ISIT'2013 1569719933

Efficient Quantum Channel Coding Scheme Requiring No Preshared Entanglement

David Sutter*, Joseph M. Renes*, Frédéric Dupuis*†, and Renato Renner*
*Institute for Theoretical Physics, ETH Zurich, Switzerland
†Department of Computer Science, Aarhus University, Denmark
Email: {suttedav,renes,renner}@phys.ethz.ch, dupuis@cs.au.dk

***Abstract*—We construct an explicit entanglement distillation scheme which achieves the *coherent information* when used to send quantum information over a noisy quantum channel. For Pauli and erasure channels we present efficient encoding and decoding algorithms based on polar codes. Unlike previous constructions, this scheme does not require the sender and receiver to share noiseless entanglement before the protocol begins. It is possible, but still unproven, that the scheme even achieves a rate beyond the coherent information, due to *degeneracies* of certain error correcting codes. Finally we discuss how the scheme can be used for secret key distillation and private channel coding.**

I. Introduction

Shannon's channel coding theorem determines the capacity of a classical discrete memoryless channel W by random coding arguments and finds that it is given by

$$C(\mathsf{W}) = \max_{P_X} I(X:\mathsf{W}(X))\,, \tag{1}$$

where X is a random variable describing the input to the channel and P_X is its probability distribution.

Analogous random coding arguments for the problem of transmitting quantum information over a memoryless quantum channel $\mathcal{N}^{A'\to B}$ lead to a communication rate given by

$$Q_1(\mathcal{N}) := \max_{\phi^{AA'}} I(A\rangle B)_{\mathcal{N}^{A'\to B}(\phi^{AA'})}\,, \tag{2}$$

where $I(A\rangle B)_\rho := H(B)_\rho - H(AB)_\rho$ is the *coherent information* and H the von Neumann entropy [1], [2], [3]. It has been shown that $Q_1(\mathcal{N})$ is not generally optimal [4] and that the quantum capacity is given by its *regularization*

$$Q(\mathcal{N}) = \lim_{k\to\infty} \frac{1}{k} Q_1\big(\mathcal{N}^{\otimes k}\big)\,. \tag{3}$$

Notwithstanding the difficulties surrounding the regularized expression, it is already difficult to construct *explicit* coding schemes that achieve the coherent information of an arbitrary quantum channel, and the task becomes that much harder if we also ask for *efficient* encoding and decoding. Until very recently, essentially nothing was known about explicit, efficient, *provably* capacity-achieving classical error-correcting codes, to say nothing of the quantum case.

Polar codes, introduced in 2008 by Arıkan [5], are the first family of classical error-correcting codes which both provably achieve the *symmetric* ($X \sim$ uniform in (1)) classical capacity for any discrete memoryless channel and have an essentially linear encoding and decoding complexity. These codes have been generalized to the quantum setup. Wilde and Guha adapted polar codes to transmit classical information over quantum channels [6] and gave a scheme for transmitting quantum information over degradable quantum channels [7], at the cost of an unknown decoding efficiency. Three of us showed in [8] how to achieve the *symmetric* coherent information ($\phi^{AA'}$ a Bell state in (2)) of any Pauli or erasure channel with efficient encoding and decoding operations. In [9], Wilde and Renes extended this method to arbitrary quantum channels, but without providing an efficient decoder.

However, all of these quantum error-correcting schemes generally require entanglement-asssistance, i.e., preshared entanglement between the sender and receiver. More details about entanglement-assisted quantum coding can be found in [10]. In this contribution we present an explicit coding scheme that provably achieves the (true) coherent information for an arbitrary quantum channel without using any entanglement assistance. For Pauli or erasure channels, the use of quantum polar codes in our scheme leads to efficient encoding and decoding.

II. Entanglement Distillation

A. Protocol, Rate, and Reliability

Inspired by previous work in a purely classical scenario [11], we consider a concatenated entanglement distillation scheme based on CSS codes. The scheme consists of an inner layer which performs error-correction—more correctly, information reconciliation (IR)—in the amplitude, or Z-basis and an outer layer which performs information reconciliation in the phase, or X-basis. Each layer utilizes a quantum stabilizer code and together the amplitude and phase codes form a CSS quantum error-correcting code. Information reconciliation at the inner layer is performed on M independent blocks, each consisting of L input systems. The unmeasured qubits after the amplitude information reconciliation are forwarded to the phase information reconciliation block. Due to this two-level structure the scheme has a blocklength $N = LM$. Letting K denote the number of unmeasured outputs per amplitude block, Figure 1 depicts the case $L = 4$, $M = 2$, and $K = 2$.

To explain the scheme in more detail, we start with a single bipartite system ψ^{AB} shared by Alice and Bob, with A a qubit.

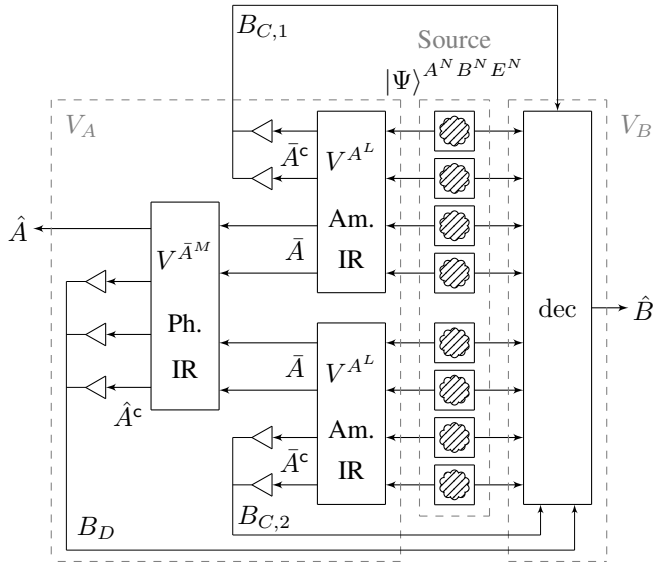

Fig. 1. The entanglement distillation scheme for $L = 4$, $M = 2$ and $K = 2$. Alice performs M times an amplitude IR transformation, measures part of the output with respect to the amplitude basis and sends the outcomes to Bob. The non-measured qubits are applied to an IR operation in the complementary phase basis and part of the outcome is again measured and sent to Bob. Using Alice's classical information, Bob runs a decoder such that his and Alice's outcome—described by the systems $\hat{A}$ and $\hat{B}$—are a good approximation to maximally entangled qubits.

Purifying ψ^{AB} and expressing A in the amplitude basis gives

$$|\psi\rangle^{ABE} = \sum_{z\in\{0,1\}} \sqrt{p_z}\,|z\rangle^A\,|\varphi_z\rangle^{BE}\,, \tag{4}$$

where p_z is some probability distribution and $\{|\varphi_z\rangle^{BE}\}$ some set of normalized states, not necessarily orthogonal. The input to each block of the first layer will be the state

$$|\Psi\rangle^{A^L B^L E^L} = \left(|\psi\rangle^{ABE}\right)^{\otimes L}. \tag{5}$$

The amplitude stabilizer code is chosen so that Bob can determine z^L, with probability exceeding $1-\epsilon_1$ using his systems B^L if he is also supplied with the syndromes of the code. These are determined by Alice and transmitted to him over a public classical channel. Given a particular z^L, denote by $\bar{z}^{\mathsf{c}}$ the syndrome and $\bar{z}$ the encoded information. Since stabilizer codes are linear codes, z^L determines $(\bar{z},\bar{z}^{\mathsf{c}})$ and *vice versa*. Moreover, for every stabilizer code on L systems there exists a unitary operation which maps the stabilizer and encoded operators to physical qubits. Call this unitary V^{A^L}; after applying it, Alice need only measure certain subsystems to generate the syndrome. Let $\bar{A}^{\mathsf{c}}$ be the systems which are then measured to yield the syndromes and $\bar{A}$ the remaining systems (corresponding to encoded qubits). After applying the unitary, the joint state becomes

$$|\Psi_1\rangle^{A^L B^L E^L} = V^{A^L}\,|\Psi\rangle^{A^L B^L E^L} \tag{6}$$

$$= \sum_{(\bar{z},\bar{z}^{\mathsf{c}})\in\{0,1\}^L} \sqrt{p_{z^L}(\bar{z},\bar{z}^{\mathsf{c}})}\,|\bar{z}\rangle^{\bar{A}}\,|\bar{z}^{\mathsf{c}}\rangle^{\bar{A}^{\mathsf{c}}}\left|\varphi_{z^L}(\bar{z},\bar{z}^{\mathsf{c}})\right\rangle^{B^L E^L}. \tag{7}$$

Sending $\bar{z}^{\mathsf{c}}$ to Bob can be modeled as copying $\bar{z}^{\mathsf{c}}$ to a register B_C he controls, plus another one for the environment, E_C:

$$|\Psi_2\rangle^{A^L B^L B_C E^L E_C} = \sum_{(\bar{z},\bar{z}^{\mathsf{c}})\in\{0,1\}^L} \sqrt{p_{z^L}}\,|\bar{z}\rangle^{\bar{A}}\,|\bar{z}^{\mathsf{c}}\rangle^{\bar{A}^{\mathsf{c}}}|\bar{z}^{\mathsf{c}}\rangle^{B_C}|\bar{z}^{\mathsf{c}}\rangle^{E_C}|\varphi_{z^L}\rangle^{B^L E^L}. \tag{8}$$

After Bob applies his decoding operation, he has a perfect copy of $\bar{z}$ as well, at least to the extent that ϵ_1 is near zero, which also implies that the state $|\varphi_{z^L}\rangle$ after the measurement does only change by an amount that is vanishing for $\epsilon_1 \to 0$. Thus, after the encoding and decoding associated with the first layer, the joint state is

$$|\Psi_3\rangle^{A^L B^L C^L E^L E_C} \approx_{\epsilon_1} \sum_{z^L\in\{0,1\}^L} \sqrt{p_{z^L}}\left|z^L\right\rangle^{A^L}\left|z^L\right\rangle^{C^L}|\varphi_{z^L}\rangle^{B^L E^L}\left|\bar{z}^{\mathsf{c}}(z^L)\right\rangle^{E_C}, \tag{9}$$

where now Bob's system C^L contains a full, coherent copy of z^L (and thus can absorb the system B_C). This approximation can be made precise in terms of ϵ_1 using the fidelity [12].

The outer layer performs phase information reconciliation on M instances of the $\bar{A}$ systems of the state $|\Psi_3\rangle$, where Bob's side information is given by $B^L C^L$ in each instance. In contrast to the inner layer, here the information to be reconciled is not a bit, but a sequence of bits. Therefore, to use the formalism of stabilizer codes, we either need to consider codes over larger dimension or multilevel coding schemes. Either would work for our purposes, but for concreteness let us opt for the latter. Thus, Alice and Bob sequentially run blocksize-M phase IR protocols on each of the qubits in system $\bar{A}$, treating already completed qubits as side information.

Ultimately the effect of this procedure can be regarded, as at the inner layer, as applying a unitary $V^{\bar{A}^M}$ and measuring a subset of the output qubits to obtain the syndromes. These measurement results are sent to Bob, which is modeled as copying them to a register B_D he controls, plus another one for the environment E_D. Remaining at the end of this process are a set of unmeasured qubits, the encoded qubits $\hat{A}$ of the error-correcting code used in phase information reconciliation.

In the following, we describe the above protocol in more detail. Associated with any set of qubits are a set of X and Z operators acting on these qubits; abusing notation, let us refer to the entire collection of these by, for instance, $X^{\bar{A}}$ and $Z^{\bar{A}}$ for the set $\bar{A}$. The predictability of an observable Z^{A^L} given measurement of some system B^L can be expressed by

$$p_{\text{guess}}\left(Z^{A^L}|B^L\right)_\Psi := \max_{\mathcal{M}_{Z^L}} \sum_{z\in\{0,1\}^L} p_{z^L}\,\mathrm{Tr}\left[\Lambda^{B^L}_{z^L}\varphi^{B^L}_{z^L}\right], \tag{10}$$

where the maximum is taken over all measurements $\mathcal{M}_{Z^L}$ with elements $\Lambda^{B^L}_{z^L}$. In the following we will use the error probability instead of the guessing probability which is defined as $p_{\text{err}}(Z^{A^L}|B^L)_\Psi := 1 - p_{\text{guess}}(Z^{A^L}|B^L)_\Psi$.

The amplitude IR protocol is chosen to be ϵ_1-good, i.e., $p_{\text{err}}(Z^{A^L}|B^L B_C)_{\Psi_2} \leq \epsilon_1$. Since the scheme uses M independent amplitude information reconciliation blocks, we can

use the union bound to write

$$p_{\text{err}}\left(Z^{A^N}|B^N B_C^M\right)_{\Psi_2^{\otimes M}} \leq M\epsilon_1. \tag{11}$$

Sidestepping the details of the multilevel coding for the moment, the phase IR protocol is chosen to have

$$p_{\text{err}}\left(X^{\bar{A}^M}|B^N C^N B_D\right) \leq \epsilon_2. \tag{12}$$

Clearly $X^{\hat{A}}$ (cf. Figure 1) is a deterministic function of $X^{\bar{A}^M}$ due to the action of $V^{\bar{A}^M}$. However, since this unitary implements a linear function in the basis conjugate to the amplitude observable $Z^{\bar{A}^M}$, it also implements a linear function in the amplitude basis itself. (This fact was used to show that Arıkan's polar encoding circuit is directly useful in the quantum setting in [8].) Therefore, $Z^{\hat{A}}$ is a deterministic function of $Z^{\bar{A}^M}$ and hence also of Z^{A^N}. Put differently, since both layers are built from linear error-correcting codes, we have constructed a CSS quantum error-correcting code, for which this property holds. Thus, we have

$$p_{\text{err}}\left(X^{\hat{A}}|B^N C^N B_D\right) \leq \epsilon_2 \quad \text{and} \tag{13}$$

$$p_{\text{err}}\left(Z^{\hat{A}}|B^N B_C^M\right) \leq M\epsilon_1. \tag{14}$$

These conditions ensure Alice and Bob share a good approximation to $|\hat{A}|$ maximally entangled qubit pairs. Alice's part of the distillation process (as described above) can be described by a unitary $U_A^{A^N \to \hat{A}B_C^M B_D E_C^M E_D}$. Bob's part is to decode the state $|\Psi\rangle^{A^N B^N E^N}$ using B^N and the side information $B_C^M B_D$ he receives from Alice. Inequalities (13) and (14) together with [13, Theorem 1] ensure that there exists a decoding unitary $U_B^{B^N B_C^M B_D \to \hat{B}}$. It is constructed from the two IR decoders.

To make the reliability statement precise, define $V_A := U_A^{A^N \to \hat{A}B_C^M B_D E_C^M E_D}$, $V_B := U_B^{B^N B_C^M B_D \to \hat{B}}$, and introduce

$$\mathcal{E}(\cdot) := \text{Tr}_{E_C^M E_D E^N}[V_B(V_A(\cdot)V_A^\dagger)V_B^\dagger]. \tag{15}$$

Proposition 1. *Let $|\phi\rangle_d^{\hat{A}\hat{B}}$ be a maximally entangled state of dimension d, where $d = \dim \hat{A}$. Then*

$$\delta\left(|\phi\rangle_d^{\hat{A}\hat{B}}, \mathcal{E}\left(\Psi^{A^N B^N E^N}\right)\right) \leq \sqrt{2\epsilon_2} + \sqrt{2M\epsilon_1}. \tag{16}$$

Theorem 2. *The rate of the scheme is*

$$R = \frac{1}{L}\left(I(\bar{A}\rangle B^L C^L)_{\Psi_3'} + o(L)\right), \tag{17}$$

where

$$|\Psi_3'\rangle = \sum_{(\bar{z},\bar{z}^{\mathsf{c}})\in\{0,1\}^L} \sqrt{p_{z^L}}\,|\bar{z}\rangle^{\bar{A}}|\bar{z}^{\mathsf{c}}\rangle^{\bar{A}^{\mathsf{c}}}|\varphi_{z^L}\rangle^{B^L E^L}|z^L\rangle^{C^L} \tag{18}$$

and z^L is a function of the pair $(\bar{z}, \bar{z}^{\mathsf{c}})$.

Corollary 3. *For ψ as given in* (4)*, we have $R \geq I(A\rangle B)_\psi$.*

Proof of Proposition 1, Theorem 2, and Corollary 3: See [14]. ∎

B. Using Quantum Polar Codes for Pauli or Erasure Channels

By using polar codes, Alice and Bob can perform the above operations in a computationally efficient manner for states $|\psi\rangle^{ABE}$ that arise from sending half of an entangled pair through a Pauli or erasure channel.

Code Construction.— Before the protocol starts one must construct the code, i.e., determine the qubits comprising the systems $\bar{A}^{\mathsf{c}}$ at the inner layer and $\hat{A}^{\mathsf{c}}$ at the outer layer. (Recall that these are the qubits that are measured by Alice its outcome is sent to Bob.) Constructing the system $\bar{A}^{\mathsf{c}}$ can be approximately done in linear time using Tal and Vardy's algorithm [15] and its adaptation to an asymmetric setup as explained in [16] or alternatively using the more recent algorithm by Tal *et al.* [17].

To determine the system $\hat{A}^{\mathsf{c}}$ requires more effort. Applying the above algorithm for a "super-source" seen by the outer layer will not be efficient in the overall blocklength N since its alphabet size is exponential in L. Nonetheless, due to the structure of the inner layer, it is perhaps possible that the method of approximation by limiting the alphabet size [15], [17] can be extended to this case.

Encoding.—As described in Section II-A and Figure 1, starting with a state $|\Psi\rangle^{A^N B^N E^N}$, Alice first applies M times a unitary V^{A^L} to perform amplitude information reconciliation, which is in the specific case of using quantum polar codes $V^{A^L} = \sum_{z^L\in\{0,1\}^L} \left|G_{\log L} z^L\right\rangle\left\langle z^L\right|$, where $G_{\log L} = G^{\otimes L}$ with $G = \left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ denotes the Arıkan or polar transform [5]. Alice measures the frozen qubits with respect to the amplitude basis and sends the outcome to Bob.

Alice next applies another polar transform $V^{\bar{A}^M}$—this time with respect to the phase basis—to the M systems $\bar{A}$. The frozen qubits are measured with respect to the phase basis and its outcomes are sent again to Bob. The remaining qubits form the system $\hat{A}$.

Decoding.—Decoding of the B^N system, with the additional information stored in the $B_C^M B_D$ registers, can be done by combining ideas from [13] and [8]. Bob's operation is constructed by using the classical polar decoders for amplitude and phase IR in sequence. Note however that these two decoding tasks are not indepent as this would neglect possible correlations between amplitude and phase.

In the first step Bob performs the amplitude IR decoding operation $\mathcal{D}_A$ (M times), which corresponds to the standard classical polar decoder as introduced in [5], and stores the result in an auxiliary system F_i, $i \in \{1, \ldots, M\}$. Each instance of $\mathcal{D}_A$ requires the corresponding frozen information, the values $\bar{z}^{\mathsf{c}}$, which is provided in B_C^M.

Bob next performs the phase IR decoding operation $\mathcal{D}_P$, using the information gained from decoding the first layer. This corresponds to the classical polar decoder in a concatenated scenario introduced in [11]. Bob therefore needs to know the frozen bits $\hat{x}^{\mathsf{c}}$, given in B_D.

Proposition 4. *Encoding and decoding of the distillation scheme can be done with $O(N \log N)$ steps.*

Proof: See [14]. ∎

When using quantum polar codes for Pauli or erasure channels we can derive explicit expressions for ϵ_1 and ϵ_2 and hence make a precise statement about the reliability of the distillation scheme.

Corollary 5. *The reliability of the scheme introduced above for Pauli and erasure channels and the use of quantum polar codes is as given in Proposition 1 with* $\epsilon_1 = O(2^{-L^\beta})$ *and* $\epsilon_2 = O(L2^{-M^{\beta'}})$ *for any* $\beta, \beta' < \frac{1}{2}$.

Proof: See [14]. ∎

III. Channel Coding

Bennett *et al.* [18] showed that any entanglement distillation scheme can be turned into a channel coding scheme. We consider a channel coding scheme that uses classical-assistance as depicted schematically in Figure 2. Before applying the actual encoding transformation, the outer encoder adds redundancy in form of random qubits which are sent to the decoder. As explained in the entanglement distillation scheme in the previous section, we know that after the inner layer the state is perfectly known with respect to the amplitude basis. Therefore, we can choose the additional qubits at random in the complementary phase basis.

The inner encoder also adds redundancy. The additional qubits are generated as explained in [11, Section II] and sent to the decoder, before applying the actual encoding transform. The encoded data is then transmitted over N identical channels $\mathcal{N}$. The decoding is identical to the Bob's task in the entanglement distillation scenario, explained in Section II.

For the code construction, the set of frozen qubits (the indices sets which determine at which position the redundant qubits are added) at the outer and inner layer have to be determined, that is explained in Section II-B.

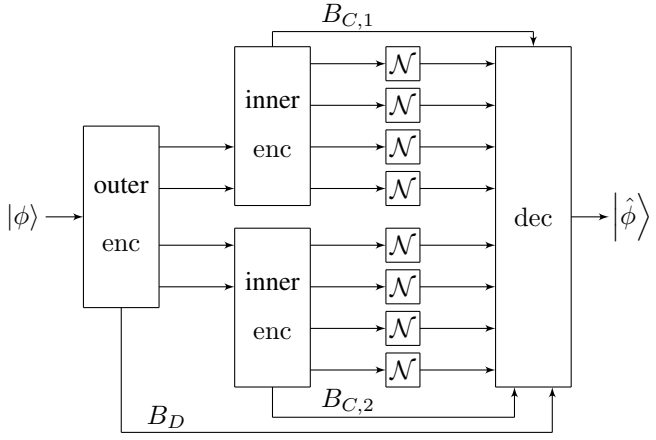

Fig. 2. The channel coding view of the scheme for $L = 4$, $M = 2$ and $K = 2$. The outer encoder encoder adds randomly generated qubits, which are forwarded to the decoder, before applying the actual encoding transform. At the inner layer the encoder mimics the extra qubits as explained in [11, Section II] and sends them to the decoder as well. The decoding is analogously as for the entanglement distillation setup explained in Section II.

Corollary 6. *For Pauli and erasure channels and the use of polar codes, there exists an encoder and a decoder for the scheme described above that have* $O(N \log N)$ *complexity.*

Proof: See [14]. ∎

The reliability of the efficient encoder and decoder introduced above is an immediate consequence of Proposition 1.

Corollary 7. *The trace distance between the state produced by the decoder and the ideal, maximally entangled state is less than* $\sqrt{2\epsilon_2} + \sqrt{2M\epsilon_1}$ *where* $\epsilon_1 = O(2^{-L^\beta})$, $\epsilon_2 = O(L2^{-M^{\beta'}} + L2^{-\frac{1}{2}L^{\beta''}})$ *for* $\beta, \beta', \beta'' < \frac{1}{2}$.

Corollary 3 shows that the scheme achieves the coherent information. However, were the inequality in Corollary 3 not tight, the scheme could achieve a higher rate.

Question. Is $R > 0$ such that $R > I(A\rangle B)_\psi$ possible?

There are several ways to phrase the question above differently (cf. [14]). The following Proposition leads to a particularly clean reformulation.

Proposition 8. *The rate given in* (17) *can be written as*

$$R = -H(A|B)_\psi + H\left(Z^A|B\right)_\psi - \tfrac{1}{L} H\left(Z^{\bar{A}^c}\middle|E^L\right)_{\Psi'_3}. \quad (19)$$

Proof: See [14]. ∎

Question. Is $\lim_{L\to\infty} \frac{1}{L} H(Z^{\bar{A}^c}|E^L)_{\Psi'_3} < \lim_{L\to\infty} \frac{1}{L}|\bar{A}^c|$ for $R > 0$ possible?

Considering degradable channels as a sanity check, we obtain $H(Z^{\bar{A}^c}|E^L)_{\Psi'_3} \geq H(Z^{\bar{A}^c}|B^L)_{\Psi'_3} = LH(Z^A|B)_\psi + o(L)$, where the last step follows from the polarization phenomenon [19, Theorem 1]. Using (19), we obtain for sufficiently large L, that $R \leq I(A\rangle B)_\psi$. This is in agreement with the known result that for *degradable* channels the coherent information is optimal [20].

IV. Secret Key Distillation and Private Channel Coding

With minor changes, the above entanglement distillation scheme also works for secret key distillation. Consider the scenario in which Alice and Bob share an additional "shield" system S [21], [12]. A shield is any system not held by the eavesdropper Eve but nevertheless cannot be used for amplitude IR by Alice and Bob, where the amplitude information is used to create the secret key. One can show that

$$p_{\text{err}}\left(X^{\hat{A}}|B^N C^N B_D S\right) \leq \epsilon_2 \quad \text{and} \quad (20)$$

$$p_{\text{err}}\left(Z^{\hat{A}}|B^N B_C^M\right) \leq M\epsilon_1, \quad (21)$$

characterizes a state where $Z^{\hat{A}}$ can be used as a secret key.

Due to the uncertainty principle, the secrecy of the amplitude information from Eve is ensured if Alice and Bob could implement phase IR.

An observable Z^A is approximately secure if the trace distance to the ideal case is small. Thus for $\psi^S = \text{Tr}_A[\psi^{AS}]$,

we introduce $p_{\text{secure}}\left(Z^A|S\right) := \frac{1}{2}\left\|\psi^{AS} - \frac{1}{d}\mathbb{1}\otimes\psi^S\right\|_1$, where $\left\|M\right\|_1 := \text{Tr}[\sqrt{M^\dagger M}]$.

Corollary 9. *Inequality* (20) *implies*

$$p_{\text{secure}}\left(Z^{\hat{A}}\middle|E^N E_C^M E_D\right) \leq \sqrt{2M\epsilon_1}. \tag{22}$$

Proof: See [14]. ∎

As mentioned above the secret key distillation scheme is very similar to the entanglement distillation scheme introduced in Section II. More precisely, Alice's first task, i.e., the M amplitude information reconciliation blocks are identical as in the entanglement distillation. The phase IR step is slightly different as one has to consider side information S, which leads to a different set of frozen qubits. Furthermore, Alice keeps the outcomes from measuring $\hat{A}^{\mathsf{c}}$ secret from Eve, i.e., she does not send them to Bob. Alice's task thus can be done with $O(N\log N)$ complexity as proven in Proposition 4.

Bob's task is also similar to the decoding he performs in the entanglement distillation setup. He first decodes the amplitude Z^{A^N}, which can be done with a standard classical polar decoder. He next computes the value of $Z^{\hat{A}}$ using the details of the phase IR code. Hence Bob's decoding operation has $O(N\log N)$ complexity.

The reliability and secrecy are as given in Proposition 1 and Corollary 9 with $\epsilon_1 = O(2^{-L^\beta})$ and $\epsilon_2 = O(L2^{-M^{\beta'}})$ for any $\beta, \beta' < \frac{1}{2}$.

The rate for this scenario can be computed analogously as in Section II-A, which leads to

$$\begin{aligned} R &\geq 1 - H\big(Z^A|B\big) - H\big(X^A|BCS\big) && (23)\\ &= H\big(Z^A|E\big) - H\big(Z^A|B\big). && (24)\end{aligned}$$

The equality step uses the exact uncertainty relation introduced in [22], which ensures that $H(Z^A|E)_\psi + H(X^A|BCS)_\psi = 1$. Note that we no longer obtain the coherent information $-H(A|B)_\psi$, since E no longer purifies AB. The reliability of the secret key distillation scheme is analogous to that of the entanglement distillation scheme (cf. Proposition 1).

The secret key distillation scheme described above also works in a purely classical setup, since the phase IR protocol can be turned into a privacy amplification protocol needing only classical operations [23].

Moreover, the quantum coding scheme can be used for efficient private channel coding at a high rate (as given in (23) and (24)). As in Section III, the idea is to run key distillation in reverse, simulating the measurement outputs with appropriately-chosen random intputs. These are then the frozen bits. The frozen bits of the inner and outer encoder can be sent over an insecure channel to Bob, since privacy is ensured by the outer layer whose frozen bits are uncorrelated to the message bits since the corresponding protocol produces entanglement.

V. Conclusion

We have constructed a protocol that can be used to perform reliable entanglement distillation or quantum communication at a rate equal to (or possibly larger than) the coherent information. Compared to previous work in this area, our scheme does not require any preshared entanglement and achieves the coherent information also for asymmetric channels (where $\phi^{AA'}$ in (2) is not necessarily a Bell state). When communicating over a Pauli or erasure channel using polar codes, encoding and decoding can be performed with a number of operations essentially linear in the blocklength. We have also shown how the protocol can be modified for efficient, high-rate secret key distillation and private channel coding.

References

[1] S. Lloyd, "Capacity of the noisy quantum channel," *Phys. Rev. A*, vol. 55, no. 3, pp. 1613–1622, 1997.

[2] P. W. Shor, "The quantum channel capacity and coherent information." Presented at the MSRI Workshop on Quantum Computation, 2002.

[3] I. Devetak, "The private classical capacity and quantum capacity of a quantum channel," *IEEE Trans. on Inf. Theory*, vol. 51, no. 1, pp. 44–55, 2005.

[4] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, "Quantum-channel capacity of very noisy channels," *Phys. Rev. A*, vol. 57, pp. 830–839, Feb 1998.

[5] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels," *IEEE Trans. on Inf. Theory*, vol. 55, pp. 3051 –3073, Jul 2009.

[6] M. M. Wilde and S. Guha, "Polar codes for classical-quantum channels," *IEEE Trans. on Inf. Theory*, vol. 59, pp. 1175 –1187, Feb 2013.

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

[8] J. M. Renes, F. Dupuis, and R. Renner, "Efficient polar coding of quantum information," *Phys. Rev. Let.*, vol. 109, p. 050504, Aug 2012.

[9] M. M. Wilde and J. M. Renes, "Quantum polar codes for arbitrary channels," *Proceedings IEEE ISIT*, pp. 334 –338, Jul 2012.

[10] T. Brun, I. Devetak, and M.-H. Hsieh, "Correcting quantum errors with entanglement," *Science*, vol. 314, no. 5798, pp. 436–439, 2006.

[11] D. Sutter, J. M. Renes, F. Dupuis, and R. Renner, "Achieving the capacity of any DMC using only polar codes," *Proceedings IEEE ITW*, pp. 114 –118, Sep 2012. extended version available at arXiv:1205.3756.

[12] J. M. Renes and J.-C. Boileau, "Physical underpinnings of privacy," *Phys. Rev. A*, vol. 78, p. 032335, Sep 2008.

[13] J. M. Renes, "Approximate quantum error correction via complementary," 2012. available at arXiv:1003.1150.

[14] An extended version of this paper containing all the proofs will be submitted as soon as possible to the arXiv. Available at http://www.phys.ethz.ch/~suttedav/ISIT2013/LongVersion.

[15] I. Tal and A. Vardy, "How to construct polar codes," 2011. available at arXiv:1105.6164.

[16] J. Honda and H. Yamamoto, "Polar coding without alphabet extension for asymmetric channels," *Proceedings IEEE ISIT*, pp. 2147 –2151, Jul 2012.

[17] I. Tal, A. Sharov, and A. Vardy, "Constructing polar codes for non-binary alphabets and macs," *Proceedings IEEE ISIT*, pp. 2132 –2136, july 2012.

[18] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, no. 5, pp. 3824–3851, 1996.

[19] E. Arıkan, "Source polarization," *Proceedings IEEE ISIT*, pp. 899 –903, Jun 2010.

[20] 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, pp. 287–303, 2005.

[21] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure key from bound entanglement," *Phys. Rev. Let.*, vol. 94, pp. 160502–4, Apr 2005.

[22] J. M. Renes and J.-C. Boileau, "Conjectured strong complementary information tradeoff," *Phys. Rev. Let.*, vol. 103, p. 020402, Jul 2009.

[23] D. Sutter, J. M. Renes, and R. Renner, "Efficient one-way secret-key agreement and private channel coding via polarization," 2013. available at arXiv:1304.3658.