the polarized channel structure, for any $\beta < 0.5$, and assuming $n \to \infty$:

$$\lim_{n \to \infty} \Pr\left(B\left(\mathcal{N}^{\otimes n}\right) < 2^{-2n\beta}\right) = I\left(\mathcal{N}^{\otimes n}\right). \tag{17}$$

The following important result can be derived from (16) for the mutual information of these channels for uniform inputs u_1 and u_2, namely (Wilde and Guha, 2011)

$$\begin{aligned} & I\left(\mathcal{N}_2\left(y_1, y_2 | u_1\right)\right) + I\left(\mathcal{N}_2\left(u_1, y_1, y_2 | u_2\right)\right) \\ & = I\left(u_1 : y_1 y_2\right) + I\left(u_2 : u_1 y_1 y_2\right) \\ & = 2I\left(\mathcal{N}_1\right), \end{aligned} \tag{18}$$

where

$$I\left(u_1 : y_1 y_2\right) \le I\left(\mathcal{N}_1\right) \tag{19}$$

and

$$I\left(u_2 : u_1 y_1 y_2\right) \ge I\left(\mathcal{N}_1\right), \tag{20}$$

i.e.,

$$\begin{aligned} & I\left(u_1 : y_1 y_2\right) \le I\left(\mathcal{N}_1\right) \le I\left(u_2 : u_1 y_1 y_2\right) \\ & I\left(\mathcal{N}_2\left(y_1, y_2 | u_1\right)\right) \le I\left(\mathcal{N}_1\right) \le I\left(\mathcal{N}_2\left(u_1, y_1, y_2 | u_2\right)\right). \end{aligned} \tag{21}$$

For the polarized 'bad' $\mathcal{B}(\mathcal{N}, \beta)$ and 'good' $\mathcal{G}(\mathcal{N}, \beta)$ channels the following rules hold:

$$\mathcal{G}(\mathcal{N},\beta) \equiv \left\{ i \in n : B\left(\mathcal{N}_i^{\otimes n}\right) < \frac{1}{n} 2^{-n^{\beta}} \right\},$$
$$\mathcal{B}(\mathcal{N},\beta) = [n] \setminus \mathcal{G}(\mathcal{N}_i,\beta). \tag{22}$$

In (22), parameter β is defined as

$$\beta = \frac{1}{n}\sum_{i=1}^{n} \log_n d_i \text{ ,} \tag{23}$$

where $d_i = d_{\min}\left(\mathbf{g_i}, \mathbf{g_{i+1}}, \ldots, \mathbf{g_n}\right)$, and g_i is the i^{th} row vector of matrix G_n As was shown by Arikan (Arikan, 2009), Korada, Sasoglu, and Urbanke (Korada et al, 2010), $\beta \leq 0.5$ if $k < 15$, while for $n \geq 16$: $\beta > 0.5$, along with

$$\lim_{n\to\infty} \frac{1}{n}\beta = 1 \text{ .} \tag{24}$$

Private classical communication over these structures means the following: in her message *A*, Alice sends her encoded private message *M* only over channels $\mathcal{G}(\mathcal{N},\beta)$, while the remaining parts of *A* are transmitted via $\mathcal{B}(\mathcal{N},\beta)$. Moreover, after the channels are being polarized, the fraction of $\mathcal{G}(\mathcal{N},\beta)$ and $\mathcal{B}(\mathcal{N},\beta)$ will be equal to the symmetric private classical capacity $P_{sym}(\mathcal{N})$. In our case, the input quantum channels $\mathcal{N}^{\otimes n}$ are insecure, i.e., they cannot transmit the amplitude and phase information simultaneously; however, using polar encoding, the parties will be able send both the amplitude and the phase over $\mathcal{N}^{\otimes n}$.

4 The Polaractivator Encoding Scheme

The proposed polar coding scheme assumes the use of noisy quantum channels with amplitude and phase coding, similar to the scheme of Renes et al. (Renes et al., 2011). The parties can use either the amplitude or the phase to encode classical information; however, the transmission of private classical *information* requires both amplitude and phase coding *simultaneously*. If Alice wants to send Bob classical (i.e., not private) information, then she can encode her information either into the amplitude or phase using the *Z* and *X* bases. It is possible for quantum channels, since for these channels the polarization occurs in *both* amplitude and phase (Renes et al., 2011). On the other hand, if she wants to send her classical information privately, then she has to encode her information *simultaneously* in the amplitude (in the *Z* basis) and in the phase (in the *X* basis). As shown by Christandl and Winter (Christandl and Winter, 2005), if Alice can send both amplitude and phase, then she can also send entanglement to Bob.

The successful decoding of the amplitude information (key) is a necessary but not sufficient condition for the positive private classical capacity $P > 0$; the $P_{sym}(\mathcal{N})$ symmetric private capacity is calculated only from the symmetric classical capacity $C_{sym.}^{phase}(\mathcal{N})$, which can be achieved by the phase information. The input quantum channels are so noisy that they cannot transmit the amplitude and phase information simultaneously; however, they can send the amplitude or the phase, but not both of them at the same time (i.e., these channels have some symmetric classical capacity $C_{sym}(\mathcal{N}) > 0$, but have no symmetric private classical capacity, i.e., $P_{sym}(\mathcal{N}) = 0$). First we show that with the help of the polarization effect, the P_{sym} symmetric private classical capacity of these noisy channels can be polaractivated.

4.1 Theorems and Proofs

In this section we present the theorems and the proofs regarding the polaractivation of private classical capacity of zero private-capacity quantum channels.

<u>Theorem 1.</u> *The polaractivation of the symmetric private classical capacity of arbitrary quantum channels results in a non-empty set of polar codewords which set achieves the symmetric private classical capacity of the quantum channel.*

Proof. First we construct the input codewords and show that while initially the set of polar codewords which can transmit private classical information is empty in the initial phase, by the proposed polar encoder this set can be transformed into a non-empty set. The S_{in} set of polar codewords that can transmit private information is defined as follows:

$$S_{in} = \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right), \tag{25}$$

where $\left|S_{in}\right| = l$. All of the other input codewords cannot be used for private classical communication and defined by the set S_{bad} as follows:

$$\begin{aligned} S_{bad} = &\left(\mathcal{G}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{B}\left(\mathcal{N}_{phase}, \beta\right)\right) \\ &\cup\left(\mathcal{B}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)\right) \\ &\cup\left(\mathcal{B}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{B}\left(\mathcal{N}_{phase}, \beta\right)\right), \end{aligned} \tag{26}$$

where $\left|S_{bad}\right| = n - l$. From set S_{bad}, we define the completely useless codewords as

$$\mathcal{B} = \mathcal{B}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{B}\left(\mathcal{N}_{phase}, \beta\right), \tag{27}$$

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

$$\mathcal{P}_1 = \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{B}\left(\mathcal{N}_{phase}, \beta\right) \tag{28}$$

and

$$\mathcal{P}_2 = \mathcal{B}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right). \tag{29}$$

The input codewords from $\mathcal{P}_1$ and $\mathcal{P}_2$ cannot be used to transmit classical information *privately*, since these codewords do not satisfy our requirements on the encoding of private information (only set S_{in} is allowed in the proposed scheme). Before the polaractivation is realized, the quantum channel $\mathcal{N}$ could not transmit any private classical information, i.e.:

$$S_{in} = \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right) = \varnothing \tag{30}$$

and $\left|S_{in}\right| = 0$. To prove the polaractivation of private classical capacity we have to show that by using quantum polar codes, the transformation of $S_{in} = \varnothing$ into $S_{in} \neq \varnothing$ can be achieved. The valuable indexes of input message *A* transmit the *l*-length private message. Eve will receive only garbage bits in the remaining $n - l$ bits of *A*. The private information is encoded in the amplitude and phase, simultaneously. From Alice's input message *M*, her $\mathcal{E}$ encoder creates a *n*-length message A. If $S_{in} \neq \varnothing$, then private communication is possible between Alice and Bob, and *l* bits from the *A* input message of the noisy quantum channel $\mathcal{N}$ will be a codeword from the set S_{in}, denoted by $s_{in} \in S_{in}$. From the channel output message *B*, Bob's decoder $\mathcal{D}$ constructs the decoded private message M'. Using p_{Eve} Eve's error probability and positive parameters $\gamma > 0$ and $\lambda > 1$ for codeword set $\mathcal{P}_1 \cup \mathcal{P}_2$:

$$\left|\mathcal{P}_1 \cup \mathcal{P}_2\right| \geq n\left(1 - p_{Eve} - \frac{1}{n^{\lambda}}\gamma\right). \tag{31}$$

From this result, for the set $S_{in} = \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)$:

$$\left|S_{in}\right| = n \cdot p_{Eve} + \frac{1}{n^{1-\lambda}}\gamma, \tag{32}$$

and

$$\begin{aligned} H(M) &= \left|\mathcal{G}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)\right| \\ &= \left|S_{in}\right| = n \cdot p_{Eve} + \frac{1}{n^{1-\lambda}}\gamma. \end{aligned} \tag{33}$$

Using $\left|S_{in}\right|$, it follows that the following private capacity can be achieved between Alice and Bob, assuming *n* channel uses:

$$P_{sym} \geq C_{Bob} - \frac{1}{n^{\lambda}}\gamma, \tag{34}$$

and, as shown by Arikan (Arikan, 2009), this result is guaranteed by those codewords for which the following conditions are satisfied. For the *l* valuable bits from the given codeword s_{in} selected from $\left|S_{in}\right|$, a $seq_n^i \leq C_{Bob} \cdot e^{n^{\beta}}$, $for\ i \in [n]$ sequence is generated using the initial condition $seq_1^{(1)} = p_{Eve}$:

$$\begin{aligned} seq_{2l}^{(2i-1)} &= 2seq_l^{(i)} - \left(seq_l^{(i)}\right)^2,\ for\ i \in [l] \\ seq_{2l}^{(2i)} &= \left(seq_l^{(i)}\right)^2,\ for\ i \in [l]. \end{aligned} \tag{35}$$

For this sequence, as $n \to \infty$

$$H\left(M \middle| E\right) \to H(M) \tag{36}$$

and, as a corollary, (32) and (33) are trivially satisfied, which concludes the proof on the achievability of codeword s_{in} from the set S_{in}. The sets $\mathcal{P}_1$ and $\mathcal{P}_2$ are disjoint, thus

$$\left|\mathcal{P}_1 \cup \mathcal{P}_2\right| = \left|\mathcal{P}_1\right| + \left|\mathcal{P}_2\right|, \tag{37}$$

since if Eve's channel is assumed to be degraded thus

$$\lim_{n \to \infty} \frac{1}{n}\left|\mathcal{P}_2\right| = 0 \tag{38}$$

and $\left|\mathcal{P}_2 \cap \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right)\right| = 0$ with $\left|\mathcal{B}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right)\right| = 0$, which follows from the fact that $\mathcal{P}_2 \subseteq \mathcal{B}\left(\mathcal{N}_{amp}, \beta\right)$, where $\mathcal{B}\left(\mathcal{N}_{amp}, \beta\right) = [n] \setminus \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right)$ and $\left|\mathcal{P}_2 \cap \left(S_{in} \cup \mathcal{B}\right)\right| = 0$ along with $\mathcal{P}_1 \cup \mathcal{P}_2 \subseteq \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right)$. For the proposed scheme, $\mathcal{P}_1 \subseteq \mathcal{G}\left(\mathcal{N}_{amp}, \beta\right)$, which proves that the defined codewords sets $\mathcal{P}_1$ and $\mathcal{P}_2$ are pairwise disjoint, since

$$\lim_{n \to \infty} \frac{1}{n}\left|\mathcal{G}\left(\mathcal{N}_{amp}, \beta\right)\right| + \lim_{n \to \infty} \frac{1}{n}\left|[n] \setminus \left(\mathcal{P}_1 \cup \mathcal{P}_2\right)\right| = 1, \tag{39}$$

with

$$\begin{aligned} &\left|\mathcal{G}\left(\mathcal{N}_{amp}, \beta\right)\right| + \left|\mathcal{B}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)\right| \\ &+ \left|[n] \setminus \left(\mathcal{P}_1 \cup \mathcal{P}_2\right)\right| \leq n \end{aligned} \tag{40}$$

and

$$\begin{aligned} &\left([n] \setminus \left(\mathcal{P}_1 \cup \mathcal{P}_2\right)\right) \subseteq \left(\mathcal{G}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)\right) \\ &\cup \left(\mathcal{B}\left(\mathcal{N}_{amp}, \beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta\right)\right) \end{aligned} \tag{41}$$

are satisfied, i.e., the empty set of private input codewords is transformed into a non-empty set

$$S_{in} = \mathcal{G}\left(\mathcal{N}_{amp},\beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase},\beta\right) \neq \varnothing \tag{42}$$

which proves that if there exists a non-empty set S_{in}, then the polaractivation of private classical capacity of arbitrary quantum channels can be achieved which concludes the proof.

■

The proposed results on the achievable rate of secret private communication assuming a degraded quantum channel $\mathcal{N}_{Eve}$ between Alice and Bob are summarized in Theorem 2.

<u>Theorem 2.</u> The symmetric private classical capacity of degraded quantum channels can be polaractivated.

Proof. Assuming a *degraded* quantum channel $\mathcal{N}_{Eve}$, the following P_{sym} symmetric private classical capacity can be achieved over the quantum channel $\mathcal{N}_{Bob}$:

$$\begin{aligned} P_{sym} &= \lim_{n\to\infty}\frac{1}{n}\max\left(\left|S_{in}\right|\right) \\ &= \lim_{n\to\infty}\frac{1}{n}\max\left|\mathcal{G}\left(\mathcal{N}_{amp},\beta\right) \cap \mathcal{G}\left(\mathcal{N}_{phase},\beta\right)\right|. \end{aligned} \tag{43}$$

First, we give the proof of P_{sym}, then for the rate R_{sym}. Assuming $\beta < 0.5$,

$$C\left(\mathcal{N}_{Eve}^{\otimes n}\right) = \lim_{n\to\infty}\frac{1}{n}\max\left(\left|\mathcal{P}_1\right| + \left|\mathcal{P}_2\right|\right). \tag{44}$$

Combing this result with (38), we get

$$C\left(\mathcal{N}_{Eve}^{\otimes n}\right) = \lim_{n\to\infty}\frac{1}{n}\max\left(\left|\mathcal{P}_1\right|\right) \tag{45}$$

and

$$\begin{aligned} &C\left(\mathcal{N}_{Bob}^{\otimes n}\right) = 1 - C\left(\mathcal{N}_{Eve}^{\otimes n}\right) \\ &= 1 - \lim_{n\to\infty}\frac{1}{n}\max\left(\left|\mathcal{P}_1\right|\right). \end{aligned} \tag{46}$$

The result obtained in (46) can be rewritten as follows:

$$C\left(\mathcal{N}_{Bob}^{\otimes n}\right) = \lim_{n\to\infty}\frac{1}{n}\max\left(\left|S_{in}\right| \cup \left|\mathcal{P}_2\right|\right) = \lim_{n\to\infty}\frac{1}{n}\max\left(\left|S_{in}\right|\right). \tag{47}$$

According to our polar coding scheme, for the B Bhattacharya parameter, the input codewords in $\mathcal{P}_1$:

$$\mathcal{P}_1 = \left\{ i \in n : B\left(\mathcal{N}_i^{\otimes n}\right) < \frac{1}{n}2^{-n^{\beta}} \right\}, \tag{48}$$

where $\beta < 0.5$, and

$$S_{in} \cup \mathcal{P}_2 = \left\{ i \in n : B\left(\mathcal{N}_i^{\otimes n}\right) \geq \frac{1}{n}2^{-n^{\beta}} \right\}. \tag{49}$$

From the definition of (48) and (49), for the Bhattacharya parameters of these codewords, we have the following relation. From the polar encoding scheme, it follows that

$$B\left(S_{in} \cup \mathcal{P}_2\right) \leq \frac{1}{n}2^{-n^{\beta}}, \tag{50}$$

and for the Bhattacharya parameters of $\mathcal{P}_1$:

$$B\left(\mathcal{P}_1\right) \geq 1 - \frac{1}{n}2 \cdot 2^{-n^{\beta}}. \tag{51}$$

Since

$$\mathcal{P}_1 \cap \left(S_{in} \cup \mathcal{P}_2 \right) = \varnothing , \tag{52}$$

the constructed codeword sets S_{in}, $\mathcal{P}_1$, $\mathcal{P}_2$, and $\mathcal{B}$ are disjoint sets with relation $\left| S_{in} \cup \mathcal{P}_1 \cup \mathcal{P}_2 \right| = n$. Since Eve's channel is degraded,

$$\lim_{n\to\infty} \frac{1}{n} \left| \mathcal{B} \right| = 0, \tag{53}$$

which concludes our proof on $P_{sym}\left(\mathcal{N} \right)$ for a degraded eavesdropper channel:

$$P_{sym}\left(\mathcal{N} \right) = \lim_{n\to\infty} \frac{1}{n} \max \left| S_{in} \right|. \tag{54}$$

The rate R_{sym} can be rewritten as follows:

$$\begin{aligned} R_{sym} &= \lim_{n\to\infty} \frac{1}{n} \max \left(\left| S_{in} \right| - \left| \mathcal{P}_2 \right| + \left| \mathcal{P}_2 \right| \right) = \lim_{n\to\infty} \frac{1}{n} \max \left(\left| S_{in} \right| \right) \\ &= \lim_{n\to\infty} \frac{1}{n} \max \left(\left| \mathcal{G}\left(\mathcal{N}_{amp}, \beta \right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta \right) \right| \right). \end{aligned} \tag{55}$$

If $\mathcal{N}_{Eve}$ is a degraded quantum channel, then achievable codewords are

$$\left| \mathcal{G}\left(\mathcal{N}_{amp}, \beta \right) \cap \mathcal{G}\left(\mathcal{N}_{phase}, \beta \right) \right| , \tag{56}$$

from which the proof of (43) is concluded. These results conclude that for the non-empty sets $\left| S_{in} \right|$ the private classical capacity will be positive which concludes the proof on the polaractivation.

■

The results on the achievable rate of secret private communication assuming a non-degraded quantum channel can be derived in similar way. From the proposed encoding scheme follows, that for the positive P_{sym} symmetric capacity there exits the codeword set $S_{in} \neq \varnothing$, and the theorem is proven for any non-degraded quantum channels.

4.2 Polaractivated Private Capacity

The symmetric private classical capacity of *arbitrary* degraded and non-degraded quantum channels is proven. The polaractivation will result in the non-empty set $S_{in} \neq \varnothing$, and the channel will be able to transmit classical information privately.

The polaractivation of any symmetric channel capacities of arbitrary quantum channels requires only the proposed polar encoding scheme and the multiple uses of the same quantum channel. The polaractivation works for any channel capacities, here we demonstrate the results for polaractivation of the P_{sym} symmetric private classical capacity of quantum channels and prove that the polaractivation of arbitrary quantum channels can be achieved by the proposed polar encoding scheme. The quantum channel $\mathcal{N}$ has some positive symmetric capacity $C_{sym} > 0$, while it has zero private classical capacity, $P_{sym} = 0$. We prove that using quantum polar encoding and the same quantum channel $\mathcal{N}$ with n times, the private classical capacity can be polaractivated, i.e., the transformation $P_{sym} = 0 \rightarrow P_{sym} > 0$ can be achieved.

5 Conclusions

The polar coding is a revolutionary channel coding technique, which makes it possible to achieve the symmetric capacity of a noisy communication channel by the restructuring of the initial error probabilities. In the case of a quantum system, the problem is more complicated, since the error characteristic of a quantum communication channel significantly differs from the characteristic of quantum communication channels. In this paper, we introduced the term *polaractivation*. The result of polaractivation is similar to the superactivation effect without the necessary preliminary conditions on the quantum channels or on the joint structure. The proposed polaractivation is limited neither by any preliminary conditions on the quantum channel nor on the maps of other channels involved in the joint channel structure and requires only the proposed quantum polar encoding scheme and the multiple uses of the given quantum channel. We have shown that quantum polar coding can help to achieve the polaractivation of private classical capacity of noisy quantum channels in the asymptotic setting, where individually, each channel is so noisy that it cannot transmit any classical information privately.

Acknowledgment

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

References

Arikan, E. (2006), Channel combining and splitting for cutoff rate improvement. IEEE Transactions on Information Theory, 52(2):628–639, arXiv:cs/0508034.

Arikan, E. (2009), Channel polarization: A method for constructing capacity achieving codes for symmetric binary-input memoryless channels. IEEE Transactions on Information Theory, 55(7):3051–3073, arXiv:0807.3917.

Arikan, E. and Telatar, E. (2009a), On the rate of channel polarization. In Proceedings of the 2009 International Symposium on Information Theory, pages 1493–1495, Seoul, Korea, arXiv:0807.3806.

Arikan, E. (2010), Source polarization. In Proceedings of the 2010 IEEE International Symposium on Information Theory, pages 899–903, Austin, Texas, USA, arXiv:1001.3087.

Boileau, J.-C. and Renes, J. M. (2009), Optimal State Merging Without Decoupling, arXiv:0905.1324v1 [quant-ph].

Brandao, F.G.S.L. and Oppenheim, J. (2010), Public Quantum Communication and Superactivation, arXiv:1005.1975.

Brandao, F.G.S.L., Oppenheim, J. and S. Strelchuk (2011), When does noise increase the quantum capacity?, arXiv:1107.4385v1 [quant-ph].

Christandl, M. and Winter, A. (2005), Uncertainty, Monogamy, and Locking of Quantum Correlations, IEEE Trans Inf Theory, vol 51, no 9, pp 3159-3165, arXiv:quant-ph/0501090.

Cubitt, T. and Smith, G. (2009), Super-Duper-Activation of Quantum Zero-Error Capacities, arXiv:0912.2737v1.

Cubitt, T., Chen, J. X. and Harrow, A. (2009), Superactivation of the Asymptotic Zero-Error Classical Capacity of a Quantum Channel, arXiv: 0906.2547.

Devetak, I. (2005), The private classical capacity and quantum capacity of a quantum channel," IEEE Trans. Inf. Theory, vol. 51, pp. 44–55, quant-ph/0304127.

Duan, R. (2009), Superactivation of zero-error capacity of noisy quantum channels.arXiv:0906.2527.

Gyongyosi, L. and Imre, S. (2011), Information Geometric Superactivation of Classical Zero-Error Capacity of Quantum Channels, Progress in Informatics, Quantum Information Technology, Quantum Information Science Theory Group, National Institute of Informatics, Tokyo, Japan, Print ISSN : 1349-8614, Online ISSN : 1349-8606.

Gyongyosi, L. and Imre, S. (2012), Algorithmic Superactivation of Asymptotic Quantum Capacity of Zero-Capacity Quantum Channels, Information Sciences, ELSEVIER, ISSN: 0020-0255.

Gyongyosi, L. and Imre, S. (2012), Long-Distance Quantum Communications with Superactivated Gaussian Optical Quantum Channels, SPIE Optical Engineering, ISSN: 0091-3286, E-ISSN: 1560-2303; USA.

Gyongyosi, L. and Imre, S. (2012), Polaractivation of Zero-Capacity Quantum Channels, Quantum Theory: Reconsideration of Foundations - 6 (QTRF6) Conference, International Centre for Mathematical Modelling in physics, engineering and cognitive sciences (ICMM), Linnaeus University, Växjö, Sweden.

Gyongyosi, L. and Imre, S. (2012), 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), The University of Tokyo, Tokyo, Japan.

Gyongyosi, L. and Imre, S. (2012), 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, (American Physical Society), Anaheim, California, USA.

Hastings, M. (2009), A Counterexample to Additivity of Minimum Output Entropy" Nature Physics 5, 255, arXiv:0809.3972.

Hayashi M. and Nagaoka, H. (2003), "General formulas for capacity of classical-quantum channels," IEEE Transactions on Information Theory, Vol.49, No.7, pp.1753-1768.

Holevo, A. (1998), The capacity of the quantum channel with general signal states", IEEE Trans. Info. Theory 44, 269 - 273.

Hussami, N. Urbanke, R. and Korada, S. B. (2009), Performance of polar codes for channel and source coding. In IEEE International Symposium on Information Theory 2009, pages 1488–1492. IEEE.

Imre, S. and Balazs, F. (2005): *Quantum Computing and Communications – An Engineering Approach*, Published by John Wiley and Sons Ltd.

Imre, S. and Gyongyosi, L. (2012), *Advanced Quantum Communications: An Engineering Approach*, Wiley-IEEE Press.

Imre, S. and Gyongyosi, L. (2012), Quantum-assisted and Quantum-based Solutions in Wireless Systems, with Lajos Hanzo, Harald Haas, Dominic O'Brien and Markus Rupp, in: "Wireless Myths, Realities and Futures: From 3G/4G to Optical and Quantum Wireless", Proceedings of the IEEE, ISSN: 0018-9219.

Korada, S. B, Sasoglu, E. and Urbanke, R. (2010), Polar codes: Characterization of exponent, bounds, and constructions. IEEE Transactions on Information Theory, 56(12):6253–6264.

Koyluoglu, O. O. and El Gamal, H. (2010), Polar Coding for Secure Transmission and Key Agreement. arXiv.org > cs > arXiv:1003.1422v1

Lloyd, S. (1997), Capacity of the noisy quantum channel, Phys. Rev. A, vol. 55, pp. 1613–1622.

Mahdavifar, H. and Vardy, A. (2010), Achieving the Secrecy Capacity of Wiretap Channels Using Polar Codes. arXiv:1001.0210v2 [cs.IT].

Mori, R. and Tanaka, T. (2009), Performance and construction of polar codes on symmetric binary-input memoryless channels. In IEEE International Symposium on Information Theory 2009, pages 1496–1500. IEEE Press.

Renes, J. M., Dupuis, F. and Renner, R. (2011), Efficient Quantum Polar Coding, arXiv:1109.3195v1 [quant-ph].

Sasoglu, E., Telatar, E. and Arıkan, E. (2009), Polarization for arbitrary discrete memoryless channels. In IEEE Information Theory Workshop 2009, pages 144–148. IEEE.

Schumacher, B. and Westmoreland, M. (1997), Sending classical information via noisy quantum channels," Phys. Rev. A, vol. 56, no. 1, pp. 131–138.

Schumacher, B. and Westmoreland, M. (2000), Relative Entropy in Quantum Information Theory 2000, LANL ArXiV e-print quant-ph/0004045, to appear in *Quantum Computation and Quantum Information: A Millenium Volume* , S. Lomonaco, editor (American Mathematical Society Contemporary Mathematics series).

Shor, P. (2002), The quantum channel capacity and coherent information." lecture notes, MSRI Workshop on Quantum Computation, Available online at http://www.msri.org/publications/ln/msri/2002/quantumcrypto/shor/1/.

Smith, G. and Yard, J. (2008), Quantum Communication with Zero-capacity Channels. Science 321, 1812-1815.

Smith, G., Smolin, J. A. and Yard, J. (2011), Gaussian bosonic synergy: quantum communication via realistic channels of zero quantum capacity.

Wilde, M. M. and Renes, J. (2012), "Polar codes for private classical communication", arXiv:1203.5794.

Wilde, M. M. and Guha. S. (2011), Polar codes for classical-quantum channels. arXiv:1109.2591v1 [quant-ph].

Wilde, M. M. and Renes, J. (2012), Quantum polar codes for arbitrary channels, arXiv:1201.2906v1 [quant-ph].