12-1-2012

Performance of polar codes for quantum and private classical communication

Zachary Dutton
BBN Technologies

Saikat Guha
BBN Technologies

Mark M. Wilde
Université McGill

Recommended Citation

Dutton, Z., Guha, S., & Wilde, M. (2012). Performance of polar codes for quantum and private classical communication. *2012 50th Annual Allerton Conference on Communication, Control, and Computing, Allerton 2012*, 572-579. https://doi.org/10.1109/Allerton.2012.6483269

Performance of polar codes for quantum and private classical communication

Zachary Dutton and Saikat Guha
Raytheon BBN Technologies,
Cambridge, Massachusetts, USA 02138

Mark M. Wilde
School of Computer Science, McGill University
Montreal, Quebec, Canada

***Abstract*—We analyze the practical performance of quantum polar codes, by computing rigorous bounds on block error probability and by numerically simulating them. We evaluate our bounds for quantum erasure channels with coding block lengths between 2^{10} and 2^{20}, and we report the results of simulations for quantum erasure channels, quantum depolarizing channels, and "BB84" channels with coding block lengths up to $N = 1024$. For quantum erasure channels, we observe that high quantum data rates can be achieved for block error rates $P_e \leq 10^{-4}$ and that somewhat lower quantum data rates can be achieved for quantum depolarizing and BB84 channels. Our results here also serve as bounds for and simulations of private classical data transmission over these channels, essentially due to Renes' duality bounds for privacy amplification and classical data transmission of complementary observables. Future work might be able to improve upon our numerical results for quantum depolarizing and BB84 channels by employing a polar coding rule other than the heuristic used here.**

Arikan's polar codes are an important recent development in coding theory [1]. These codes provably achieve the Shannon capacity of symmetric binary-input memoryless channels and have an $O(N \log N)$ complexity for both encoding and decoding, where N is the number of channel uses. Polar codes exploit the channel polarization effect, in which a particular recursive encoding induces a set of virtual channels, such that some of the virtual channels are near perfect for data transmission and the others are near useless for this task. The fraction of the virtual channels that are near perfect is equal to the symmetric capacity of the original channel.

Several authors have now extended the ideas of Arikan to the domain of quantum information theory, in order to accomplish a variety of information processing tasks, including classical data transmission [2], [3], private classical data transmission [4], [5], and quantum data transmission [6], [4], [7]. Among these works, Ref. [6] demonstrated that all of the above impressive features of classical polar codes are preserved when constructing quantum polar codes for sending quantum data over quantum Pauli channels or quantum erasure channels. Refs. [4], [5] then followed up with similar results for private classical data transmission over these channels. The importance of Pauli channels stems from the fact that any noisy qubit channel can be "twirled" to a Pauli channel with a quantum capacity not higher than the original channel. A quantum depolarizing channel is a Pauli channel that is often used as a "worst-case scenario" noise model, and a quantum erasure channel is a simplified model of photon loss.

In light of the above theoretical works, it seems natural now to assess the practical performance of finite-blocklength quantum polar codes on any of the aforementioned channels. One could get a better idea of this by deriving rigorous bounds on performance like Arikan's bounds for classical erasure channels [1], and another way to do so is simply by simulating their performance numerically. Indeed, since the quantum decoder for Pauli and erasure channels is a coherent version of Arikan's successive cancellation decoder combined with other efficient operations [6], it is possible to have an efficient numerical simulation of these codes' performance.

In this paper, we derive bounds on the performance of quantum polar codes on quantum erasure channels, and we report the results of numerical simulations determining the performance of quantum polar codes on quantum erasure, depolarizing, and BB84 channels. In our numerical simulations, we consider the performance of quantum successive cancellation decoding for block lengths of 64, 256, and 1024. We find that with these moderate block lengths, relatively large rates can be achieved on the quantum erasure channel with a block error rate $P_e \leq 10^{-4}$. For the depolarizing and BB84 channels, we compare our results against the well-known hashing bound for quantum data transmission. For these channels, we discuss how our results serve equally as simulations of polar codes for private classical data transmission.

We structure this paper as follows. To start, Sections I, II and III review some of the recent advances in polar coding for quantum channels [2], [6], [4], [7], [5], [3], focusing on the approaches given in Refs. [2], [7], [5]. Section IV derives our bounds on quantum polar code performance for quantum erasure channels. We then detail the results of our numerical simulations in Section V. In Section VI, we discuss how our results apply in the setting of private classical communication, and we finally conclude in Section VII.

I. Polar codes for classical communication

Consider a channel W with a classical input $x \in \{0, 1\}$ and a quantum output ρ_x:

$$W : x \to \rho_x. \tag{1}$$

Such a channel is known as a classical-quantum or cq channel for short. Two parameters that characterize the performance of this channel for transmitting classical data are the fidelity

$F(W) \equiv \left\| \sqrt{\rho_0}\sqrt{\rho_1} \right\|_1^2$ and the symmetric Holevo information $I(W) \equiv H((\rho_0+\rho_1)/2) - [H(\rho_0)+H(\rho_1)]/2$, where $H(\sigma) \equiv -\text{Tr}\{\sigma \log_2 \sigma\}$ is the von Neumann entropy. A channel is near perfect for transmitting classical data if $I(W) \approx 1$ and $F(W) \approx 0$, and it is nearly useless for this task if $I(W) \approx 0$ and $F(W) \approx 1$ (Ref. [2] gives a precise relationship between these channel parameters).

When encoding classical information for the channel W, we consider $N = 2^n$ uses of it, so that the resulting channel is of the form: $x^N = x_1 \cdots x_N \to \rho_{x^N} \equiv \rho_{x_1} \otimes \cdots \otimes \rho_{x_N}$, where x^N is the classical input sequence and ρ_{x^N} is the output quantum state. Arikan's idea of channel combining and splitting extends to this case by considering his encoding matrix G_N [1] acting on an input sequence u^N: $u^N \to \rho_{u^N G_N}$, where $u^N G_N$ is the binary vector resulting from multiplication of the row vector u^N by Arikan's encoding matrix G_N. We can then define the "split" channels $W_N^{(i)}$ from the above "combined" channels as follows:

$$W_N^{(i)} : u_i \to \rho_{(i),u_i}^{U_1^{i-1}B^N}, \tag{2}$$

$$\rho_{(i),u_i}^{U_1^{i-1}B^N} \equiv \sum_{u_1^{i-1}} \frac{1}{2^{i-1}} \left|u_1^{i-1}\right\rangle \left\langle u_1^{i-1}\right|^{U_1^{i-1}} \otimes \overline{\rho}_{u_1^i}^{B^N}, \tag{3}$$

$$\overline{\rho}_{u_1^i}^{B^N} \equiv \sum_{u_{i+1}^N} \frac{1}{2^{N-i}} \rho_{u^N G_N}^{B^N}. \tag{4}$$

The interpretation of this channel is that it is the one "seen" by the bit u_i if all of the previous bits u_1^{i-1} are available and if we consider all the future bits u_{i+1}^N as randomized. This motivates the development of a quantum successive cancellation decoder [2] that attempts to distinguish $u_i = 0$ from $u_i = 1$ by adaptively exploiting the results of previous measurements and quantum hypothesis tests for each bit decision.

The above synthesized channels polarize, in the sense that some become near perfect for classical data transmission while the others become near useless. This result follows in the quantum case by a martingale argument similar to Arikan's: model the channel splitting and combining as a random birth process, and it is possible to prove that the parameters $I(W_N^{(i)})$ and $F(W_N^{(i)})$ converge almost surely to zero-one valued random variables in the limit of many recursions of the encoding. The following theorem characterizes the rate with which the channel polarization effect takes hold [8], [2]:

Theorem 1: Given a binary input cq channel W and any $\beta < 1/2$, it holds that $\lim_{n\to\infty} \Pr_I\{\sqrt{F(W_{2^n}^{(I)})} < 2^{-2^{n\beta}}\} = I(W)$, where n indicates the level of recursion for the encoding, $W_{2^n}^{(I)}$ is a random variable characterizing the I^{th} split channel, and $F(W_{2^n}^{(I)})$ is the fidelity of that channel.

Suppose now that we can determine which channels are the good ones and which ones are bad. In this case, we can construct a polar coding scheme by dividing the synthesized channels according to the following polar coding rule:

$$\mathcal{G}_N(W,\beta) \equiv \left\{i \in [N] : \sqrt{F(W_N^{(i)})} < 2^{-N^\beta}\right\}, \tag{5}$$

and $\mathcal{B}_N(W,\beta) \equiv [N] \setminus \mathcal{G}_N(W,\beta)$, so that $\mathcal{G}_N(W,\beta)$ is the set of "good" channels and $\mathcal{B}_N(W,\beta)$ is the set of "bad" channels. The sender then transmits the information bits through the good channels and "frozen" bits through the bad ones. A helpful assumption for error analysis is that the frozen bits are chosen uniformly at random such that the sender and receiver both have access to these frozen bits. Ref. [2] provided an explicit construction of a quantum successive cancellation decoder that has an error probability equal to $o(2^{-(1/2)N^\beta})$—let $\{\Lambda_{u_\mathcal{A}}^{(u_{\mathcal{A}^c})}\}$ denote the corresponding decoding positive operator-valued measure (POVM), with $u_\mathcal{A}$ the information bits and $u_{\mathcal{A}^c}$ the frozen bits.

II. Polar codes for quantum communication

Wilde and Renes recently showed how to construct quantum polar codes for sending quantum data over an arbitrary qubit-input quantum channel [7] (before this, Renes *et al*. addressed the case of Pauli channels [6]). The polar coding scheme in Ref. [7] follows the general approach of Renes and Boileau [9], in which they showed how to build up quantum codes from classical codes for two different cq channels induced by the quantum channel of interest. We briefly overview the approach given in Ref. [7].

Suppose that a quantum channel $\mathcal{N}$ connects a sender to a receiver. Consider that the sender can induce a cq "amplitude-basis" channel W_A from $\mathcal{N}$ by inputting a computational basis state $|z\rangle$ depending on some classical bit z:

$$W_A : z \to \mathcal{N}(|z\rangle\langle z|). \tag{6}$$

Since the induced channel W_A is of the form in (1), it is possible to construct a polar code for it of rate $I(W_A)$, consisting of the classical encoding G_N and a corresponding quantum successive cancellation decoder as described in the previous section. Now suppose that Alice shares a maximally entangled state $|\Phi\rangle$ with Bob, where

$$|\Phi\rangle \equiv 2^{-1/2} \sum_{z\in\{0,1\}} |z\rangle|z\rangle.$$

Alice can modulate her share of this state with Z^x depending on some bit x, so that the global state for Alice and Bob becomes $2^{-1/2}(|0\rangle|0\rangle + (-1)^x|1\rangle|1\rangle)$. If Alice sends her share of the state through the channel, this process induces a cq "phase-basis" channel W_P of the following form:

$$W_P : x \to (\mathcal{N}\otimes I)(Z^x|\Phi\rangle\langle\Phi|Z^x). \tag{7}$$

It is also possible to construct a polar code for W_P of rate $I(W_P)$, again consisting of the classical encoding G_N and a quantum successive cancellation decoder.

The insight of Refs. [6], [7] is to build up a quantum polar code from the polar codes for the above two channels. The sender and receiver can compute offline which channel inputs will be good or bad for the amplitude and phase channels. The sender then inputs the following types of qubits into the different encoder inputs:

1) Information qubits into the synthesized channels that are good in both amplitude and phase.
2) Ancilla qubits in the state $|0\rangle$ into the synthesized channels that are bad in amplitude and good in phase.

3) Ancilla qubits in the state $|+\rangle \equiv 2^{-1/2}(|0\rangle + |1\rangle)$ into the synthesized channels that are good in amplitude and bad in phase.
4) Shares of ebits in the state $|\Phi\rangle$ into the synthesized channels that are bad in both amplitude and phase.

The intuition behind this approach is that the receiver should be able to recover quantum data if it is possible to recover classical data encoded into complementary variables. Thus, the sender puts information qubits into the synthesized channels which are good for both bases. The receiver will need help in the decoding process in the form of frozen ancilla qubits for the synthesized channels which are bad in one of the bases (this is the same as in Arikan's classical polar coding scheme [1], with the exception that the ancillas should be frozen in the basis that is bad). Finally, if both bases are bad, a shared ebit is in some sense frozen in both bases, because Bob can always predict the outcome of a Pauli X or Z measurement that Alice performs on her end if she tells him which measurement she performs.

The net rate of this quantum polar coding scheme (rate of quantum communication minus the rate of entanglement consumption) is equal to the symmetric coherent information rate [7], [6]:

$$\begin{aligned} I(W_A) + I(W_P) - 1 &= I(A\rangle B)_{\mathcal{N}(\Phi)} \\ &\equiv H(B)_{\mathcal{N}(\Phi)} - H(AB)_{\mathcal{N}(\Phi)}. \end{aligned}$$

The polar code operates as follows (see Ref. [7] for a detailed discussion of the operation). Alice sends qubits as described above into a coherent version of Arikan's encoder (this just consists of quantum CNOT gates). Bob then exploits a coherent version of the quantum successive cancellation decoder for the amplitude cq channel in order to coherently decode the information qubits, placing them in a register C^N. Bob sends the coherently decoded information qubits through the inverse of the coherent polar encoder. This process induces the phase channel in (7) from the point of view of the phase basis of the qubits at the input of the encoder. Bob then acts with a coherent version of the quantum successive cancellation decoder for the phase channels, coherently placing the outcomes in a register D^N. Finally, he performs a linear number of CNOT gates from the C^N registers to the D^N registers. The result is that he will have decoded the information qubits with a fidelity that is lower bounded by $1 - 2\sqrt{\epsilon_A} - 2\sqrt{\epsilon_P}$, where ϵ_A and ϵ_P are the error probabilities of the respective polar codes for the cq amplitude and phase channels.

The polar encoder is efficient because it is the same network of CNOT gates in Arikan's encoder (this part requires only $O(N \log N)$ operations). For general channels, it is still an open question to determine if the polar decoder has an efficient implementation. For Pauli channels or erasure channels, Renes *et al*. showed that the polar decoder has an efficient implementation with $O(N \log N)$ operations [6], essentially because the induced cq amplitude and phase channels are classical and they could thus exploit coherent versions of Arikan's efficient polar decoder in the quantum polar decoder.

III. Polar codes for private communication

An approach similar to the one above gives polar codes for sending classical data privately over a quantum wiretap channel [5]. Again, this approach follows the general approach of Renes and Boileau [9] for transmitting private classical data, in which we build up such a protocol by considering two induced cq channels for complementary variables. A quantum wiretap channel $\mathcal{N}^{A\to BE}$ has an input system A for the sender, an output system B for the legitimate receiver, and an output system E for the wiretapper. The goal in this setting is for the sender to transmit classical data to the legitimate receiver in such a way that the wiretapper obtains a negligible amount of information about the input data.

We now review the private polar coding protocol from Ref. [5]. The first cq channel $\mathcal{M}_A$ that we consider has Alice prepare a quantum state ρ_z depending upon a bit z and feed this state into the quantum wiretap channel $\mathcal{N}$:

$$\mathcal{M}_A : z \to \mathcal{N}^{A\to B}(\rho_z). \tag{8}$$

By purifying the input state ρ_z^A to $|\psi_z\rangle^{AS_1}$ and the quantum wiretap channel $\mathcal{N}^{A\to BE}$ to the isometric map $U_{\mathcal{N}}^{A\to BES_2}$ (where S_1 and S_2 are "shield" systems not possessed by the wiretapper [10], [11]), we can see that the above channel arises by tracing over the wiretapper's system E and the shield systems S_1S_2:

$$z \to |\psi_z\rangle^{BES_1S_2} \equiv U_{\mathcal{N}}^{A\to BES_2} |\psi_z\rangle^{AS_1}.$$

The channel in (8) is a cq channel, and as such, we can construct a polar code for it with rate $I(\mathcal{M}_A)$ along with an encoder and quantum successive cancellation decoder [2].

The other cq channel that we consider is in some sense a virtual channel because we only make use of it in order to reason about the security of our private polar coding protocol (we do not actually exploit a decoder for it in the operation of our protocol). This channel is a phase channel with quantum side information. Suppose that Alice possesses an entangled state of the following form:

$$|\varphi\rangle^{CAS_1} \equiv 2^{-1/2} \sum_z |z\rangle^C |\psi_z\rangle^{AS_1}.$$

Alice could then modulate the C system of the above state by applying the phase operator Z^x to it, depending on some input bit x. Suppose then that she is able to transmit the A system through the channel $\mathcal{N}^{A\to B}$ to Bob and the C and S_1 systems through an identity channel. The resulting cq phase channel to Bob is as follows:

$$\mathcal{M}_P : x \to \mathcal{N}^{A\to B}((Z^x)^C |\varphi\rangle \langle\varphi|^{CAS_1} (Z^x)^C). \tag{9}$$

Although we stated that this is a virtual channel, it is possible in principle to construct a polar code for it with rate $I(\mathcal{M}_P)$ along with a quantum successive cancellation decoder [2].

The usefulness of the phase channels for privacy may not be readily apparent, but an uncertainty relation from Ref. [9] clarifies the link. Indeed, consider the following channel to the wiretapper:

$$\mathcal{M}_E : z \to \mathcal{N}^{A\to E}(\rho_z). \tag{10}$$

The uncertainty relation (Lemma 2 of Ref. [9]) for our case is as follows:

$$I(\mathcal{M}_P) + I(\mathcal{M}_E) = 1. \tag{11}$$

The implication of this uncertainty relation is that if the phase channel $\mathcal{M}_P$ to Bob is nearly perfect, then the amplitude channel $\mathcal{M}_E$ is nearly useless to the wiretapper and vice versa.

We can then exploit the above uncertainty relation to construct a polar code for private communication. The structure is similar to that in the previous section, though the resources used are in some sense classical versions of the quantum resources. The sender and receiver compute offline which channel inputs will be good or bad for the amplitude or phase channels in (8) and (9), respectively. The sender then inputs the following types of qubits into the different encoder inputs:

1) Information bits to be kept private into the synthesized channels that are good in both amplitude and phase.
2) Ancilla bits initialized to 0 into the synthesized channels that are bad in amplitude and good in phase.
3) Ancilla bits that are randomized (0 or 1 with probability $1/2$) into the synthesized channels that are good in amplitude and bad in phase.
4) Shares of secret key bits (0 or 1 with probability $1/2$ and known to both Alice and Bob) into the synthesized channels that are bad in both amplitude and phase.

The security of this approach follows from the uncertainty relation in (11). If Alice places the information bits into the synthesized channels that are good in amplitude and phase, then Bob will be able to recover them reliably since the channels are good in amplitude and Eve learns only a negligible amount of information about them due to the uncertainty relation in (11) and the fact that the channels are good in phase for Bob. The sender places ancilla bits set to 0 in the channels that are bad in amplitude and good in phase in order to help Bob in decoding the information bits. She places randomized bits into the channels that are good in amplitude and bad in phase in order randomize Eve's knowledge of them. Finally, she places secret key bits into the channels that are bad for both variables in order to help Bob decode and to randomize Eve's knowledge of the information bits.

The net rate of this private polar coding scheme (rate of private classical communication minus the rate of secret key consumption) is equal to the symmetric private information rate [5], [9]:

$$I(\mathcal{M}_A) + I(\mathcal{M}_P) - 1 = I(\mathcal{M}_A) - I(\mathcal{M}_E).$$

We can estimate the reliability and security of this scheme by considering the performance of the constituent cq polar codes.

IV. Rigorous Bounds on Performance for the Quantum Erasure Channel

We now arrive at our first result, where we provide rigorous bounds on the performance of quantum polar codes on the quantum erasure channel. Our development here is both similar to and extends that in Section V-D of Arikan [1]. Recall that a quantum erasure channel takes a qubit in the state ρ as input and outputs this state with probability $1-\epsilon$ or an orthogonal erasure flag $|e\rangle$ with the complementary probability:

$$\rho \to (1-\epsilon)\rho + \epsilon |e\rangle\langle e|. \tag{12}$$

First, consider that in any given "run" of a quantum polar code of the form reviewed in Section II, the block error probability P_e is as follows:

$$P_e \equiv \Pr\{\alpha_{\text{err}}\} + \Pr\{\phi_{\text{err}}\} - \Pr\{\alpha_{\text{err}}, \phi_{\text{err}}\}, \tag{13}$$

where α_{err} and ϕ_{err} are the events that an error occurs during the decoding of the induced amplitude and phase channel, respectively. (The above formula ensures that we count a quantum block error when either an amplitude or phase error occurs, but that we do not overcount when both errors occur.) By exploiting the law of total probability (that $\Pr\{\phi_{\text{err}}\} = \Pr\{\alpha_{\text{err}}, \phi_{\text{err}}\} + \Pr\{\overline{\alpha_{\text{err}}}, \phi_{\text{err}}\}$, where $\overline{\alpha_{\text{err}}}$ is the event that there is no amplitude decoding error), we have that

$$\begin{aligned} P_e &= \Pr\{\alpha_{\text{err}}\} + \Pr\{\overline{\alpha_{\text{err}}}, \phi_{\text{err}}\} \\ &= \Pr\{\alpha_{\text{err}}\} + \Pr\{\phi_{\text{err}} \mid \overline{\alpha_{\text{err}}}\} \Pr\{\overline{\alpha_{\text{err}}}\} \\ &= \Pr\{\alpha_{\text{err}}\} + \Pr\{\phi_{\text{err}} \mid \overline{\alpha_{\text{err}}}\} [1 - \Pr\{\alpha_{\text{err}}\}] \\ &= \Pr\{\alpha_{\text{err}}\} + \Pr\{\phi_{\text{err}} \mid \overline{\alpha_{\text{err}}}\} - \Pr\{\phi_{\text{err}} \mid \overline{\alpha_{\text{err}}}\} \Pr\{\alpha_{\text{err}}\}. \end{aligned}$$

When considering performance for the quantum erasure channel, there is a symmetry that is helpful in simplifying the above expression. Consider that both the induced amplitude and phase channels for the quantum erasure channel in (12) are classical erasure channels with erasure probability ϵ. Let $W_N^{(i)}$ be the i^{th} synthesized channel from the classical erasure channel, η a threshold parameter between 0 and 1, and $\mathcal{A}(\eta)$ the set of information bits chosen by Arikan's polar coding rule: $\mathcal{A}(\eta) \equiv \{i : Z(W_N^{(i)}) \leq \eta\}$, with Z the Bhattacharya parameter. Recall that the order of these indices i is preserved for the induced amplitude channels but reversed for the induced phase channels. If we assume that η is the same for both the induced amplitude and phase channels, then it follows that

$$\Pr\{\alpha_{\text{err}}\} = \Pr\{\phi_{\text{err}} \mid \overline{\alpha_{\text{err}}}\}.$$

This assumption is reasonable because both of the induced channels are erasure channels with the same erasure probability. By exploiting the above symmetry, we have that

$$P_e = \Pr\{\alpha_{\text{err}}\} (2 - \Pr\{\alpha_{\text{err}}\}).$$

Thus, in order to bound the block error probability P_e from both above and below, we only need to bound $\Pr\{\alpha_{\text{err}}\}$ from above and below. In order to do so, we can exploit the following upper bound from Section V-B of Arikan [1]:

$$\Pr\{\alpha_{\text{err}}\} \leq U(\eta) \equiv \sum_{i \in \mathcal{A}(\eta)} Z(W_N^{(i)}).$$

Then by using Arikan's recursive equations for the erasure channel in (38) of Ref. [1], we can easily compute this upper bound on $\Pr\{\alpha_{\text{err}}\}$.

For a rigorous lower bound on $\Pr\{\alpha_{\text{err}}\}$, we appeal to arguments similar to those in Section V of Ref. [2], since

one can always embed classical systems into quantum systems (also, recall that Arikan only provided a heuristic lower bound in Section V-D of Ref. [1]). We can write the error probability $\Pr\{\alpha_{\text{err}}\}$ as follows:

$$\frac{1}{2^N}\sum_{u^N}\left(1-\text{Tr}\left\{\Pi^{B^N}_{(N),u_1^{N-1}u_N}\cdots\Pi^{B^N}_{(i),u_1^{i-1}u_i}\cdots\Pi^{B^N}_{(1),u_1}\right.\right.$$
$$\left.\left.\rho_{u^N}\;\Pi^{B^N}_{(1),u_1}\cdots\Pi^{B^N}_{(i),u_1^{i-1}u_i}\cdots\Pi^{B^N}_{(N),u_1^{N-1}u_N}\right\}\right), \quad (14)$$

where ρ_{u^N} is the encoded state and $\Pi^{B^N}_{(1),u_1},\ldots,\Pi^{B^N}_{(N),u_1^{N-1}u_N}$ are projectors corresponding to quantum hypothesis tests to decode each bit u_i. In the classical case, ρ_{u^N} is just a distribution given by the encoding and channel and $\Pi^{B^N}_{(1),u_1}$, $\ldots$, $\Pi^{B^N}_{(N),u_1^{N-1}u_N}$ are indicator functions corresponding to likelihood ratio tests. Consider the following operator inequalities which hold for commuting operators P_1 and P_2 such that $0\leq P_1,P_2\leq I$:

$$I-P_1P_2P_1\geq I-P_1,$$
$$I-P_1P_2P_1\geq I-P_2.$$

We can exploit these recursively in order to obtain the following lower bound on the error term in (14), since the projectors $\Pi^{B^N}_{(1),u_1},\ldots,\Pi^{B^N}_{(N),u_1^{N-1}u_N}$ all commute for a classical erasure channel:

$$\sum_{u_1^{i-1}}\frac{1}{2^{i-1}}\sum_{u_i}\frac{1}{2}\text{Tr}\left\{\left(I-\Pi^{B^N}_{(i),u_1^{i-1}u_i}\right)\sum_{u_{i+1}^N}\frac{1}{2^{N-i}}\rho_{u^N}\right\}$$
$$=\sum_{u_i}\frac{1}{2}\text{Tr}\left\{\left(I-\Pi^{U_1^{i-1}B^N}_{(i),u_i}\right)\rho^{U_1^{i-1}B^N}_{(i),u_i}\right\}\equiv P_{\text{err}}(u_i),$$

where in the last line we have exploited the states and notation defined in Section V of Ref. [2]. By recognizing that the quantity above is equivalent to the error in discriminating the states $\rho^{U_1^{i-1}B^N}_{(i),0}$ and $\rho^{U_1^{i-1}B^N}_{(i),1}$ in a quantum hypothesis test and recalling the relationship between hypothesis testing error, the trace distance, and the fidelity (Bhattacharya parameter), we have the following lower bound from Ref. [12]:

$$P_{\text{err}}(u_i)\geq\frac{1}{2}\left(1-\sqrt{1-Z(W_N^{(i)})^2}\right).$$

Thus, since this bound holds for any index i, we obtain the following lower bound on $\Pr\{\alpha_{\text{err}}\}$ for the quantum erasure channel:

$$\Pr\{\alpha_{\text{err}}\}\geq L(\eta)\equiv\max_{i\in\mathcal{A}(\eta)}\frac{1}{2}\left(1-\sqrt{1-Z(W_N^{(i)})^2}\right).$$

This bound is also easy to compute by exploiting Arikan's recursive equations for the erasure channel in (38) of Ref. [1].

The above development then leads us to the following theorem:

Theorem 2: The block error probability P_e for a quantum polar code of the form reviewed in Section II when used on a quantum erasure channel is bounded as follows:

$$L(\eta)(2-U(\eta))\leq P_e\leq U(\eta)(2-L(\eta)).$$

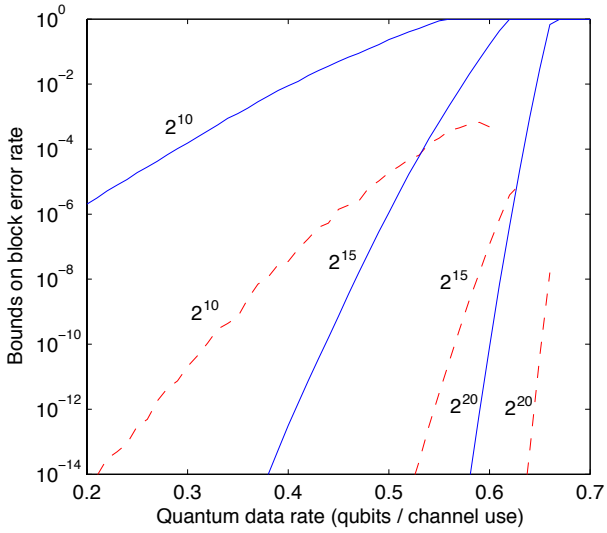

Fig. 1. The figure depicts the upper (blue solid curves) and lower (red dashed curves) bounds from Theorem 2 for a quantum erasure channel with erasure probability $\epsilon=0.15$. These bounds determine the trade-off between block error probability and rate for quantum polar codes designed for a quantum erasure channel. The channel's quantum capacity is equal to $1-2\epsilon=0.7$ qubits per channel use. Next to each curve, we also show the block length for a quantum polar code to which the corresponding bound applies.

Figure 1 depicts the bounds given by Theorem 2. What we observe is that a large block length $\approx 2^{20}$ is required in order for a quantum polar code to operate in a regime near the quantum capacity. Also, the margins between the upper and lower bounds from Theorem 2 are rather large. Thus, it is clear that numerical simulations would be helpful in determining more accurate estimates of the performance of quantum polar codes on the quantum erasure channel.

V. Numerical Simulation Results

We now describe the results of our numerical simulations of quantum polar codes on quantum erasure, depolarizing, and BB84 channels. Our simulations rely on two observations from Ref. [6] (and noted in the previous section):

- The cq channels in (6) and (7) corresponding to the respective induced phase and amplitude channels result in distinguishable states at the output (for erasure, depolarizing, and BB84 channels).
- The performance of the resulting quantum polar code is directly related to the performance of polar codes for the constituent amplitude and phase channels.

The first observation implies that the induced channels are effectively classical. Specifically, for the quantum erasure channel with erasure probability ϵ, both the induced amplitude and phase channel correspond to a classical erasure channel with erasure probability ϵ. The second observation implies that we can simulate the performance of a quantum polar code for Pauli or erasure channels by simulating the performance of Arikan's successive cancellation decoder for the constituent

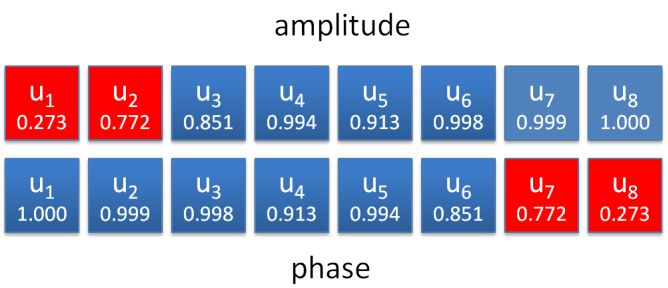

Fig. 2. Diagram of the information bits for the induced amplitude and phase channels for code length $N = 8$ and a classical rate $R_C = 0.75$. The numbers represent the symmetric capacities for each virtual channel when $\epsilon = 0.15$. The blue boxes represent the 'good' channels, which for our example are the virtual channels with symmetric capacities above the lowest quartile. The quantum code then chooses the four bits which are good for both amplitude and phase, resulting in a rate $R_Q = 0.5$ quantum polar code.

channels. Importantly, this simulation is efficient because Arikan's successive cancellation decoder is efficient, requiring only $O(N \log N)$ operations.

Our Monte Carlo simulation proceeds by randomly generating information bits, encoding them with the polar encoder, transmitting them over a given channel, and then decoding with the successive cancellation decoder. In our simulations, we vary the choice of the classical rates $R_C^{(\text{ph})}$ and $R_C^{(\text{amp})}$ for the respective phase and amplitude channels. For the case of the quantum erasure channel, it is optimal to choose these rates to be equal because the two induced amplitude and phase channels are classical erasure channels with the same erasure probability and hence have the same capacity.

Figure 2 depicts the process by which we choose an example quantum polar code with $N = 8$ and classical rates $R_C^{(\text{amp})} = R_C^{(\text{ph})} = 0.75$. The virtual channels' symmetric capacities in the erasure case can be calculated explicitly and efficiently via the recursive formulas in (38) of Ref. [1]. The reason that the symmetric capacities are reversed for the induced phase channel is that the action of the quantum CNOT gates in the encoding are reversed when acting on the phase basis (as first observed in [6]). We end up with four channels "good" for both amplitude and phase and $R_Q = 4/8 = 0.5$. In the case where the bad virtual channels are completely clustered at the ends, it holds that $R_Q = R_C^{(\text{ph})} + R_C^{(\text{amp})} - 1$. However, we note that the symmetric capacities of the virtual channels are generally not ordered sequentially (*e.g.*, u_5 has a larger symmetric capacity than u_4) and in larger block lengths N, the good virtual channels become distributed more non-contiguously, resulting in slightly higher quantum rates.

After randomly choosing the information bits u_1^N, the encoding is performed by multiplying by the encoding matrix G_N [1], and the codeword is transmitted through the channel according to its probability transition matrix. For the amplitude channels, we then sequentially decode u_1, u_2, $\cdots$. We always decode any frozen bits correctly, and we decode the information bits to be either '0' or '1' according to the likelihood ratio, which for each bit is calculated recursively in $O(\log N)$ steps by incorporating the values of previously decoded bits

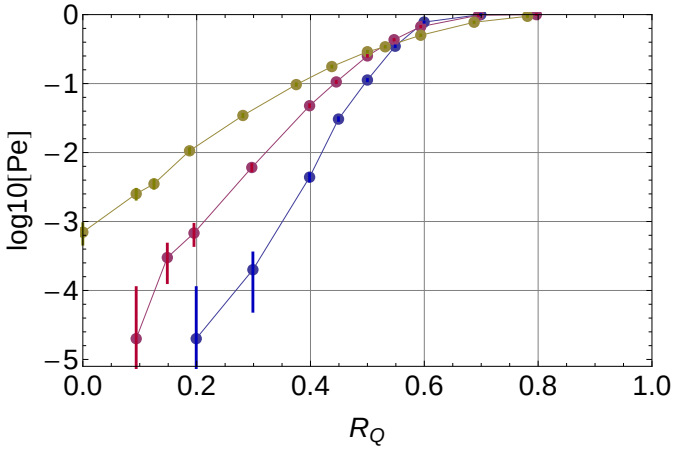

Fig. 3. Block error rate P_e versus quantum data rate for a quantum erasure channel with $\epsilon = 0.15$ and different block lengths. Yellow, red and blue points show, respectively, $N = 64$, 256, and 1024. Points show simulated results and lines are linear interpolations between points. The error bars here and in subsequent figures reflect the 90% confidence interval for the error rates given the number of simulations performed and errors observed. The quantum capacity of this channel is equal to 0.7 qubits per channel use.

[1]. For the induced phase channels, we decode in the reverse order, due to the reversal mentioned above.

We calculated the block error rates $\Pr\{\alpha_{\text{err}}\}$ and $\Pr\{\phi_{\text{err}} \mid \overline{\alpha_{\text{err}}}\}$ for the respective induced amplitude and phase channels separately by performing M such simulations of each, in each case comparing with the actual encoded word. The block error rate for quantum data transmission is equal to (13) by counting an error whenever either the amplitude or phase decoding fails (but not overcounting when both fail). For most cases, we ran $M = 50,000$ simulations in order to get statistically significant results down to $P_e \leq 10^{-4}$ (though for some larger P_e cases we ran $M = 5,000$, as this was more than sufficient to obtain small statisical error bars).

A. *Results for Quantum Erasure Channels*

Figure 3 depicts the block error rate versus quantum data rate for three different code lengths $N = 64$, 256, and 1024. All of the block error rates start to bend down slightly below the quantum capacity for the channel (which in this case is equal to 0.7 qubits per channel use), and the longer block lengths improve more rapidly at lower rates. Figure 4(a) then plots the block error rate versus erasure probability ϵ for one particular quantum data rate $R_Q \approx 0.4$. Note that the exact rates for different block lengths N are slightly different due to a slightly increasing fraction of overlapping phase-good and amplitude-good channels at larger block lengths.

Figure 4(b) summarizes performance for a variety of erasure probabilities ϵ and quantum data rates R_Q by plotting the threshold rate at which $P_e \leq 10^{-4}$. It also plots the quantum capacity $1 - 2\epsilon$ of the quantum erasure channel [13]. We observe that for the selected block lengths, quantum polar codes can perform increasingly near to capacity as the erasure probability ϵ decreases.

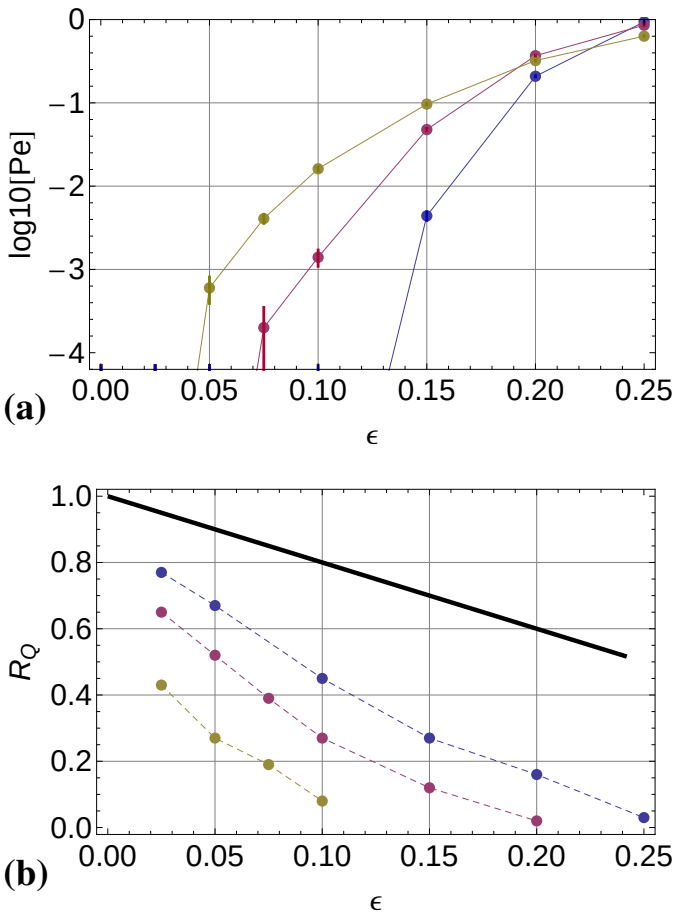

Fig. 4. Quantum erasure channel simulation results. **(a)** Block error rate P_e versus erasure probability ϵ for $N = 64$ (yellow), $N = 256$ (red), and $N = 1024$ (blue) and quantum rate $R_Q = 0.398$ (the $N = 64$ points were for $R_Q = 0.375$). **(b)** Threshold quantum data rate R_Q for block error rate $P_e \leq 10^{-4}$ versus erasure probability ϵ. The black curve shows the quantum capacity $1 - 2\epsilon$.

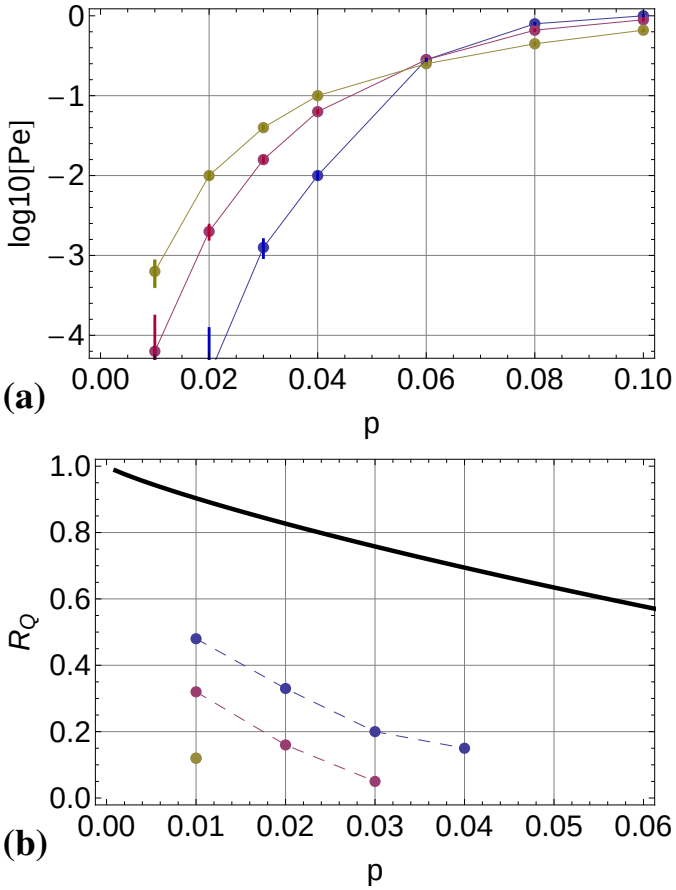

Fig. 5. Quantum depolarizing channel simulation results. **(a)** Block error rate P_e versus physical error probability p for $N = 64$ (yellow), $N = 256$ (red), and $N = 1024$ (blue) and quantum data rate $R_Q = 0.30$. **(b)** Threshold R_Q for $P_e \leq 10^{-4}$ versus p. The black curve shows the hashing limit $1 - H_2(p) - p\log_2(3)$.

B. Results for Quantum Depolarizing Channels

We also simulated the performance of quantum polar codes for the quantum depolarizing channel with depolarizing probability p, modeled as follows:

$$\rho \to (1-p)\rho + p/3\,(X\rho X + Y\rho Y + Z\rho Z).$$

In this case, the induced amplitude channel has orthogonal outputs, with errors occuring only in the case of an X or Y flip. Thus, it is equivalent to a classical binary symmetric channel (BSC) with flip probability $2p/3$. The induced phase channel has four possible outputs (corresponding to the four orthogonal Bell states), and it is thus equivalent to a classical channel with the following probability transition matrix:

$$\begin{pmatrix} 1-p & p/3 & p/3 & p/3 \\ p/3 & p/3 & p/3 & 1-p \end{pmatrix}.$$

One important subtlety for both the induced amplitude and phase channel for the quantum depolarizing channel is that there is no explicit method for calculating the symmetric capacities of each virtual channel (as in the case of an erasure channel). From Ref. [1], we know that there is a choice of good channels with exponentially decreasing error probability for any rate below capacity, but Ref. [1] does not give an explicit prescription for choosing them. One strategy from Ref. [14], which we employ here, is to calculate the symmetric capacity S of a channel and use an effective erasure probability $\epsilon = 1 - S$ to choose the good channels according the prescription for erasure channels. It is not fully known how close to optimal this heuristic is.

Another important subtlety is that the induced amplitude and phase channels have different symmetric capacities (with the phase channel's being slightly larger). For this reason, it is better to choose the amplitude classical rate slightly lower than the phase rate: $R_C^{(\text{amp})} < R_C^{(\text{ph})}$. To account for this, we varied the rates $R_C^{(\text{amp})}$ and $R_C^{(\text{ph})}$ independently and chose the combination of these two rates which optimized P_e for a given quantum data rate R_Q. We found empirically that choosing $R_C^{(\text{amp})} = 0.82 R_C^{(\text{ph})}$ gave near optimal results across the channel parameters and rates we considered but varying around this choice gives slight improvements.

Figure 5(a) plots the block error rate P_e for polar codes with quantum data rate $R_Q \approx 0.30$, and Figure 5(b) plots the threshold for which $P_e \leq 10^{-4}$ along with the hashing bound $1 - H_2(p) - p\log_2(3)$ (this is the rate achievable by a

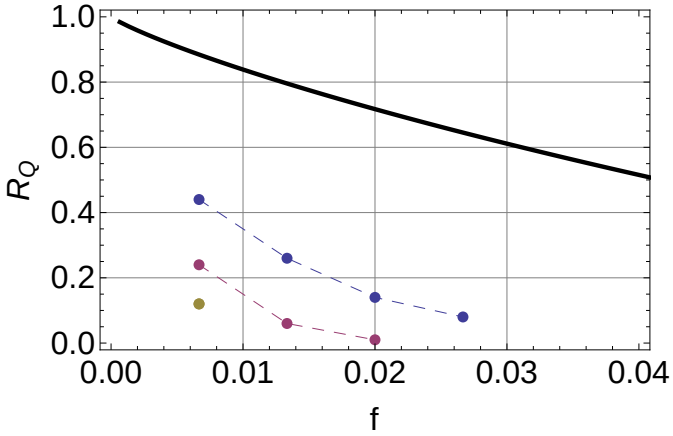

Fig. 6. BB84 channel simulation results. Threshold R_Q for $P_e \leq 10^{-4}$ versus flip probability f. The black curve is the hashing limit $1 - 2H_2(f)$.

random stabilizer code on the depolarizing channel). We see the performance relative to the bounds is not as strong as for the quantum erasure channel. Nevertheless, we obtain fairly large quantum data rates with low block error rate P_e and moderate block lengths $N = 1024$.

In Ref. [15], Kasai *et al*. presented results for quantum codes with code lengths in the range $N = 4000\text{-}35,406$ and achieved quantum rates higher than ours at the $P_e < 10^{-4}$ threshold. We should perform simulations of higher N to compare our coding scheme with theirs. However, it appears from our evidence so far that at these code lengths, achievable quantum polar code rates will be lower than theirs, unless we exploit some improved method such as that in Ref. [16] for computing the good and bad virtual channels.

C. Results for the BB84 Channel

Finally, we consider performance on the "BB84 channel" [17], which is a concatenation of a bit-flip and phase-flip channel, each having some equal flip probability f (see Section 2.1.1 of Ref. [17] for the relevance of this channel in quantum key distribution). For the BB84 channel, the induced amplitude and phase channels are simply binary symmetric channels, each with error probability f. Because the two channels are equivalent, as in the erasure channel case, it is optimal to choose equal underlying rates: $R_C^{(\text{amp})} = R_C^{(\text{phase})}$. Figure 6 plots our results for quantum data rates achieving the $P_e < 10^{-4}$ threshold. We see quantum polar code performance is very similar to that for the depolarizing channel.

VI. Application to Private Communication

Our simulations above serve equally well as simulations of polar codes for private classical data transmission over the channels we considered (where here the eavesdropper gets access to everything that the receiver does not obtain). This follows essentially from Theorem 1 of Renes [18], in which he proves that a lower bound on Bob's guessing probability for the phase variable serves as an upper bound for security against Eve with respect to the amplitude variable. Thus, the parameter in (13) serves as both a reliability and security parameter for the protection of classical data sent through the channels we have considered.

VII. Discussion

In summary, we have bounded the performance and conducted simulations of quantum communication over the quantum erasure channel, by utilizing the recently proposed quantum polar codes in Refs. [6], [7]. We found high quantum data rates for moderate block lengths $N = 1024$. We also performed simulations of these codes over the depolarizing and BB84 channels. In these cases, we found that quantum polar codes for these block lengths still performed ably but gave performance somewhat further from the hashing limits.

Going forward from here, it is important to explore the performance of larger block lengths in order to compare the performance of quantum polar codes with other error correction schemes. In the depolarizing and BB84 cases, it would be worthwhile to carry out an analysis of the optimality of the erasure-matched code choice. Also, one could exploit the techniques from Ref. [16] in order to choose which virtual channels to send the information bits through.

References

[1] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051–3073, July 2009.

[2] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," September 2011, arXiv:1109.2591.

[3] S. Guha and M. M. Wilde, "Polar coding to achieve the Holevo capacity of a pure-loss optical channel," February 2012, arXiv:1202.0533.

[4] M. M. Wilde and S. Guha, "Polar codes for degradable quantum channels," September 2011, arXiv:1109.5346.

[5] M. M. Wilde and J. M. Renes, "Polar codes for private classical communication," 2012, arXiv:1203.5794.

[6] J. M. Renes, F. Dupuis, and R. Renner, "Efficient quantum polar coding," September 2011, arXiv:1109.3195.

[7] M. M. Wilde and J. M. Renes, "Quantum polar codes for arbitrary channels," January 2012, arXiv:1201.2906.

[8] E. Arikan and E. Telatar, "On the rate of channel polarization," in *Proceedings of the 2009 International Symposium on Information Theory*, Seoul, Korea, June 2009, pp. 1493–1495, arXiv:0807.3806.

[9] J. M. Renes and J.-C. Boileau, "Physical underpinnings of privacy," *Physical Review A*, vol. 78, p. 032335, September 2008.

[10] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure key from bound entanglement," *Physical Review Letters*, vol. 94, p. 160502, April 2005.

[11] ——, "General paradigm for distilling classical key from quantum states," *IEEE Trans. Inf. Theory*, vol. 55, pp. 1898–1929, 2009.

[12] C. A. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum mechanical states," *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1216–1227, May 1998.

[13] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, "Capacities of quantum erasure channels," *Physical Review Letters*, vol. 78, pp. 3217–3220, April 1997.

[14] E. Arikan, "A performance comparison of polar codes and reed-muller codes," *IEEE Comm. Letters*, vol. 12, no. 6, pp. 447–449, June 2008.

[15] K. Kasai, M. Hagiwara, H. Imai, and K. Sakaniwa, "Quantum error correction beyond the bounded distance decoding limit," *IEEE Transactions on Information Theory*, vol. 58, no. 2, pp. 1223–1230, February 2012.

[16] I. Tal and A. Vardy, "How to construct polar codes," in *IEEE Information Theory Workshop*, Dublin, Ireland, 2010, arXiv:1105.6164.

[17] O. Kern and J. M. Renes, "Improved one-way rates for bb84 and 6-state protocols," *Quantum Information and Computation*, vol. 8, no. 8-9, pp. 756–772, 2008, arXiv:0712.1494.

[18] J. M. Renes, "Duality of privacy amplification against quantum adversaries and data compression with quantum side information," *Proceedings of the Royal Society A*, vol. 467, no. 2130, pp. 1604–1623, 2011.