1-1-2014

Polar codes for private and quantum communication over arbitrary channels

Joseph M. Renes
ETH Zürich

Mark M. Wilde
Université McGill

Recommended Citation

Renes, J., & Wilde, M. (2014). Polar codes for private and quantum communication over arbitrary channels. *IEEE Transactions on Information Theory, 60* (6), 3090-3103. https://doi.org/10.1109/TIT.2014.2314463

Polar codes for private and quantum communication over arbitrary channels

Joseph M. Renes and Mark M. Wilde

***Abstract*—We construct new polar coding schemes for the transmission of quantum or private classical information over arbitrary quantum channels. In the former case, our coding scheme achieves the symmetric coherent information and in the latter the symmetric private information. Both schemes are built from a polar coding construction capable of transmitting classical information over a quantum channel [Wilde and Guha, IEEE Transactions on Information Theory, in press]. Appropriately merging two such classical-quantum schemes, one for transmitting "amplitude" information and the other for transmitting "phase," leads to the new private and quantum coding schemes, similar to the construction for Pauli and erasure channels in [Renes, Dupuis, and Renner, Physical Review Letters 109, 050504 (2012)]. The encoding is entirely similar to the classical case, and thus efficient. The decoding can also be performed by successive cancellation, as in the classical case, but no efficient successive cancellation scheme is yet known for arbitrary quantum channels. An efficient code construction is unfortunately still unknown. Generally, our two coding schemes require entanglement or secret-key assistance, respectively, but we extend two known conditions under which the needed assistance rate vanishes. Finally, although our results are formulated for qubit channels, we show how the scheme can be extended to multiple qubits. This then demonstrates a near-explicit coding method for realizing one of the most striking phenomena in quantum information theory: the *superactivation effect,* whereby two quantum channels which individually have zero quantum capacity can have a non-zero quantum capacity when used together.**

POLAR coding is a promising code construction for transmitting classical information over classical channels [1]. Arıkan proved that polar codes achieve the symmetric capacity of any classical channel, with an encoding and decoding complexity that is $O(N \log N)$ where N is the number of channel uses. These codes exploit the channel polarization effect whereby a particular recursive encoding induces a set of virtual channels, such that some of the virtual channels are perfect for data transmission while the others are useless for this task. The fraction containing perfect virtual channels is equal to the channel's symmetric capacity.[1]

In this paper, we offer new polar coding schemes for transmitting quantum information or for privately transmitting classical information. Both are strongly based on ideas of Renes and Boileau [2], who showed that quantum or private coding protocols can be constructed from two different protocols that protect classical information encoded into complementary variables. In particular, a protocol for reliably transmitting quantum data can be built from a protocol that reliably recovers classical information encoded into an "amplitude" variable and a protocol that reliably recovers "phase" information with the assistance of quantum side information. The quantum coding scheme uses the decoders of both of these tasks, while the private coding scheme needs only the decoder of the amplitude variable and uses the fact that the phase could have been decoded in order to ensure security of the data via an entropic uncertainty relation (see [3], [4], [5], [6] for related ideas).

These ideas were used to construct quantum and private polar coding schemes with explicit, efficient decoders in [7] achieving rates equal to the symmetric coherent and private information, respectively, but only for a certain set of channels with essentially classical outputs (Pauli and erasure channels). Following a different approach, Wilde and Guha [8] constructed quantum and private polar codes at these rates for any degradable channels for which the output to the environment is essentially classical. (In both cases, the private codes obey the so-called strong security criterion, such that the eavesdropper gets essentially no information about the transmitted information, not merely that she only gets information at a vanishing rate.) Both coding techniques require entanglement or secret-key assistance in the general case.

Our new constructions have several advantages over these previous schemes:

- The net communication rate is equal to the symmetric coherent or private information for an *arbitrary* quantum channel with qubit input.
- The decoders are *explicit*; in the quantum case the decoder consists of $O(N)$ rounds of coherent quantum successive cancellation followed by N CNOT gates, while only an incoherent implementation of quantum successive cancellation is required in the private case.
- The entanglement or secret-key consumption rate vanishes for any quantum channel which is either degradable or which satisfies a certain fidelity criterion.

Following the multi-level polar coding method of [9], we show how to extend the coding scheme to channels with multiple qubit inputs. This gives an explicit code construction for the superactivation effect, in which two zero-capacity channels

JMR was supported by the Swiss National Science Foundation (SNF) through the National Centre of Competence in Research "Quantum Science and Technology" and project No. 200020-135048 and PP00P2-128455, by the European Research Council (ERC) via grant No. 258932. MMW acknowledges support from the Centre de Recherches Mathématiques at the University of Montreal.

Joseph M. Renes is with the Institute for Theoretical Physics, ETH Zurich, Zürich, Switzerland. Mark M. Wilde is with the School of Computer Science, McGill University, Montréal, Québec, Canada.

This work was presented in part at the 2012 International Symposium on Information Theory in Cambridge, Massachusetts, USA and the 2012 International Symposium on Information Theory and its Applications in Honolulu, Hawaii, USA.

[1] The symmetric capacity is equal to the channel's input-output mutual information, evaulated for a uniformly random input.

have a non-zero quantum capacity when used together [10] (in this sense, the channels *activate* each other).

We structure this paper as follows. After setting notation and defining important quantites in Section I, we describe the "amplitude" and "phase" channels relevant to our coding schemes in Section II. In Section III, we recall the results on polarization of channels with classical input and quantum output, and in Section IV, we describe the simultaneous polarization of the amplitude and phase channels, which is the heart of our coding scheme. Sections V and VI detail our quantum and private coding schemes, respectively. Section VII gives the two conditions under which the entanglement or secret-key assistance rate vanishes, while Section VIII outlines how to adapt our quantum polar coding scheme so that it can exhibit the superactivation effect. Finally, we conclude in Section IX with a summary and some open questions.

I. Notation and Definitions

A binary-input *classical-quantum* (cq) channel $\mathsf{W} : x \to \rho_x$ prepares a quantum state ρ_x at the output, depending on an input classical bit x. Two parameters that determine the performance of W are the fidelity

$$F(\mathsf{W}) \equiv \|\sqrt{\rho_0}\sqrt{\rho_1}\|_1$$

and the symmetric Holevo information

$$I(\mathsf{W}) \equiv H\big(\tfrac{1}{2}(\rho_0+\rho_1)\big) - \tfrac{1}{2}[H(\rho_0)+H(\rho_1)],$$

where $\|A\|_1 = \mathrm{Tr}[\sqrt{A^\dagger A}]$ and $H(\sigma) \equiv -\mathrm{Tr}\{\sigma \log_2 \sigma\}$ is the von Neumann entropy. These parameters generalize the Bhattacharya parameter and the symmetric mutual information [1], respectively, (note that the former is denoted by $Z(\mathsf{W})$ in [1]) and are related as [11]:

$$I(\mathsf{W}) \approx 1 \Leftrightarrow F(\mathsf{W}) \approx 0$$
$$I(\mathsf{W}) \approx 0 \Leftrightarrow F(\mathsf{W}) \approx 1.$$

The channel W is near perfect when $I(\mathsf{W}) \approx 1$ and near useless when $I(\mathsf{W}) \approx 0$.

A qubit-input *quantum channel* $\mathcal{N}^{A'\to B}$ is a completely positive, trace preserving map from a two-dimensional input system A' to a d-dimensional output system B. Every channel has an isometric extension (Stinespring dilation) to a partial isometry $U_{\mathcal{N}}^{A'\to BR}$ taking A' to B and an additional *reservoir* system R [12]. Fix an arbitrary basis with elements $|z\rangle$ and call it the computational or "amplitude" basis with $z \in \{0,1\}$. Let $|\widetilde{x}\rangle$ denote the conjugate, Hadamard, or "phase" basis with $\widetilde{x} \in \{+,-\}$ and $|\pm\rangle \equiv (|0\rangle \pm |1\rangle)/\sqrt{2}$. Furthermore, let X denote the operator such that

$$X\,|z\rangle = |z \oplus 1\rangle\,,$$

where arithmetic inside the ket is modulo 2, and Z the operator such that

$$Z\,|z\rangle = (-1)^z\,|z\rangle\,.$$

The symmetric coherent information of a channel is defined by

$$I_{\mathrm{sym}}(\mathcal{N}) \equiv H(B)_\tau - H(AB)_\tau, \tag{1}$$

where $\tau^{AB} = \mathcal{N}^{A'\to B}(\Phi^{AA'})$ and $\Phi^{AA'}$ denotes the maximally entangled state:

$$|\Phi\rangle^{AA'} \equiv \tfrac{1}{\sqrt{2}}\sum_{z\in\{0,1\}} |z\rangle^A|z\rangle^{A'} = \tfrac{1}{\sqrt{2}}\sum_{\widetilde{x}\in\{+,-\}} |\widetilde{x}\rangle^A|\widetilde{x}\rangle^{A'}.$$

A quantum wiretap channel $\mathcal{N}^{A'\to BE}$ [13], [14] is a completely positive, trace preserving map with an input system A', an output system B for the legitimate receiver (named Bob), and an output system E for the wiretapper (named Eve). Appendix B shows that a classical wiretap channel is a special case of a quantum wiretap channel. The symmetric private information of a quantum wiretap channel $\mathcal{N}^{A'\to BE}$ is defined by

$$P_{\mathrm{sym}}(\mathcal{N}) \equiv \max_{\rho^{ZA'}}[I(Z;B)_\tau - I(Z;E)_\tau], \tag{2}$$

where $\tau^{ZBE} = \mathcal{N}^{A'\to BE}(\rho^{ZA'})$ for $\rho^{ZA'}$ a cq state of the form:

$$\rho^{ZA'} = \tfrac{1}{2}\sum_z |z\rangle\langle z|^Z \otimes \rho_z^{A'},$$

and $\rho_z^{A'}$ an arbitrary set of (possibly mixed) states.

II. Classical-Quantum Channels for Complementary Variables

In this section we construct cq channels from a given quantum channel which will be relevant to the quantum coding procedure. Slight generalizations of these channels will be relevant to the private coding procedure.

A. CQ Channels for Quantum Communication

Following [2], we consider building up a quantum communication protocol from two classical communication protocols that preserve classical information encoded into complementary variables. In this vein, two particular classical-quantum (cq) channels are important. First, consider the cq channel induced by sending an amplitude basis state over $\mathcal{N}$

$$\mathsf{W}_A : z \to \mathcal{N}^{A'\to B}(|z\rangle\langle z|) \equiv \varphi_z^B, \tag{3}$$

where the classical input z is a binary variable and the notation W_A indicates that the classical information is encoded into the amplitude basis. We can regard this as the sender (Alice) modulating a standard signal $|0\rangle$ with X^z and transmitting the result to the receiver (Bob).

For the other cq channel, suppose that Alice instead transmits a binary variable x by modulating the signal with Z^x, a rephasing of the amplitude basis states. However, instead of applying this to $|0\rangle$, she modulates one share of an entangled state $\Phi^{CA'}$. To transmit the binary value x, Alice modulates C with the phase operator Z^x and then sends A' via the noisy channel $\mathcal{N}$ and C via a noiseless channel to Bob. The overall result is the state

$$|\sigma_x\rangle^{BCR} = U_{\mathcal{N}}^{A'\to BR}(Z^x)^C\,|\Phi\rangle^{A'C}\,, \tag{4}$$
$$= \tfrac{1}{\sqrt{2}}\sum_{z\in\{0,1\}} (-1)^{xz}\,|\varphi_z\rangle^{BR}\,|z\rangle^C\,, \tag{5}$$

where $|\varphi_z\rangle^{BR}$ is a purification of φ_z^B in (3). The relevant cq channel is then of the following form:

$$\mathsf{W}_P : x \to \sigma_x^{BC}, \tag{6}$$

where the notation W_P indicates that the classical information is encoded into a phase variable. In contrast to W_A, the channel W_P is one in which the receiver has quantum side information (in the form of system C) beyond what is transmitted by $\mathcal{N}$ itself. Operationally, this quantum side information becomes available to Bob after he coherently decodes the amplitude variable. It does *not* correspond operationally to a Bell state shared before communication begins.

Both cq channels in (3) and (6) arise in the error analysis of our quantum polar coding scheme, in the sense that its performance depends on the performance of constituent polar codes constructed for these cq channels. Moreover, the two channels are more closely related than they may initially appear. To see their relationship, consider the "channel state"

$$\begin{aligned} |\psi\rangle^{ABCR} &= \tfrac{1}{\sqrt{2}} \sum_{x\in\{0,1\}} |\widetilde{x}\rangle^A |\sigma_x\rangle^{BCR} \\ &= \tfrac{1}{\sqrt{2}} \sum_{z\in\{0,1\}} |z\rangle^A |z\rangle^C |\varphi_z\rangle^{BR}. \end{aligned} \tag{7}$$

Measuring system A in the phase basis $|\widetilde{x}\rangle$ generates the W_P output state σ_x^{BC} in the BC systems, while measuring A in the amplitude basis generates the W_A output φ_z^B in the B system.

Looking at the R system output of the amplitude basis measurement defines the cq channel W_R to the reservoir, pertaining to amplitude information in A:

$$\mathsf{W}_R : z \to \varphi_z^R.$$

The uncertainty principle of [3] then implies a relation between amplitude information about A present in R and phase information about A present in BC. Indeed, due to the special form of $|\psi\rangle$, namely, the coherent copy of the amplitude of A in system C, the following uncertainty relation holds [2], [3]:

$$H(Z^A|R)_\psi + H(X^A|BC)_\psi = 1, \tag{8}$$

where $H(Z^A|B)_\psi$ is the conditional von Neumann entropy of Z given B for the cq state $\frac{1}{2}\sum_z |z\rangle\langle z|^Z \otimes \phi_z^B$ (i.e., ψ after measuring A in the amplitude basis), while $H(X^A|BC)_\psi$ is the conditional entropy of X given BC for the cq state $\frac{1}{2}\sum_x |\widetilde{x}\rangle\langle\widetilde{x}|^X \otimes \sigma_x^{BC}$ (ψ after measuring A in the phase basis). For convenience, we reproduce the proof of (8) in Lemma 10 of Appendix A.

Since the channel inputs are presumed to be uniform, the uncertainty relation in (8) immediately implies

$$I(\mathsf{W}_P) + I(\mathsf{W}_R) = 1. \tag{9}$$

The more phase information goes to Bob, the less amplitude information goes to the reservoir R, and *vice versa*. In Section VII-A we will use this relationship to relate the quantum polar coding scheme presented in this article to that from prior work in [8].

B. CQ Channels for Private Communication

For the problem of private coding in the wiretap scenario, we must also specify the eavesdropper's output, not just the intended receiver's system B. In general, the eavesdropper (Eve) could have access to the reservoir R of $\mathcal{N}$ in whole *or in part*. Thus, let us suppose that R can be divided into two subsystems, S and E, the latter being the output held by the eavesdropper. Clearly, S does not negatively impact the security of communication between Alice and Bob. Indeed, S functions as a sort of "shield" [15], [2] protecting information in the honest parties' systems from leaking to E.

In the above, we have also assumed that the sender inputs a pure state to $\mathcal{N}$, in either the amplitude or phase basis. To study the private coding problem in full generality, we relax this assumption and suppose that Alice prepends an additional cq channel $\mathcal{M}$ to $\mathcal{N}$ whose job is to create (make) a state ρ_z from z:

$$\rho_z \equiv \mathcal{M}(|z\rangle\langle z|).$$

Altogether this defines the cq channel

$$\overline{\mathsf{W}}_A : z \to \mathcal{N}^{A'\to B} \circ \mathcal{M}^{A'}(|z\rangle\langle z|) \equiv \theta_z^B. \tag{10}$$

The state ρ_z admits a purification $|\varrho_z\rangle^{A'S'}$ to an additional system S', which functions as an additional shield system. The purification is created by a Stinespring dilation $U_{\mathcal{M}}^{A'\to A'S'}$ of $\mathcal{M}$ applied to $|z\rangle$:

$$|\varrho_z\rangle^{A'S'} = U_{\mathcal{M}}^{A'\to A'S'} |z\rangle^{A'}. \tag{11}$$

The relevant phase channel is the same as before, with the exception that again Alice prepends $\mathcal{M}$ to $\mathcal{N}$. The modulation now results in

$$\begin{aligned} |\omega_x\rangle^{BCSS'E} &= (Z^x)^C U_{\mathcal{N}}^{A'\to BSE} U_{\mathcal{M}}^{A'\to A'S'} |\Phi\rangle^{CA'} &(12)\\ &= \tfrac{1}{\sqrt{2}} \sum_{z\in\{0,1\}} (-1)^{xz} |z\rangle^C |\theta_z\rangle^{BSS'E}. &(13) \end{aligned}$$

The relevant cq channel is given by

$$\overline{\mathsf{W}}_P : x \to \omega_x^{BCSS'}, \tag{14}$$

Again the two channels $\overline{\mathsf{W}}_A$ and $\overline{\mathsf{W}}_P$ are related—the corresponding channel state (as in (7)) is now

$$\begin{aligned} |\overline{\psi}\rangle &= \tfrac{1}{\sqrt{2}} \sum_{x\in\{0,1\}} |\widetilde{x}\rangle^A |\omega_x\rangle^{BCSS'E} &(15)\\ &= \tfrac{1}{\sqrt{2}} \sum_{z\in\{0,1\}} |z\rangle^A |z\rangle^C |\theta_z\rangle^{BSS'E}. &(16) \end{aligned}$$

The amplitude channel to the eavesdropper, $\overline{\mathsf{W}}_E$ is simply $\overline{\mathsf{W}}_E : z \to \theta_z^E$. Again the uncertainty relation in (8) applies; it states

$$H(Z^A|E)_{\overline{\psi}} + H(X^A|BCSS')_{\overline{\psi}} = 1. \tag{17}$$

The immediately translates into

$$I(\overline{\mathsf{W}}_P) + I(\overline{\mathsf{W}}_E) = 1. \tag{18}$$

For private communication, this relation states that "*if the phase channel to Bob is nearly perfect, then the amplitude channel to Eve must be nearly useless and* vice versa."

The above uncertainty relation then enables us to construct a reliable and strongly secure polar coding scheme for sending private classical data. As outlined in Section VI-A, our scheme has the sender transmit private information bits through the synthesized channels (in the polar coding sense) that are nearly perfect in both amplitude and phase for Bob. The fact that these synthesized amplitude channels are nearly perfect guarantees that Bob will be able to recover these bits reliably. Meanwhile, the above uncertainty relation can be extended to the synthesized channels (see Lemma 11) and therefore the fact that the synthesized phase channels are nearly perfect for Bob guarantees that Eve will be able to recover only a negligibly small amount of information about the bits sent through them.

Partitioning the synthesized channels according to amplitude and phase for Bob, rather than according to amplitude for Bob and amplitude for Eve as in [8], has the advantage that the scheme achieves the symmetric private information rate for all quantum wiretap channels. Moreover, we can prove that the secret key consumption rate vanishes for all degradable quantum channels, and we can furthermore provide an additional sufficient condition for when the secret key rate of the polar coding scheme vanishes.

III. Polarization of Classical-Quantum Channels

Wilde and Guha [11] demonstrated how to construct synthesized versions of any cq channel W, by channel combining and splitting [1]. For blocklength $N = 2^n$, the synthesized channels are of the following form:

$$\mathsf{W}_N^{(i)} : u_i \to \rho_{(i),u_i}^{U_1^{i-1}B^N}, \tag{19}$$

where

$$\rho_{(i),u_i}^{U_1^{i-1}B^N} \equiv \sum_{u_1^{i-1}} \frac{1}{2^{i-1}} \left|u_1^{i-1}\right\rangle\left\langle u_1^{i-1}\right|^{U_1^{i-1}} \otimes \overline{\rho}_{u_1^i}^{B^N}, \tag{20}$$

$$\overline{\rho}_{u_1^i}^{B^N} \equiv \frac{1}{2^{N-i}} \sum_{u_{i+1}^N} \rho_{u^N G_N}^{B^N}, \tag{21}$$

$$\rho_{x^N}^{B^N} \equiv \rho_{x_1}^{B_1} \otimes \cdots \otimes \rho_{x_N}^{B_N}, \tag{22}$$

and G_N is Arıkan's encoding circuit matrix built from classical CNOT gates. The interpretation of this channel is that it is the one "seen" by the input 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 (QSCD) [11] 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 synthesized channels $\mathsf{W}_N^{(i)}$ polarize, in the sense that some become nearly perfect for classical data transmission while others become nearly useless. To prove this result, one can model the channel splitting and combining process as a random birth process [1], [11], and one can demonstrate that the induced random birth processes corresponding to the channel parameters $I(\mathsf{W}_N^{(i)})$ and $F(\mathsf{W}_N^{(i)})$ are martingales that converge almost surely to zero-one valued random variables in the limit of many recursions. The following theorem from [11] (which uses the result in [22]) characterizes the rate at which the channel polarization effect takes hold, and it is useful in proving statements about the performance of polar codes for cq channels:

Theorem 1 (Wilde & Guha [11]). *For any binary input cq channel W, let $\mathsf{W}_{2^n}^{(K)}$ be the random variable characterizing the K^{th} split channel and $F(\mathsf{W}_{2^n}^{(K)})$ the fidelity of that channel, where n indicates the level of recursion for the encoding. Then, for any $\beta < 1/2$,*

$$\lim_{n\to\infty} \Pr_K\{F(\mathsf{W}_{2^n}^{(K)}) < 2^{-2^{n\beta}}\} = I(\mathsf{W}). \tag{23}$$

Assuming knowledge of the good and bad channels, one can then construct a coding scheme based on the channel polarization effect, by dividing the synthesized channels according to the following polar coding rule:

$$\begin{aligned} \mathcal{G}_N(\mathsf{W},\beta) &\equiv \left\{ i \in [N] : F(\mathsf{W}_N^{(i)}) < 2^{-N^\beta} \right\}, \\ \mathcal{B}_N(\mathsf{W},\beta) &\equiv [N] \setminus \mathcal{G}_N(\mathsf{W},\beta) \end{aligned} \tag{24}$$

so that $\mathcal{G}_N(\mathsf{W},\beta)$ is the set of "good" channels and $\mathcal{B}_N(\mathsf{W},\beta)$ 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. An explicit construction of a QSCD that has an error probability scaling as $o(2^{-\frac{1}{2}N^\beta})$ was provided in [11]. Let $\{\Lambda_{u_{\mathcal{F}^c}}^{(u_\mathcal{F})}\}$ denote the corresponding decoding POVM, with $u_{\mathcal{F}^c}$ the information bits and $u_\mathcal{F}$ the frozen bits.

The algorithm of Tal and Vardy [17] efficiently determines which synthesized channels are good or bad (according to a fixed fidelity or error-probability criterion), but this algorithm is not known to work for channels with quantum output. Finding an efficient code construction in the quantum case is an open problem.

IV. Simultaneous Polarization

For our quantum polar coding scheme, we utilize a coherent version of Arıkan's encoder [1], meaning that the gates are quantum CNOT gates (this is the same encoder as in [7], [8]). The private polar coding scheme can simply use classical CNOT gates. Classical, amplitude-basis coding through the N-bit encoding circuit and N noisy channels results in an output state $\varphi_{z^N G_N}^{B^N}$ at the receiver, and the effect is to induce synthesized channels $\mathsf{W}_{A,N}^{(i)}$ as described in the previous section. Theorem 1 states that the fraction of amplitude-good channels (according to the criterion in (24)) is equal to $I(\mathsf{W}_A)$ or, equivalently, $I(Z^A;B)_\psi$ using the channel state $|\psi\rangle$ from (7). Again, Z^A indicates that system A of $|\psi\rangle$ is first measured in the amplitude basis.

One of the main insights of [7] is that the same encoding operation leads to channel polarization for the phase channel W_P as well. In the present context, suppose Alice modulates the C systems of the entangled states $|\Phi\rangle^{C^N A'^N}$ with x^N, but then inputs the A'^N systems to the coherent encoder before sending them via the channel to Bob. The result is

$$\begin{aligned}
&\tfrac{1}{\sqrt{2^N}} \sum_{z^N \in \{0,1\}^N} (-1)^{x^N \cdot z^N} \left|\varphi_{z^N G_N}\right\rangle^{B^N R^N} \left|z^N\right\rangle^{C^N} \qquad (25)\\
&= \tfrac{1}{\sqrt{2^N}} \sum_{z^N \in \{0,1\}^N} (-1)^{x^N \cdot z^N G_N} \left|\varphi_{z^N}\right\rangle^{B^N R^N} \left|z^N G_N\right\rangle^{C^N}\\
&= \tfrac{1}{\sqrt{2^N}} \sum_{z^N \in \{0,1\}^N} (-1)^{x^N G_N^T \cdot z^N} \left|\varphi_{z^N}\right\rangle^{B^N R^N} U_{\mathcal{E}} \left|z^N\right\rangle^{C^N},
\end{aligned}$$

since $x^N \cdot z^N G_N = x^N G_N^T \cdot z^N$ and where $U_{\mathcal{E}}$ denotes the polar encoder. Thus, the $B^N C^N$ marginal state is simply $U_{\mathcal{E}}^{C^N} \sigma_{x^N G_N^T}^{B^N C^N} U_{\mathcal{E}}^{\dagger C^N}$, so that the coherent encoder also induces synthesized channels $\mathsf{W}_{P,N}^{(i)}$ using the encoding matrix G_N^T instead of G_N, modulo the additional $U_{\mathcal{E}}$ acting on C^N. The fraction of phase-good channels is approximately equal to $I(\mathsf{W}_P)$ or equivalently $I\big(X^A; BC\big)_\psi$.

Note that the classical side information for the $\mathsf{W}_{P,N}^{(i)}$ channels is different from that in (19) because the direction of all CNOT gates is flipped due to the transpose of G_N when acting on phase variables. The change in the direction of the CNOT gates means that the i^{th} synthesized phase channel $\mathsf{W}_{P,N}^{(i)}$ is such that all of the *future* bits $x_N \cdots x_{i+1}$ are available to help in decoding bit x_i while all of the *past* bits $x_{i-1} \cdots x_1$ are randomized. (This is the same as described in [7] for Pauli channels.)

For the case of private coding, we need only make one small modification. Instead of applying the encoding operation immediately prior to $\mathcal{N}$, we apply the encoding operation prior to $\mathcal{N} \circ \mathcal{M}$. Otherwise we proceed as before.

V. Quantum Coding Scheme

In this section we describe the quantum coding scheme in detail. First we consider the encoder and establish the achievable rate of the protocol in the limit of infinitely-large blocklength. Then we describe the decoder and show that the protocol produces approximate ebits of fidelity exponentially close to unity between sender and receiver, justifying the rate calculation of the first subsection.

A. Encoder & Achievable Rates

We divide the synthesized cq amplitude channels $\mathsf{W}_{A,N}^{(i)}$ into sets $\mathcal{G}_N(\mathsf{W}_A, \beta)$ and $\mathcal{B}_N(\mathsf{W}_A, \beta)$ according to (24), and similarly, we divide the synthesized cq phase channels $\mathsf{W}_{P,N}^{(i)}$ into sets $\mathcal{G}_N(\mathsf{W}_P, \beta)$ and $\mathcal{B}_N(\mathsf{W}_P, \beta)$, where $\beta < 1/2$. The synthesized channels correspond to particular inputs to the encoding operation, and thus the set of all inputs divides into four groups: those that are good for both the amplitude and phase variable, those that are good for amplitude and bad for phase, bad for amplitude and good for phase, and those that are bad for both variables. We establish notation for these channels as follows:

$$\begin{aligned}
\mathcal{A} &\equiv \mathcal{G}_N(\mathsf{W}_A, \beta) \ \cap \ \mathcal{G}_N(\mathsf{W}_P, \beta),\\
\mathcal{X} &\equiv \mathcal{G}_N(\mathsf{W}_A, \beta) \ \cap \ \mathcal{B}_N(\mathsf{W}_P, \beta)\\
\mathcal{Z} &\equiv \mathcal{B}_N(\mathsf{W}_A, \beta) \ \cap \ \mathcal{G}_N(\mathsf{W}_P, \beta),\\
\mathcal{B} &\equiv \mathcal{B}_N(\mathsf{W}_A, \beta) \ \cap \ \mathcal{B}_N(\mathsf{W}_P, \beta).
\end{aligned}$$

Our quantum polar coding scheme has the sender transmit information qubits through the inputs in $\mathcal{A}$, frozen bits in the phase basis through the inputs in $\mathcal{X}$, frozen bits in the amplitude basis through the inputs in $\mathcal{Z}$, and halves of ebits shared with Bob through the inputs in $\mathcal{B}$ (we can think of these in some sense as being frozen simultaneously in both the amplitude and phase basis).

Thus, our coding procedure is *entanglement-assisted* [18]. Indeed, the encoder implicitly results in an entanglement-assisted Calderbank-Shor-Steane (CSS) code, as pointed out in [7]. In the stabilizer language of quantum error-correcting codes, the values of the frozen inputs determine the various stabilizers of the code, and due to the dual nature of the encoding circuit (polarizing both amplitude and phase inputs), frozen amplitude states become Z-type stabilizers and frozen phase states become X-type stabilizers. The need for entangled inputs signals that the CSS code is entanglement-assisted. As some inputs require both frozen amplitude and phase values, the resulting stabilizer code would need both the corresponding X- and Z-type stabilizers. These, however, do not commute, and the role of entanglement-assistance is to "enlarge" the stabilizers to additional systems on Bob's side such that they do commute. In spite of the fact that our quantum polar coding scheme results in a CSS code, the decoding procedure (quantum successive cancellation decoding) is very different from the standard stabilizer recovery procedure in which the receiver performs stabilizer measurements and classical post processing of syndromes.

The net rate of the protocol for blocklength N is simply $r_Q(N) \equiv \frac{|\mathcal{A}|-|\mathcal{B}|}{N}$. Upon suitable choice of amplitude basis, it equals the symmetric coherent information in the asymptotic limit:

Theorem 2. $\lim_{N\to\infty} r_Q(N) = I_{\text{sym}}(\mathcal{N})$.

Proof: From Theorem 1 it follows that

$$\lim_{N\to\infty} \frac{1}{N} |\mathcal{G}_N(\mathsf{W}_A, \beta)| = I\big(Z^A; B\big)_\psi, \qquad \text{and} \qquad (26)$$

$$\lim_{N\to\infty} \frac{1}{N} |\mathcal{G}_N(\mathsf{W}_P, \beta)| = I\big(X^A; BC\big)_\psi. \qquad (27)$$

From basic set theory we have

$$\begin{aligned}
|\mathcal{A}| =& |\mathcal{G}_N(\mathsf{W}_A, \beta)| + |\mathcal{G}_N(\mathsf{W}_P, \beta)|\\
&- |\mathcal{G}_N(\mathsf{W}_A, \beta) \ \cup \ \mathcal{G}_N(\mathsf{W}_P, \beta)|,
\end{aligned}$$

as well as

$$|\mathcal{G}_N(\mathsf{W}_A, \beta) \ \cup \ \mathcal{G}_N(\mathsf{W}_P, \beta)| = N - |\mathcal{B}|.$$

Thus, the rate of the scheme is equal to

$$\begin{aligned}
\lim_{N\to\infty} \frac{|\mathcal{A}| - |\mathcal{B}|}{N} &= I\big(Z^A; B\big)_\psi + I\big(X^A; BC\big)_\psi - 1 \qquad (28)\\
&= I\big(Z^A; B\big)_\psi - I\big(Z^A; R\big)_\psi\\
&= H(B)_\psi - H\big(B|Z^A\big)_\psi\\
&\quad - [H(R)_\psi - H\big(R|Z^A\big)_\psi]\\
&= H(B)_\psi - H(R)_\psi\\
&= H(B)_\tau - H(AB)_\tau.
\end{aligned}$$

Here the second equality uses (9). The third equality is an identity, and the fourth follows from the fact that the state on BR is pure when conditioned on a measurement outcome of A, so that $H\big(B|Z^A\big)_\psi = H\big(R|Z^A\big)_\psi$. The final equality uses the fact that the entropy expressions are equal when evaluated for the state $\tau^{AB} = \mathcal{N}^{A'\to B}(\Phi^{AA'})$. ■

B. Decoder and Error Analysis

We now describe the decoder in more detail and demonstrate that the fidelity of the entire coding scheme becomes exponentially close to one as the blocklength gets large. In particular, we will show

Theorem 3. *Given any quantum channel with a qubit input system and a finite-dimensional output system, for large enough blocksize N, there exists a quantum polar coding scheme which generates approximate ebits that are $o(2^{-\frac{1}{2}N^\beta})$-close in trace distance to exact ebits for $\beta < 1/2$. Furthermore, the rate of this scheme is equal to the symmetric coherent information of the channel.*

Proof: The sender and receiver begin with the following state:

$$|\Psi_0\rangle = N_0 \sum_{u_\mathcal{A},u_\mathcal{B}} |u_\mathcal{A}\rangle|u_\mathcal{A}\rangle|u_\mathcal{Z}\rangle|\widetilde{u}_\mathcal{X}\rangle|u_\mathcal{B}\rangle \otimes |u_\mathcal{B}\rangle,$$

where Alice possesses the first five registers, Bob the last one,[2] and $N_0 \equiv 1/\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|}}$. We also assume for now that the bits in $u_\mathcal{Z}$ and $u_\mathcal{X}$ are chosen uniformly at random and are known to both the sender and receiver. Note that the fourth register is expressed in the phase basis; using the amplitude basis instead gives

$$|\Psi_0\rangle = N_1 \sum_{u_\mathcal{A},u_\mathcal{B},v_\mathcal{X}} (-1)^{u_\mathcal{X}\cdot v_\mathcal{X}}|u_\mathcal{A}\rangle|u_\mathcal{A}\rangle|u_\mathcal{Z}\rangle|v_\mathcal{X}\rangle|u_\mathcal{B}\rangle \otimes |u_\mathcal{B}\rangle,$$

where $N_1 \equiv 1/\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}$. The sender then feeds the middle four registers through the polar encoder and channel, leading to a state of the following form:

$$|\Psi_1\rangle = N_1 \sum_{u_\mathcal{A},u_\mathcal{B},v_\mathcal{X}} (-1)^{u_\mathcal{X}\cdot v_\mathcal{X}}|u_\mathcal{A}\rangle \otimes |\varphi_{u_\mathcal{A},u_\mathcal{Z},v_\mathcal{X},u_\mathcal{B}}\rangle^{B^N R^N}|u_\mathcal{B}\rangle,$$

where $|\varphi_{u_\mathcal{A},u_\mathcal{Z},v_\mathcal{X},u_\mathcal{B}}\rangle^{B^N R^N} \equiv U_\mathcal{N}^{\otimes N} U_\mathcal{E}|u_\mathcal{A}\rangle|u_\mathcal{Z}\rangle|v_\mathcal{X}\rangle|u_\mathcal{B}\rangle$ (abusing notation, the encoding operation G_N is left implicit).

Observe that, conditioned on amplitude measurements of $|u_\mathcal{A}\rangle$ and $|u_\mathcal{B}\rangle$, the B^N subsystem is identical to the polar-encoded output of W_A. Thus, the first step of the decoder is the following coherent implementation of the QSCD for the amplitude channel W_A

$$V_A = \sum_{u_\mathcal{A},u_\mathcal{B},v_\mathcal{X}} \sqrt{\Lambda^{(u_\mathcal{B},u_\mathcal{Z})}_{u_\mathcal{A},v_\mathcal{X}}} \otimes |u_\mathcal{A}\rangle|v_\mathcal{X}\rangle \otimes |u_\mathcal{B}\rangle|u_\mathcal{B}\rangle\langle u_\mathcal{B}| \otimes |u_\mathcal{Z}\rangle. \tag{29}$$

The idea here is that the decoder coherently recovers the bits in $u_\mathcal{A}$ and $v_\mathcal{X}$, using $u_\mathcal{Z}$ and $u_\mathcal{B}$ as classical and quantum side information, respectively. Appendix C provides a detailed argument that the state resulting from this first decoding step is $o(2^{-\frac{1}{2}N^\beta})$-close in expected trace distance to the following ideal state:

$$|\Psi_2\rangle = N_1 \sum_{u_\mathcal{A},u_\mathcal{B},v_\mathcal{X}} (-1)^{u_\mathcal{X}\cdot v_\mathcal{X}}|u_\mathcal{A}\rangle|\varphi_{u_\mathcal{A},u_\mathcal{Z},v_\mathcal{X},u_\mathcal{B}}\rangle^{B^N R^N} \otimes |u_\mathcal{A}\rangle|v_\mathcal{X}\rangle|u_\mathcal{B}\rangle|u_\mathcal{B}\rangle|u_\mathcal{Z}\rangle, \tag{30}$$

where the expectation is with respect to the uniformly random choice of $u_\mathcal{X}$. Thus, Bob has coherently recovered the bits $u_\mathcal{A}$ and $v_\mathcal{X}$ with the decoder in (29), while making a second coherent and incoherent copy of the bits $u_\mathcal{B}$ and $u_\mathcal{Z}$, respectively.

The next step in the process is to make coherent use of the W_P decoder. For this to be useful, however, we must show that encoded versions of $|\sigma_x\rangle^{BCE}$, as in (25), are present in $|\Psi_2\rangle$. To see this, first observe that we can write

$$|\Psi_2\rangle = N_2 \sum_{\substack{u_\mathcal{A},u_\mathcal{B},v_\mathcal{X},\\ x_\mathcal{A},x_\mathcal{B}}} (-1)^{u_\mathcal{X}\cdot v_\mathcal{X}+x_\mathcal{A}\cdot u_\mathcal{A}+x_\mathcal{B}\cdot u_\mathcal{B}}|\widetilde{x}_\mathcal{A}\rangle\otimes |\varphi_{u_\mathcal{A},u_\mathcal{Z},v_\mathcal{X},u_\mathcal{B}}\rangle^{B^N R^N}|u_\mathcal{A}\rangle|v_\mathcal{X}\rangle|u_\mathcal{B}\rangle|\widetilde{x}_\mathcal{B}\rangle|u_\mathcal{Z}\rangle,$$

where $N_2 \equiv 1/\sqrt{2^{2|\mathcal{A}|+2|\mathcal{B}|+|\mathcal{X}|}}$, by expressing the first register and the second $|u_\mathcal{B}\rangle$ register in the phase basis. This is nearly the expression we are looking for, as all the desired phase factors are present, except one corresponding to $|u_\mathcal{Z}\rangle$.

As $u_\mathcal{Z}$ is chosen at random, we can describe it quantum-mechanically as arising from part of an entangled state. The other part is shared by Alice and an inaccessible reference system. Including this purification degree of freedom, $|\Psi_2\rangle$ becomes

$$|\Psi'_2\rangle = N_3 \sum_{\substack{u_\mathcal{A},u_\mathcal{B},v_\mathcal{X},\\ u_\mathcal{Z},x_\mathcal{A},x_\mathcal{B}}} (-1)^{u_\mathcal{X}\cdot v_\mathcal{X}+x_\mathcal{A}\cdot u_\mathcal{A}+x_\mathcal{B}\cdot u_\mathcal{B}}|\widetilde{x}_\mathcal{A}\rangle\otimes |\varphi_{u_\mathcal{A},u_\mathcal{Z},v_\mathcal{X},u_\mathcal{B}}\rangle^{B^N E^N}|u_\mathcal{A}\rangle|v_\mathcal{X}\rangle|u_\mathcal{B}\rangle|\widetilde{x}_\mathcal{B}\rangle|u_\mathcal{Z}\rangle \otimes |u_\mathcal{Z}\rangle\,,$$

where $N_3 = N_2/\sqrt{2^{|\mathcal{Z}|}}$. Again utilizing the phase basis gives

$$|\Psi'_2\rangle = N_3 \sum_{\substack{u_\mathcal{A},u_\mathcal{B},v_\mathcal{X},u_\mathcal{Z},\\ x_\mathcal{A},x_\mathcal{B},x_\mathcal{Z}}} (-1)^{u_\mathcal{X}\cdot v_\mathcal{X}+x_\mathcal{A}\cdot u_\mathcal{A}+x_\mathcal{B}\cdot u_\mathcal{B}+x_\mathcal{Z}\cdot u_\mathcal{Z}}|\widetilde{x}_\mathcal{A}\rangle\otimes |\varphi_{u_\mathcal{A},u_\mathcal{Z},v_\mathcal{X},u_\mathcal{B}}\rangle^{B^N E^N}|u_\mathcal{A}\rangle|v_\mathcal{X}\rangle|u_\mathcal{B}\rangle|\widetilde{x}_\mathcal{B}\rangle|u_\mathcal{Z}\rangle \otimes |\widetilde{x}_\mathcal{Z}\rangle\,.$$

Thus, $|\Psi'_2\rangle$ is a superposition of polar encoded states as in (25) and therefore the phase decoder will be useful to the receiver. In particular, Bob can first apply $U_\mathcal{E}^{\dagger C^N}$ and then coherently apply the QSCD for the phase channel W_P,

$$V_P = \sum_{x_\mathcal{A},x_\mathcal{Z},x_\mathcal{B}} \sqrt{\Gamma^{(x_\mathcal{B},u_\mathcal{X})}_{x_\mathcal{A},x_\mathcal{Z}}} \otimes |\widetilde{x}_\mathcal{A}\rangle|\widetilde{x}_\mathcal{Z}\rangle|\widetilde{u}_\mathcal{X}\rangle \otimes |\widetilde{x}_\mathcal{B}\rangle\langle\widetilde{x}_\mathcal{B}| \tag{31}$$

to coherently extract the values of $x_\mathcal{A}$ and $x_\mathcal{Z}$ using the frozen bits $x_\mathcal{B}$ and $u_\mathcal{X}$. He then applies $U_\mathcal{E}^{C^N}$ to restore the C^N registers to their previous form. As with the amplitude decoding step, a similar argument (detailed in Appendix D) ensures the closeness of the output of this process to the ideal output as governed by the error probability of the W_P

[2] In quantum information theory the tensor product symbol is often used implicitly. Our convention in this section is to leave it implicit for systems belonging to the same party and use it explicitly to denote a division between two parties.

decoder. To express the ideal output succinctly, we first make the assignments

$$|\Phi_{\mathcal{A}}\rangle \equiv \frac{1}{\sqrt{2^{|\mathcal{A}|}}} \sum_{u_{\mathcal{A}}} |u_{\mathcal{A}}\rangle |u_{\mathcal{A}}\rangle, \;\; |\Phi_{\mathcal{Z}}\rangle \equiv \frac{1}{\sqrt{2^{|\mathcal{Z}|}}} \sum_{v_{\mathcal{Z}}} |v_{\mathcal{Z}}\rangle |v_{\mathcal{Z}}\rangle,$$
$$|\Phi_{\mathcal{X}}\rangle \equiv \frac{1}{\sqrt{2^{|\mathcal{X}|}}} \sum_{v_{\mathcal{X}}} |v_{\mathcal{X}}\rangle |v_{\mathcal{X}}\rangle, \;\; |\Phi_{\mathcal{B}}\rangle \equiv \frac{1}{\sqrt{2^{|\mathcal{B}|}}} \sum_{u_{\mathcal{B}}} |u_{\mathcal{B}}\rangle |u_{\mathcal{B}}\rangle.$$

Rewriting phase terms with Pauli operators, we then have that the actual output of this step of the decoder is $o(2^{-\frac{1}{2}N^{\beta}})$-close in expected trace distance to the following ideal state:

$$|\Psi_3\rangle = N_4 \sum_{x_{\mathcal{A}}, x_{\mathcal{B}}, x_{\mathcal{Z}}} |\widetilde{x}_{\mathcal{A}}\rangle \otimes |\widetilde{x}_{\mathcal{A}}\rangle \, |\widetilde{x}_{\mathcal{Z}}\rangle \, |\widetilde{u}_{\mathcal{X}}\rangle \, |\widetilde{x}_{\mathcal{B}}\rangle$$
$$Z^{x_{\mathcal{A}}, x_{\mathcal{Z}}, u_{\mathcal{X}}, x_{\mathcal{B}}} U_{\mathcal{N}}^{\otimes N} U_{\mathcal{E}} \, |\Phi_{\mathcal{A}}\rangle \, |\Phi_{\mathcal{Z}}\rangle \, |\Phi_{\mathcal{X}}\rangle \, |\Phi_{\mathcal{B}}\rangle \otimes |\widetilde{x}_{\mathcal{Z}}\rangle \, , \tag{32}$$

where $N_4 \equiv 1/\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{Z}|}}$. Here $Z^{x_{\mathcal{A}}, x_{\mathcal{Z}}, u_{\mathcal{X}}, x_{\mathcal{B}}}$ is shorthand for $Z^{x_{\mathcal{A}}} \otimes Z^{x_{\mathcal{Z}}} \otimes Z^{u_{\mathcal{X}}} \otimes Z^{x_{\mathcal{B}}}$, which acts on the second qubits in the entangled pairs, while the encoding and channel unitaries act on the first.

The final step in the decoding process is to remove (or "decouple") the phase operator $Z^{x_{\mathcal{A}}, x_{\mathcal{Z}}, v_{\mathcal{X}}, x_{\mathcal{B}}}$ by controlled operations from the registers $|\widetilde{x}_{\mathcal{A}}\rangle \, |\widetilde{x}_{\mathcal{Z}}\rangle \, |\widetilde{u}_{\mathcal{X}}\rangle \, |\widetilde{x}_{\mathcal{B}}\rangle$ to the second qubits in the entangled pairs. This phase-basis controlled phase operation is equivalent to N CNOT operations from the latter systems to the former and results in

$$N_0 \sum_{x_{\mathcal{A}}} |\widetilde{x}_{\mathcal{A}}\rangle \otimes |\widetilde{x}_{\mathcal{A}}\rangle \, U_{\mathcal{N}}^{\otimes N} U_{\mathcal{E}} \, |\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle \sum_{x_{\mathcal{B}}} |u_{\mathcal{X}}\rangle \, |\widetilde{x}_{\mathcal{B}}\rangle \, ,$$

with Bob sharing $1/\sqrt{2^{|\mathcal{Z}|}} \sum_{x_{\mathcal{Z}}} |\widetilde{x}_{\mathcal{Z}}\rangle \otimes |\widetilde{x}_{\mathcal{Z}}\rangle$ with the inaccessible reference. Thus, applying the triangle inequality for trace distance, the protocol finishes with Alice and Bob sharing a state close in trace distance to the following state:

$$\frac{1}{\sqrt{|\mathcal{A}|}} \sum_{x_{\mathcal{A}}} |\widetilde{x}_{\mathcal{A}}\rangle \otimes |\widetilde{x}_{\mathcal{A}}\rangle \, ,$$

That is, the sender and receiver generate $|\mathcal{A}|$ approximate ebits with trace distance less than $o(2^{-\frac{1}{2}N^{\beta}})$ to ideal ebits at the end of the protocol. ∎

Remark 4. *The above scheme performs well with respect to a uniformly random choice of the bits $u_{\mathcal{X}}$ and $u_{\mathcal{Z}}$, in the sense that the expectation of the fidelity is high. However, Markov's inequality implies that a large fraction of the possible codes have good performance.*

Remark 5. *The first step of the decoder is identical to the first step of the decoder from [8]. Though, the second step above is an improvement over the second step in [8] because it is an explicit coherent QSCD, rather than an inexplicit controlled-decoupling unitary. Additionally, the decoder's complexity is equivalent to $O(N)$ quantum hypothesis tests and other unitaries resulting from the polar decompositions of $\Lambda_{u_{\mathcal{A}}, v_{\mathcal{X}}}^{(u_{\mathcal{B}}, u_{\mathcal{Z}})}$ and $\Gamma_{x_{\mathcal{A}}, x_{\mathcal{Z}}}^{(x_{\mathcal{B}}, u_{\mathcal{X}})}$, but it remains unclear how to implement these efficiently.*

VI. Private Coding Scheme

The private coding scheme is a slight variation of the quantum coding scheme and makes use of the fact that the quantum encoder is based on a CSS code. Indeed, one can reduce the quantum case to a classical protocol, as was first demonstrated by Shor and Preskill [19]. Renes *et al.* [7] point out that this reduction applies to quantum polar codes, being CSS codes. Here we shall follow a more direct route by defining and analyzing the private coding procedure independently of the quantum protocol.

A. Encoder & Achievable Rates

As before, we divide the encoder inputs into four groups

$$\mathcal{A} \equiv \mathcal{G}_N\big(\mathsf{W}_A, \beta\big) \;\cap\; \mathcal{G}_N\big(\mathsf{W}_P, \beta\big),$$
$$\mathcal{X} \equiv \mathcal{G}_N\big(\mathsf{W}_A, \beta\big) \;\cap\; \mathcal{B}_N\big(\mathsf{W}_P, \beta\big),$$
$$\mathcal{Z} \equiv \mathcal{B}_N\big(\mathsf{W}_A, \beta\big) \;\cap\; \mathcal{G}_N\big(\mathsf{W}_P, \beta\big),$$
$$\mathcal{B} \equiv \mathcal{B}_N\big(\mathsf{W}_A, \beta\big) \;\cap\; \mathcal{B}_N\big(\mathsf{W}_P, \beta\big).$$

Unlike the quantum coding scheme, all inputs are now made in the amplitude basis. The sender again inputs information bits to $\mathcal{A}$ and frozen bits into $\mathcal{Z}$. Now the sender mimics frozen phase inputs to $\mathcal{X}$ with random bits and mimics halves of ebits input to $\mathcal{B}$ with secret key bits. Thus, our private coding procedure is generally *secret-key assisted*. Its rate is simply $r_P(N) = \frac{|\mathcal{A}|-|\mathcal{B}|}{N}$. It equals the symmetric private information in the asymptotic limit:

Theorem 6. $\lim_{N\to\infty} r_P(N) = P_{\text{sym}}(N)$.

Proof: The proof is entirely similar to the proof of Theorem 2, with the exception that we choose $\mathcal{M}$ to create the optimal states ρ_z in the symmetric private information. Then we use

$$\lim_{N\to\infty} \frac{1}{N} \big|\mathcal{G}_N\big(\mathsf{W}_A, \beta\big)\big| = I\big(Z^A; B\big)_{\overline{\psi}}, \tag{33}$$
$$\lim_{N\to\infty} \frac{1}{N} \big|\mathcal{G}_N\big(\mathsf{W}_P, \beta\big)\big| = I\big(X^A; BCSS'\big)_{\overline{\psi}}, \tag{34}$$

and appeal to (18) instead of (9). ∎

We should stress that our consideration of the phase channels in this part of the paper is only necessary in order to compute the index sets $\mathcal{A}$, $\mathcal{X}$, $\mathcal{Z}$, and $\mathcal{B}$. The decoder in the next section does not make explicit use of these phase channels—they only arise in our security analysis, where we appeal to the uncertainty relation in (17) in order to guarantee security of the scheme. This is in contrast to the quantum polar coding scheme of the previous sections, in which the decoder makes explicit use of the phase channels.

B. Decoder & Reliability and Security Analysis

We now describe the decoder and examine the reliability and security of the resulting protocol. Our approach leads to strong security, as stated in the following theorem:

Theorem 7. *For sufficiently large N, the private polar coding scheme given above satisfies the following reliability and security criteria:*

1) $\Pr\{\widehat{U}_{\mathcal{C}} \neq U_{\mathcal{C}}\} \leq o\Big(2^{-\frac{1}{2}N^{\beta}}\Big)$, *for* $\mathcal{C} \equiv \mathcal{A} \cup \mathcal{X}$, *and*
2) $I(U_{\mathcal{A}}; E^N) \leq o\Big(2^{-\frac{1}{2}N^{\beta}}\Big)$.

Proof: First, it is straightforward to prove that the code has good reliability, by appealing to the results from [11]. That is, there exists a POVM $\{\Lambda^{(u_{\mathcal{Z}}, u_{\mathcal{B}})}_{u_{\mathcal{A}}, u_{\mathcal{X}}}\}$, the quantum successive cancellation decoder, such that

$$\Pr\{\widehat{U}_{\mathcal{C}} \neq U_{\mathcal{C}}\} \leq \sqrt{2 \sum_{i \in \mathcal{C}} F(\mathsf{W}^{(i)}_{A,N})} \tag{35}$$
$$= o\Big(2^{-\frac{1}{2}N^{\beta}}\Big). \tag{36}$$

where $\mathcal{C} \equiv \mathcal{A} \cup \mathcal{X}$. The QSCD operates exactly as in [11], treating $\mathcal{Z} \cup \mathcal{B}$ as the frozen set and decoding all bits in the set $\mathcal{A} \cup \mathcal{X}$, though of course only the bits in $\mathcal{A}$ contain the transmitted message. This decoder has an efficient implementation if the channel to Bob is classical [1]. This is the case for the amplitude damping channel, the erasure channel, and any Pauli channel, for example.

We now prove that strong security, in the sense of [20], holds for our polar coding scheme. Consider that

$$\begin{aligned} I(U_{\mathcal{A}}; E^N) &= \sum_{i \in \mathcal{A}} I\Big(U_i; E^N \big| U_{\mathcal{A}_i^-}\Big) \\ &= \sum_{i \in \mathcal{A}} I\Big(U_i; E^N U_{\mathcal{A}_i^-}\Big) \\ &\leq \sum_{i \in \mathcal{A}} I\big(U_i; E^N U_1^{i-1}\big) \\ &= \sum_{i \in \mathcal{A}} I(\overline{\mathsf{W}}^{(i)}_{E,N}) \end{aligned}$$

The first equality is from the chain rule for quantum mutual information and by defining $\mathcal{A}_i^-$ to be the indices in $\mathcal{A}$ preceding i. The second equality follows from the assumption that the bits in $U_{\mathcal{A}_i^-}$ are chosen uniformly at random. The first inequality is from quantum data processing. The third equality is from the definition of the synthesized channels $\overline{\mathsf{W}}^{(i)}_{E,N}$. Continuing, we have

$$\begin{aligned} &\leq \sum_{i \in \mathcal{A}} \sqrt{1 - F(\overline{\mathsf{W}}^{(i)}_{E,N})^2} \\ &\leq \sum_{i \in \mathcal{A}} \sqrt{1 - (1 - 2F(\overline{\mathsf{W}}^{(i)}_{P,N}))^2} \\ &\leq \sum_{i \in \mathcal{A}} \sqrt{4F(\overline{\mathsf{W}}^{(i)}_{P,N})} \\ &\leq 2 \sum_{i \in \mathcal{A}} \sqrt{2^{-N^{\beta}}} \\ &= o\Big(2^{-\frac{1}{2}N^{\beta}}\Big). \end{aligned}$$

The first inequality is from [11, Proposition 1]. The second holds since the two synthesized channels obey an uncertainty relation, shown in Lemma 11, which then gives a fidelity uncertainty relation, shown in Lemma 12. Here we set $\mathsf{W}_1 = \overline{\mathsf{W}}^{(i)}_{P,N}$ and $\mathsf{W}_2 = \overline{\mathsf{W}}^{(i)}_{E,N}$ in the latter lemma. The fourth inequality follows from the definition of the set $\mathcal{A}$. ■

A clear advantage of the current approach over the previous construction from [8] is that Theorem 1 directly applies to the phase-good channels with the "goodness criterion" given by (24). Only the amplitude channels to Eve (rather than the phase-good channels to Bob) were considered in [8], and it seemed only possible to prove polarization results for quantum wiretap channels in which the amplitude channel to Eve is classical. Our approach here overcomes this difficulty by appealing to Theorem 1 directly for polarization and later relating the phase channels to Bob and the amplitude channels to Eve via an uncertainty relation.

VII. Entanglement & Secret-Key Assistance Are Not Always Needed

In this section we give two different conditions for when the quantum or private coding schemes require only a sublinear amount of entanglement or secret-key assistance. The first occurs when the channel is degradable [21], in the sense that the R output (Eve's output E in the private case) can be generated from Bob's output B by some quantum operation. The second stems from properties of the binary erasure channel (BEC) as an "extreme point" in the channel synthesis process.

A. Degradable Channels

Suppose that the channel $\mathcal{N}$ is degradable in the sense that the R output φ_z^R can be generated from the B output φ_z^B by some other quantum channel $\mathcal{D}$: $\varphi_z^R = \mathcal{D}(\varphi_z^B)$. Similarly, in the private coding scenario, suppose that $\varrho_z^E = \mathcal{D}(\varrho_z^B)$. Then we can show

Theorem 8. *For degradable channels in the quantum or private coding scenerios as described above, the rate of entanglement or secret key assistance, respectively, vanishes in the limit of large blocklength:*

$$\lim_{N \to \infty} \tfrac{1}{N} |\mathcal{B}| = 0. \tag{37}$$

We provide a brief summary of the proof and then follow with more detail. First, the channel uncertainty relation (9) can be extended to synthesized channels (as the inequality given in Lemma 11) and implies that phase-good channels (output fidelity near zero) to Bob are amplitude-"very bad" channels to R (output fidelity near one). From degradability, we also know that the doubly-bad channels $\mathcal{B}$ are amplitude-bad channels to R. These two observations imply that the doubly-bad channels to Bob, the phase-good channels to Bob, and amplitude-good channels to R are disjoint sets. The sum of the fractional sizes of the latter two sets equals $I\big(X^A; BC\big)_{\psi} + I\big(Z^A; R\big)_{\psi} = 1$ by (8), implying that the rate of the doubly-bad channel set $\mathcal{B}$ (the entanglement consumption rate) approaches zero in the same limit. Replaying the argument for the channels in the private communication scenario gives the same result.

Proof: The proof is a modification of the argument in [8], which in turn came from [20]. First observe that following three sets of channels are disjoint: the doubly bad channels $\mathcal{B}$, the amplitude-good channels to R, $\mathcal{G}_N(\mathsf{W}_R, \beta)$, and the phase-good channels to Bob, $\mathcal{G}_N(\mathsf{W}_P, \beta)$. Clearly the first and last are disjoint by the definition of $\mathcal{B}$. The first two are disjoint by the degradability condition: any channel amplitude-bad for Bob must also be amplitude-bad for R. Formally, the output fidelity can only go down under the degrading map; see [8, Lemma 3]. Finally, that the second two are disjoint follows from the fidelity uncertainty relations in Lemma 12. Setting $\mathsf{W}_1 = \mathsf{W}_{P,N}^{(i)}$ and $\mathsf{W}_2 = \mathsf{W}_{R,N}^{(i)}$ therein, the lemma states that the fidelities of $\mathsf{W}_{P,N}^{(i)}$ and $\mathsf{W}_{R,N}^{(i)}$ cannot both be small:

$$2 \cdot 2^{-N^\beta} \geq 2 \cdot F(\mathsf{W}_{P,N}^{(i)}) \geq 1 - F(\mathsf{W}_{R,N}^{(i)}). \tag{38}$$

This implies

$$F(\mathsf{W}_{R,N}^{(i)}) \geq 1 - 2 \cdot 2^{-N^\beta}, \tag{39}$$

whenever $2^{-N^\beta} \geq F(W_{P,N}^{(i)})$. Thus, all of the channels that are phase-good for Bob are amplitude-“very bad” for R. Therefore the following relation holds for large enough N:

$$\mathcal{G}_N(\mathsf{W}_P, \beta) \cap \mathcal{G}_N(\mathsf{W}_R, \beta) = \emptyset. \tag{40}$$

Since these three sets are disjoint, the sum of their sizes cannot exceed N, the total number of channels:

$$\frac{1}{N}(|\mathcal{G}_N(W_R, \beta)| + |\mathcal{G}_N(\mathsf{W}_P, \beta)| + |\mathcal{B}|) \leq 1. \tag{41}$$

Finally, we know from Theorem 1 that the rates of the sets $\mathcal{G}_N(W_R, \beta)$ and $\mathcal{G}_N(W_P, \beta)$ in the asymptotic limit are

$$\lim_{N\to\infty} \frac{1}{N}|\mathcal{G}_N(W_R, \beta)| = I(Z^A; R)_\psi,$$
$$\lim_{N\to\infty} \frac{1}{N}|\mathcal{G}_N(W_P, \beta)| = I(X^A; BC)_\psi = 1 - I(Z^A; R)_\psi,$$

so that the rate of $\mathcal{B}$ must be zero in the asymptotic limit. ■

Note that in the limit $N \to \infty$, the channels polarize, so that the channels which are good in phase for Bob are bad in amplitude for R, and the ones which are good in amplitude for R are bad in phase for Bob. This demonstrates that our quantum polar coding scheme given here is asymptotically equivalent to the scheme of Wilde and Guha [8] in the limit of many recursions of the encoding after the channel polarization effect takes hold. Thus, this same argument implies that the entanglement consumption rate for the quantum polar codes in [8] vanishes for general degradable quantum channels because the rate of the phase-good channels to Bob is a lower bound on the rate of the amplitude-“very bad” channels to R.

B. General Condition Based on Erasure Channels

The binary erasure channel (BEC) plays a special role in the channel synthesis process. Suppose we have an arbitrary channel W with output fidelity F_0. Then, the i^{th} channel synthesized from the BEC with fidelity F_0 is always less reliable than the corresponding i^{th} channel synthesized from W. This is due to the fact that, among all channels with a fixed symmetric capacity, the BEC with that capacity has the smallest output fidelity. This was shown for classical channels in [1, Proposition 11], and the same argument works in the quantum case using (21) and (22) of [11] instead of (34) and (35) of [1]. Thus, if the i^{th} synthesized BEC channel is good, then surely the i^{th} synthesized W is also. From this observation, [7] gave a condition under which entanglement assistance is needed only at a sublinear rate. Here we show that the same condition holds in the more general setting discussed in this paper.

Theorem 9. *In the quantum and private coding schemes above,* $\lim_{N\to\infty} \frac{1}{N}|\mathcal{B}| = 0$ *if*

$$F(\mathsf{W}_A) + F(\mathsf{W}_P) \leq 1. \tag{42}$$

We first provide a heuristic proof sketch which clarifies the main idea behind the proof, and then we follow with the full proof. Since the encoder applies the transformation G_N for the amplitude channel but G_N^T for the phase channel, an input i corresponds to a doubly-bad synthesized channel if the i^{th} synthesized amplitude channel is bad and the $(N-i)^{\text{th}}$ synthesized phase channel is bad. For a given input or synthesized channel i, call $N - i$ the complementary-variable channel.

Letting F_i^p be the output fidelity of the i^{th} channel synthesized from the BEC with erasure probability p, the proof rests on the fact that

$$F_{N-i}^p = 1 - F_i^{1-p}. \tag{43}$$

Since $F_i^{p'} \geq F_i^p$ for $p' \geq p$, this relation implies that, for $p < 1/2$ the complement of a bad channel is a good channel, while for $p > 1/2$ the complement of a good channel is a bad channel. Note that p itself is the output fidelity of the BEC with erasure probability p.

Now suppose the two channels W_A and W_P are erasure channels with erasure probabilities p_A and p_P, respectively, such that $p_A \leq p_P < 1/2$. Thus they satisfy the stated constraint. Indeed, we need only check that no doubly bad channels occur for the case $p_A = p_P$, since then they certainly will not occur when one of the erasure probabilities is smaller and some inputs switch from bad to good. Now, if i is a bad input for W_P, the complementary-variable input is good, and therefore i must be a good input to W_A. Similarly, a bad input for W_A must be a good input to W_P and so indeed no doubly-bad inputs can occur in this case. On the other hand, this line of argumentation fails when one or other of the erasure probabilities is greater than $1/2$.

Finally, since the BEC is the worst case under channel synthesis among all base channels with a given output fidelity, the stated condition holds for all channels.

Proof: As described in Section III, one can prove that channel polarization takes hold by considering the channel splitting and combining process as a random birth process $\{\mathsf{W}_n : n \geq 0\}$ (with the channel choice determined by an iid Bernoulli process $\{B_n : n \geq 1\}$ and setting $\mathsf{W}_0 = \mathsf{W}$). One can then consider the induced birth process for the fidelity parameter

$$\{F_n : n \geq 0\} \equiv \{F(\mathsf{W}_n) : n \geq 0\}.$$

In [22] it is shown that the following extremal process $\{F_n' : n \geq 0\}$ bounds the actual channel process $\{F_n : n \geq 0\}$:

$$F_{n+1}' = \begin{cases} F_n'^2 & \text{if} \quad B_n = 0 \\ 2F_n' - F_n'^2 & \text{if} \quad B_n = 1 \end{cases},$$

a relation which can be written more symmetrically as

$$\begin{aligned} F'_{n+1} &= F'^2_n \qquad &\text{if} \quad B_n = 0, \\ 1 - F'_{n+1} &= (1 - F'_n)^2 \quad &\text{if} \quad B_n = 1. \end{aligned} \tag{44}$$

Note that the extremal process is based on the process for a BEC with the same initial fidelity F_0. From now on, we make abbreviations such as $\{F_n\} = \{F_n : n \geq 0\}$ in order to simplify the notation. The extremality of the process is based on recursive relations for the synthesized channel fidelities, equations (34) and (35) of [1]. These have been extended to the case the channel has quantum outputs as equations (21) and (22) of [11]. Therefore, the results derived in [22] hold in the present setting as well.

In particular, the extremal process above has the nice property [22, Observation 4 (ii)] that for every realization $\{b_n\}$ of the process $\{B_n\}$ (and thus for every realization $\{f'_n\}$ of $\{F'_n\}$) there exists a particular initial threshold value $F'_{\text{th}}(\{b_n\})$ such that either

$$\lim_{n\to\infty} f'_n = 0 \text{ if } F'_0 < F'_{\text{th}}(\{b_n\}),$$

or

$$\lim_{n\to\infty} f'_n = 1 \text{ if } F'_0 \geq F'_{\text{th}}(\{b_n\}).$$

(Note that F'_0 is deterministic and is the initial value of the process.)

We can denote the respective fidelity processes for the amplitude and phase channels in our coding scheme as $\{F^A_n\}$ and $\{F^P_n\}$ and the respective random birth processes as $\{B^A_n\}$ and $\{B^P_n\}$. Also, let $\{F^{A\prime}_n\}$ and $\{F^{P\prime}_n\}$ denote the corresponding extremal processes. The important observation made in [7] is that the process $\{F^P_n\}$ makes the opposite choice of channel at each step of the birth process because the phase encoder is the reverse of the amplitude encoder. That is, it holds for every n and for every realization $\{b^A_n\}$ and $\{b^P_n\}$ that

$$b^P_n = 1 - b^A_n.$$

Thus, we can write $B^P_n = 1 - B^A_n$, so that B^P_n is completely determined by B^A_n. The extremal amplitude channel process $\{F^{A\prime}_n\}$ is already of the form in (44), and we can consider the extremal phase process as $\{1 - F^{P\prime}_n\}$ in order for it to have this same form. Thus, a realization $\{f^{A\prime}_n\}$ of the extremal amplitude channel process $\{F^{A\prime}_n\}$ converges to one if

$$F^{A\prime}_0 \geq F'_{\text{th}}(\{b^A_n\}),$$

and a realization $\{1 - f^{P\prime}_n\}$ of the extremal phase process $\{1 - F^{P\prime}_n\}$ converges to zero if

$$1 - F^{P\prime}_0 < F'_{\text{th}}(\{b^A_n\}),$$

implying that $\{f^{P\prime}_n\}$ converges to one if

$$F^{P\prime}_0 > 1 - F'_{\text{th}}(\{b^A_n\}).$$

Thus, the sum process $\{F^{A\prime}_n + F^{P\prime}_n\}$ converges to two if

$$\begin{aligned} F^{A\prime}_0 + F^{P\prime}_0 &\geq F'_{\text{th}}(\{b^A_n\}) + 1 - F'_{\text{th}}(\{b^A_n\}) \\ &= 1. \end{aligned} \tag{45}$$

The above bound is a *universal*, sufficient lower bound for the sum process to converge to two, that holds regardless of the threshold value $F'_{\text{th}}(\{b^A_n\})$ for a particular realization $\{b^A_n\}$. It follows that a given realization $\{f^A_n + f^P_n\}$ of the actual sum process $\{F^A_n + F^P_n\}$ can only converge to two when (45) holds because we set $F^{A'}_0 = F^A_0$ and the extremal process bounds the actual process (note that some realizations might converge to one or zero as well). If a realization $\{f^A_n + f^P_n\}$ of the sum process $\{F^A_n + F^P_n\}$ converges to two, then this implies that the set $\mathcal{B}$ is non-empty, i.e., the code will require some preshared entanglement or secret key. So, if the condition in the statement of the theorem holds, no realization of the sum process can ever converge to two, and the code will not require any secret key bits. ■

The above argument only holds in the asymptotic limit of many recursions of the encoding such that the channel polarization effect takes hold (where all synthesized channels are polarized to be completely perfect or useless). That is, the argument does not apply whenever there is a finite number of recursions—in this case, if the number of recursions is large enough, then a large fraction of synthesized channels polarize according to some tolerance, but there is always a small fraction that have not polarized. Thus, we can only conclude that the above proof applies in the limit of many recursions and that the rate of secret key consumption vanishes in this limit.

VIII. Superactivation

Our quantum polar coding scheme can be adapted to realize the superactivation effect, in which two zero-capacity quantum channels can *activate* each other when used jointly, such that the joint channel has a non-zero quantum capacity [10]. Recall that the channels from [10] are a four-dimensional PPT channel and a four-dimensional 50% erasure channel. Each of these have zero quantum capacity, but the joint tensor-product channel has non-zero capacity.[3]

We now discuss how to realize a quantum polar coding scheme for the joint channel. Observe that the input space of the joint channel is 16-dimensional and thus has a decomposition as a tensor product of four qubit-input spaces: $\mathbb{C}^4 \otimes \mathbb{C}^4 \simeq \mathbb{C}^{16} \simeq \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2 \otimes \mathbb{C}^2$. Thus, we can exploit a slightly modified version of our qubit polar coding scheme. Following [9], the idea is for Alice and Bob to employ a quantum polar code for each qubit in the tensor factor. Let $Z_1, \ldots, Z_4$ denote the amplitude variables of these qubits and let $X_1, \ldots, X_4$ denote the phase variables. Bob's decoder is such that he coherently decodes Z_1, uses it as quantum side information (QSI) to decode Z_2, uses both Z_1 and Z_2 as QSI to decode Z_3, and then uses all of $Z_1, \ldots, Z_3$ to help decode Z_4. With all of the amplitude variables decoded, Bob then uses these as QSI to decode X_1, and continues successively until

[3] We are speaking of *catalytic* superactivation. A catalytic protocol uses entanglement assistance, but the figure of merit is the net rate of quantum communication—the total quantum communication rate minus the entanglement consumption rate. Note that the catalytic quantum capacity is equal to zero if the standard quantum capacity is zero. Thus, the superactivation effect that we speak of in this section is for the catalytic quantum capacity.

he coherently decodes X_4. At the end he performs controlled phase gates to recover entanglement established with Alice.

We now calculate the total rate of this scheme. For the first qubit space in the tensor factor, the channels split up into four types depending on whether they are good/bad for amplitude/phase. Using the formula (28), the net quantum data rate for the first tensor factor is equal to

$$I(Z_1;B) + I(X_1;BZ_1Z_2Z_3Z_4) - 1.$$

(The formula is slightly different here because Bob decodes the phase variable X_1 with all of the amplitude variables as QSI.) For the second qubit space in the tensor factor, the net quantum data rate is

$$I(Z_2;BZ_1) + I(X_2;BZ_1Z_2Z_3Z_4X_1) - 1.$$

We can similarly determine the respective net quantum data rates for the third and fourth qubit spaces as

$$\begin{aligned}&I(Z_3;BZ_1Z_2) + I(X_3;BZ_1Z_2Z_3Z_4X_1X_2) - 1,\\&I(Z_4;BZ_1Z_2Z_3) + I(X_4;BZ_1Z_2Z_3Z_4X_1X_2X_3) - 1.\end{aligned}$$

Summing all these rates together with the chain rule and using the fact that any two amplitude and/or phase variables are independent whenever $i \neq j$, we obtain the overall net quantum data rate:

$$I(Z_1Z_2Z_3Z_4;B) + I(X_1X_2X_3X_4;BZ_1Z_2Z_3Z_4) - 4,$$

which is equal to the coherent information of the joint channel (as in the proof of Theorem 2). The fact that our quantum polar code can achieve the symmetric coherent information rate then proves that superactivation occurs, given that Smith and Yard already showed that this rate is non-zero for the channels mentioned above [10].

IX. Conclusion

We have demonstrated new polar coding schemes for quantum or private communication which achieve high rates for *arbitrary* quantum channels, unlike the constructions in [8], [7]. The encoding operations are efficient, though currently no efficient algorithm to construct the code itself. (That is, for general quantum channels, no efficient algorithm is known for determining which inputs correspond to good or bad synthesized channels.) For the decoder the situation is somewhat reversed: Given the code construction, the decoder is explicit—it is based on the quantum successive cancellation method of [11]—but no efficient implementation is known.

Finding an efficient code construction algorithm and an efficient successive cancellation decoder are the main questions left open in this work. It would be interesting to determine conditions beyond those of Section VII under which entanglement or secret-key assistance are not needed or to find an argument ensuring reliability and strong security of the private coding scheme which relies only on the "amplitude" properties of the wiretap channel.

Acknowledgments

The authors acknowledge helpful discussions with Frédéric Dupuis, Saikat Guha, and Graeme Smith.

Appendix A
Useful Lemmas

Lemma 10 (Renes & Boileau [3])**.** *The following uncertainty relation holds*

$$H(Z^A|R)_\psi + H(X^A|BC)_\psi = 1, \tag{46}$$

where

$$|\psi\rangle^{ABCR} = \sum_z \sqrt{p_z}\, |z\rangle^A |z\rangle^C |\varphi_z\rangle^{BR}.$$

Proof: Rewriting system A of ψ using the conjugate basis gives

$$\begin{aligned}|\psi\rangle^{ABCR} &= \sum_z \sqrt{p_z}\tfrac{1}{\sqrt{2}} \sum_x (-1)^{xz} |\widetilde{x}\rangle^A |z\rangle^C |\varphi_z\rangle^{BR} &(47)\\ &= \tfrac{1}{\sqrt{2}} \sum_x |\widetilde{x}\rangle^A (Z^x)^C |\psi'\rangle^{CBR}, &(48)\end{aligned}$$

where

$$|\psi'\rangle^{CBR} = \sum_z \sqrt{p_z}\, |z\rangle^C |\varphi_z\rangle^{BR}.$$

To compute $H(X^A|BC)_\psi$ first write it as

$$H(X^A|BC)_\psi = H(X^A)_\psi + H(BC|X^A)_\psi - H(BC)_\psi$$

whose terms are easier to evaluate. The first is simply $H(X^A)_\psi = 1$, while the second is just

$$H(BC|X^A)_\psi = H(CB)_{\psi'} = H(R)_{\psi'} = H(R)_\psi$$

since the two marginal states of BC given X^A are unitarily-related and one of the marginals is ψ'^{CB}. Since ψ'^{CBR} is pure, $H(CB)_{\psi'} = H(R)_{\psi'}$ and a quick calculation reveals that $H(R)_{\psi'} = H(R)_\psi$. Meanwhile, the BC marginal is $\psi^{BC} = \sum_z p_z\, |z\rangle\langle z|^C \otimes \varphi_z^B$, and so

$$\begin{aligned}H(CB)_\psi &= H(Z^A)_\psi + \sum_z p_z H(\varphi_z^B) &(49)\\ &= H(Z^A)_\psi + \sum_z p_z H(\varphi_z^R) &(50)\\ &= H(Z^A R)_\psi, &(51)\end{aligned}$$

using the entropic properties of bipartite pure states. Thus,

$$\begin{aligned}H(X^A|BC)_\psi &= 1 + H(R)_\psi - H(Z^A R)_\psi &(52)\\ &= 1 - H(Z^A|R)_\psi. &(53)\end{aligned}$$

■

Lemma 11. *The synthesized channels $\mathsf{W}_{P,N}^{(i)}$ and $\mathsf{W}_{R,N}^{(i)}$ obey*

$$I(\mathsf{W}_{P,N}^{(i)}) + I(\mathsf{W}_{R,N}^{(i)}) \leq 1. \tag{54}$$

The same relation holds when replacing $\mathsf{W}_{P,N}^{(i)}$ and $\mathsf{W}_{R,N}^{(i)}$ with $\overline{\mathsf{W}}_{P,N}^{(i)}$ and $\overline{\mathsf{W}}_{E,N}^{(i)}$, respectively.

Proof: Consider N copies of the channel state $|\psi\rangle^{ABCR}$ in (7) where the B systems are first subjected to the polarization transformation before input to the channel:

$$|\Psi_N\rangle^{A^NB^NC^NR^N} = \frac{1}{\sqrt{2^N}} \sum_{z^N} |z^N\rangle^{A^N} |z^N\rangle^{C^N} |\varphi_{z^N G_N}\rangle^{B^NR^N}$$

Then let $\overline{\Psi}^i_N$ be the state after measuring the systems $A_1 \cdots A_{i-1}$ in the amplitude basis and the systems $A_{i+1} \cdots A_N$ in the phase basis, indicating the various measurement output systems as $Z_1, \dots Z_{i-1}$ and $X_{i+1}, \dots, X_N$ so that it is clear these systems become classical. From $\overline{\Psi}^i_N$ one can simultaneously generate the outputs of the i^{th} phase channel to Bob, $\mathsf{W}^{(i)}_{P,N}$ and the i^{th} amplitude channel $\mathsf{W}^{(i)}_{R,N}$ to the reservoir R, just as in the simple case of $|\xi\rangle$ in Section II. In particular, $\overline{\Psi}^i_N$ is a tripartite state on

$$A_i | B^N C^N X^N_{i+1} | R^N Z^{i-1}_1,$$

where the vertical bars indicate the divisions of the parties. Applying the uncertainty principle from [3] gives

$$H(X^{A_i} | B^N C^N X^N_{i+1})_{\overline{\Psi}^i_N} + H(Z^{A_i} | R^N Z^{i-1}_1)_{\overline{\Psi}^i_N} \geq 1 \quad (55)$$

Combining this with $H\big(X^{A_i}\big) + H\big(Z^{A_i}\big) = 2$, which holds because X^{A_i} and Z^{A_i} are uniform random bits, yields

$$I\big(X^{A_i}; B^N C^N X^N_{i+1}\big)_{\overline{\Psi}^i_N} + I\big(Z^{A_i}; R^N Z^{i-1}_1\big)_{\overline{\Psi}^i_N} \leq 1,$$

or equivalently,

$$I(\mathsf{W}^{(i)}_{P,N}) + I(\mathsf{W}^{(i)}_{R,N}) \leq 1. \quad (56)$$

The same argument applies starting from N copies of the channel state $|\overline{\psi}\rangle$ from (15). ■

Lemma 12. *For complementary binary-input channels* W_1 *and* W_2 *obeying the uncertainty relation* $I(\mathsf{W}_1) + I(\mathsf{W}_2) \leq 1$,

$$2F(\mathsf{W}_1) + \ \ F(\mathsf{W}_2) \geq 1, \qquad \textit{and} \quad (57)$$
$$F(\mathsf{W}_1) + 2F(\mathsf{W}_2) \geq 1. \quad (58)$$

Proof: Start with the following inequality for binary-input channels W [11, Proposition 1]:

$$I(\mathsf{W}) \geq \log_2\left(\frac{2}{1 + F(\mathsf{W})}\right). \quad (59)$$

This is equivalent to $F(\mathsf{W}) \geq 2^{1 - I(\mathsf{W})} - 1$. Then we have

$$F(\mathsf{W}_1) \geq 2^{1 - I(\mathsf{W}_1)} - 1 \quad (60)$$
$$\geq 2^{I(\mathsf{W}_2)} - 1 \quad (61)$$
$$\geq \frac{2}{1 + F(\mathsf{W}_2)} - 1, \quad (62)$$

where we used the uncertainty relation in the second step. Rewriting this, we obtain

$$(1 + F(\mathsf{W}_2))F(\mathsf{W}_1) \geq 2 - (1 + F(\mathsf{W}_2)). \quad (63)$$

Since the fidelity is less than unity, this gives the first inequality. Interchanging the two channels and repeating the argument gives the second. ■

Appendix B
Classical Wiretap Channels as Quantum Wiretap Channels

Suppose that $p(y, z|x)$ is a classical wiretap channel such that x is the input and y and z are the outputs for the legitimate receiver and the wiretapper, respectively. Then we can embed the random variables X, Y, and Z into quantum systems, so that the resulting wiretap channel has the following action on an arbitrary input state ρ:

$$\mathcal{N}_{\text{C}}^{A' \to BE}(\rho) \equiv \sum_{x,y,z} \langle x|\rho|x\rangle \; p(y, z|x) |y\rangle\langle y|^B \otimes |z\rangle\langle z|^E. \quad (64)$$

The physical interpretation of the above channel is that it first *measures* the input system in the orthonormal basis $\{|x\rangle\langle x|\}$ (ensuring that the input is effectively classical) and *prepares* the classical states $|y\rangle^B$ and $|z\rangle^E$ for Bob and Eve with probability $p(y, z|x)$. One can check that the Kraus operators [12] for this classical channel are

$$\left\{ \sqrt{p(y, z|x)} \big(|y\rangle^B \otimes |z\rangle^E\big) \langle x|^{A'} \right\}_{x,y,z}.$$

Thus, by a standard construction [12], an isometric extension of this classical wiretap channel acts as follows on a pure state input $|\psi\rangle$:

$$U_{\mathcal{N}_{\text{C}}}^{A' \to BES_2} |\psi\rangle^{A'}$$
$$= \sum_{x,y,z} \sqrt{p(y, z|x)} \, \langle x|\psi\rangle^{A'} \, |y\rangle^B \, |z\rangle^E \, |x, y, z\rangle^{S_2}$$

so that tracing over system S_2 recovers the action of the original channel in (64).

Appendix C
Detailed Error Analysis for the Coherent Amplitude Decoder

We provide details of the error analysis in Section V-B for the first decoding step, in which Bob coherently recovers the amplitude information. Given the frozen bits $u_{\mathcal{X}}$ and $u_{\mathcal{Z}}$, the ideal state after the first step of the decoder is given in (30) and for convenience, again in (65). Applying the coherent amplitude measurement V_A in (29) actually results in (66). Computing their overlap results in (67). Next, we take the expectation of their overlap with respect to the uniformly random choice of the frozen bits $u_{\mathcal{X}}$ and $u_{\mathcal{Z}}$. This leads to the steps in (68)-(72), which give the desired result. The penultimate inequality is just $\sqrt{\Lambda} \geq \Lambda$ for any $0 \leq \Lambda \leq \mathbb{1}$. The last inequality in this sequence follows from the good performance of the quantum successive cancellation decoder for the cq amplitude channels [11, Proposition 4].

Appendix D
Detailed Error Analysis for the Coherent Phase Decoder

We provide details of the error analysis in Section V-B for the second decoding step, in which Bob coherently recovers the phase information. We can prove that the phase decoder works well with a uniformly random choice of the bits $u_{\mathcal{X}}$ and $u_{\mathcal{Z}}$. Observe that a uniformly random choice of the bits $u_{\mathcal{Z}}$ induces a uniform distribution of the bits $x_{\mathcal{Z}}$. Let us fix a value of $x_{\mathcal{Z}}$. Then, a similar error analysis as in Appendix C then works for this case. The ideal state resulting from the second decoding step is given in (74). This state is the same as in (32) with a fixed, but randomly-chosen value of $x_{\mathcal{Z}}$. The actual state from using the coherent decoder V_P in 31 is given in (76). The overlap between the above two states is

$$|\Psi_{2;u_{\mathcal{X}},u_{\mathcal{Z}}}\rangle = \frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}} \sum_{u''_{\mathcal{A}},u''_{\mathcal{B}},v''_{\mathcal{X}}} (-1)^{u_{\mathcal{X}}\cdot v''_{\mathcal{X}}} |u''_{\mathcal{A}}\rangle \big|\varphi_{u''_{\mathcal{A}},u_{\mathcal{Z}},v''_{\mathcal{X}},u''_{\mathcal{B}}}\big\rangle^{B^N E^N} |u''_{\mathcal{A}}\rangle|v''_{\mathcal{X}}\rangle|u''_{\mathcal{B}}\rangle|u''_{\mathcal{B}}\rangle|u_{\mathcal{Z}}\rangle. \tag{65}$$

$$|\Psi^{\text{actual}}_{2;u_{\mathcal{X}},u_{\mathcal{Z}}}\rangle = \frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}}} \sum_{\substack{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},\\ u'_{\mathcal{A}},v'_{\mathcal{X}}}} (-1)^{u_{\mathcal{X}}\cdot v_{\mathcal{X}}} |u_{\mathcal{A}}\rangle \sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u'_{\mathcal{A}},v'_{\mathcal{X}}}} |\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\big\rangle^{B^N E^N} |u'_{\mathcal{A}}\rangle|v'_{\mathcal{X}}\rangle|u_{\mathcal{B}}\rangle|u_{\mathcal{B}}\rangle|u_{\mathcal{Z}}\rangle \tag{66}$$

$$\langle\Psi_{2;u_{\mathcal{X}},u_{\mathcal{Z}}}|\Psi^{\text{actual}}_{2;u_{\mathcal{X}},u_{\mathcal{Z}}}\rangle = \frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|}} \sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},v'_{\mathcal{X}}} (-1)^{u_{\mathcal{X}}\cdot\left(v'_{\mathcal{X}}+v_{\mathcal{X}}\right)} \langle\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v'_{\mathcal{X}},u_{\mathcal{B}}}| \sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v'_{\mathcal{X}}}} |\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\big\rangle^{B^N E^N} \tag{67}$$

$$\begin{aligned}
&\mathbb{E}_{U_{\mathcal{X}},U_{\mathcal{Z}}}\left\{\langle\Psi_{2;U_{\mathcal{X}},U_{\mathcal{Z}}}|\Psi^{\text{actual}}_{2;U_{\mathcal{X}},U_{\mathcal{Z}}}\rangle\right\} && (68)\\
&= \frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}} \frac{1}{2^{|\mathcal{X}|}} \sum_{u_{\mathcal{X}},u_{\mathcal{Z}}} \sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},v'_{\mathcal{X}}} (-1)^{u_{\mathcal{X}}\cdot\left(v'_{\mathcal{X}}+v_{\mathcal{X}}\right)} \langle\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v'_{\mathcal{X}},u_{\mathcal{B}}}| \sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v'_{\mathcal{X}}}} |\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\big\rangle^{B^N E^N} && (69)\\
&= \frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}} \sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},v'_{\mathcal{X}},u_{\mathcal{Z}}} \delta_{v'_{\mathcal{X}},v_{\mathcal{X}}} \langle\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v'_{\mathcal{X}},u_{\mathcal{B}}}| \sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v'_{\mathcal{X}}}} |\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\big\rangle^{B^N E^N} && (70)\\
&= \frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}} \sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},u_{\mathcal{Z}}} \langle\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}| \sqrt{\Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v_{\mathcal{X}}}} |\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\big\rangle^{B^N E^N} && (71)\\
&\geq \frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}} \sum_{u_{\mathcal{A}},u_{\mathcal{B}},v_{\mathcal{X}},u_{\mathcal{Z}}} \langle\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}| \Lambda^{(u_{\mathcal{B}},u_{\mathcal{Z}})}_{u_{\mathcal{A}},v_{\mathcal{X}}} |\varphi_{u_{\mathcal{A}},u_{\mathcal{Z}},v_{\mathcal{X}},u_{\mathcal{B}}}\big\rangle^{B^N E^N} && (72)\\
&\geq 1 - o(2^{-\frac{1}{2}N^{\beta}}), && (73)
\end{aligned}$$

$$|\Xi^{\text{ideal}}_{x_{\mathcal{Z}},u_{\mathcal{X}}}\rangle = \frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|}}} \sum_{x_{\mathcal{A}},x_{\mathcal{B}}} |\widetilde{x}_{\mathcal{A}}\rangle Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}} U_{\mathcal{N}} U_{\mathcal{E}}^{A'^N} |\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle|\widetilde{x}_{\mathcal{A}}\rangle|\widetilde{x}_{\mathcal{Z}}\rangle|\widetilde{u}_{\mathcal{X}}\rangle|\widetilde{x}_{\mathcal{B}}\rangle, \tag{74}$$

$$\begin{aligned}
|\Xi^{\text{actual}}_{x_{\mathcal{Z}},u_{\mathcal{X}}}\rangle &= U_{\mathcal{E}}^{C^N} V_P U_{\mathcal{E}}^{\dagger C^N} \left(\frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|}}} \sum_{x_{\mathcal{A}},x_{\mathcal{B}}} |\widetilde{x}_{\mathcal{A}}\rangle Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}} U_{\mathcal{N}} U_{\mathcal{E}}^{A'^N} |\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle|\widetilde{x}_{\mathcal{B}}\rangle\right) && (75)\\
&= \frac{1}{\sqrt{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{Z}|}}} \sum_{x'_{\mathcal{A}},x'_{\mathcal{Z}},x'_{\mathcal{B}},x_{\mathcal{A}}} |\widetilde{x}_{\mathcal{A}}\rangle U_{\mathcal{E}}^{C^N} \sqrt{\Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x'_{\mathcal{A}},x'_{\mathcal{Z}}}} U_{\mathcal{E}}^{\dagger C^N} Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}} U_{\mathcal{N}} U_{\mathcal{E}}^{A'^N} |\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle\, |\widetilde{x}'_{\mathcal{A}}\rangle\, |\widetilde{x}'_{\mathcal{Z}}\rangle\, |\widetilde{u}_{\mathcal{X}}\rangle\, |\widetilde{x}_{\mathcal{B}}\rangle\,. && (76)
\end{aligned}$$

$$\begin{aligned}
&\langle\Xi^{\text{ideal}}_{x_{\mathcal{Z}},u_{\mathcal{X}}}|\Xi^{\text{actual}}_{x_{\mathcal{Z}},u_{\mathcal{X}}}\rangle\\
&= \frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|}} \sum_{x_{\mathcal{A}},x_{\mathcal{B}}} \langle\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}| U_{\mathcal{E}}^{\dagger A'^N} U_{\mathcal{N}}^{\dagger} Z^{-x_{\mathcal{A}},-u_{\mathcal{X}},-x_{\mathcal{B}},-x_{\mathcal{Z}}} U_{\mathcal{E}}^{C^N} \sqrt{\Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x_{\mathcal{A}},x_{\mathcal{Z}}}} U_{\mathcal{E}}^{\dagger C^N} Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}} U_{\mathcal{N}} U_{\mathcal{E}}^{A'^N} |\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle && (77)\\
&\geq \frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|}} \sum_{x_{\mathcal{A}},x_{\mathcal{B}}} \langle\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}| U_{\mathcal{E}}^{\dagger A'^N} U_{\mathcal{N}}^{\dagger} Z^{-x_{\mathcal{A}},-u_{\mathcal{X}},-x_{\mathcal{B}},-x_{\mathcal{Z}}} U_{\mathcal{E}}^{C^N} \Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x_{\mathcal{A}},x_{\mathcal{Z}}} U_{\mathcal{E}}^{\dagger C^N} Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}} U_{\mathcal{N}} U_{\mathcal{E}}^{A'^N} |\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle && (78)
\end{aligned}$$

$$\begin{aligned}
&\mathbb{E}_{U_{\mathcal{X}},X_{\mathcal{Z}}}\left\{\langle\Xi^{\text{ideal}}_{X_{\mathcal{Z}},U_{\mathcal{X}}}|\Xi^{\text{actual}}_{X_{\mathcal{Z}},U_{\mathcal{X}}}\rangle\right\} && (79)\\
&= \frac{1}{2^{|\mathcal{A}|+|\mathcal{B}|+|\mathcal{X}|+|\mathcal{Z}|}} \sum_{x_{\mathcal{A}},x_{\mathcal{B}},u_{\mathcal{X}},x_{\mathcal{Z}}} \langle\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}| U_{\mathcal{E}}^{\dagger A'^N} U_{\mathcal{N}}^{\dagger} Z^{-x_{\mathcal{A}},-u_{\mathcal{X}},-x_{\mathcal{B}},-x_{\mathcal{Z}}} U_{\mathcal{E}}^{C^N} \Gamma^{(x_{\mathcal{B}},u_{\mathcal{X}})}_{x_{\mathcal{A}},x_{\mathcal{Z}}} U_{\mathcal{E}}^{\dagger C^N} Z^{x_{\mathcal{A}},u_{\mathcal{X}},x_{\mathcal{B}},x_{\mathcal{Z}}} U_{\mathcal{N}} U_{\mathcal{E}}^{A'^N} |\Phi_{\mathcal{A},\mathcal{Z},\mathcal{X},\mathcal{B}}\rangle && (80)\\
&\geq 1 - o(2^{-\frac{1}{2}N^{\beta}}), && (81)
\end{aligned}$$

analyzed in (77)-(78). Taking the expectation of this term over a uniformly random choice of $u_{\mathcal{X}}$ and $u_{\mathcal{Z}}$ (which implies a uniformly random choice of $x_{\mathcal{Z}}$) leads to the steps in (79)-(81). The last inequality of this sequence again follows from the performance of the quantum successive cancellation decoder for the phase channels.

REFERENCES

[1] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Transactions on Information Theory*, vol. 55, no. 7, pp. 3051–3073, Jul. 2009. [Online]. Available: http://dx.doi.org/10.1109/TIT.2009.2021379

[2] J. M. Renes and J.-C. Boileau, "Physical underpinnings of privacy," *Physical Review A*, vol. 78, no. 3, p. 032335, Sep. 2008, arXiv:0308.3096. [Online]. Available: http://link.aps.org/abstract/PRA/v78/e032335

[3] ——, "Conjectured strong complementary information tradeoff," *Physical Review Letters*, vol. 103, no. 2, pp. 020 402–4, Jul. 2009, arXiv:0806.3984. [Online]. Available: http://link.aps.org/abstract/PRL/v103/e020402

[4] J.-C. Boileau and J. M. Renes, "Optimal state merging without decoupling," in *Fourth Workshop on Theory of Quantum Computation, Communication, and Cryptography*, ser. Lecture Notes in Computer Science, A. M. Childs and M. Mosca, Eds., vol. 5906. Berlin: Springer Verlag, May 2009, p. 76, 0905.1324. [Online]. Available: http://springerlink.com/content/6765055437786656

[5] J. M. Renes, "Duality of privacy amplification against quantum adversaries and data compression with quantum side information," *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Science*, vol. 467, no. 2130, pp. 1604–1623, Jun. 2011. [Online]. Available: http://rspa.royalsocietypublishing.org/content/467/2130/1604

[6] ——, "Approximate quantum error correction via complementary observables," Mar. 2010, submitted to Physical Review Letters. [Online]. Available: http://arxiv.org/abs/1003.1150

[7] J. M. Renes, F. Dupuis, and R. Renner, "Efficient polar coding of quantum information," *Physical Review Letters*, vol. 109, no. 5, p. 050504, Aug. 2012. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.109.050504

[8] M. M. Wilde and S. Guha, "Polar codes for degradable quantum channels," *arXiv:1109.5346*, Sep. 2011. [Online]. Available: http://arxiv.org/abs/1109.5346

[9] E. Sasoglu, E. Telatar, and E. Arikan, "Polarization for arbitrary discrete memoryless channels," in *IEEE Information Theory Workshop, 2009*. IEEE, Oct. 2009, pp. 144–148. [Online]. Available: http://dx.doi.org/10.1109/ITW.2009.5351487

[10] G. Smith and J. Yard, "Quantum communication with zero-capacity channels," *Science*, p. 1162242, Aug. 2008. [Online]. Available: http://www.sciencemag.org/cgi/content/abstract/1162242v3

[11] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," *IEEE Transactions on Information Theory*, vol. PP, no. 99, p. 1, 2012. [Online]. Available: http://dx.doi.org/10.1109/TIT.2012.2218792

[12] M. M. Wilde, "From classical to quantum Shannon theory," *arXiv:1106.1445*, Jun. 2011. [Online]. Available: http://arxiv.org/abs/1106.1445

[13] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Transactions on Information Theory*, vol. 51, no. 1, p. 44, January 2005, arXiv:quant-ph/0304127.

[14] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Problems of Information Transmission*, vol. 40, no. 4, pp. 318–336, October 2004.

[15] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure key from bound entanglement," *Physical Review Letters*, vol. 94, no. 16, p. 160502, Apr. 2005. [Online]. Available: http://link.aps.org/abstract/PRL/v94/e160502

[16] M. M. Wilde and J. M. Renes, "Polar codes for private classical communication," *arXiv:1203.5794*, Mar. 2012. [Online]. Available: http://arxiv.org/abs/1203.5794

[17] I. Tal and A. Vardy, "How to construct polar codes," *arXiv:1105.6164*, May 2011. [Online]. Available: http://arxiv.org/abs/1105.6164

[18] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, Oct. 2006. [Online]. Available: http://www.sciencemag.org/content/314/5798/436

[19] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," *Physical Review Letters*, vol. 85, no. 2, p. 441, Jul. 2000. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevLett.85.441

[20] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 6428–6443, Oct. 2011. [Online]. Available: http://dx.doi.org/10.1109/TIT.2011.2162275

[21] I. Devetak and P. W. Shor, "The capacity of a quantum channel for simultaneous transmission of classical and quantum information," *Communications in Mathematical Physics*, vol. 256, no. 2, pp. 287–303, Mar. 2005. [Online]. Available: http://www.springerlink.com/content/m446u32w50883272/

[22] E. Arikan and E. Telatar, "On the rate of channel polarization," *arXiv:quant-ph/0807.3806*, Jul. 2008. [Online]. Available: http://arxiv.org/abs/0807.3806