Entanglement generation with a quantum channel and a shared state

Mark M. Wilde and Min-Hsiu Hsieh

***Abstract*—We introduce a new protocol, the channel-state coding protocol, to quantum Shannon theory. This protocol generates entanglement between a sender and receiver by coding for a noisy quantum channel with the aid of a noisy shared state. The mother and father protocols arise as special cases of the channel-state coding protocol, where the channel is noiseless or the state is a noiseless maximally entangled state, respectively. The channel-state coding protocol paves the way for formulating entanglement-assisted quantum error-correcting codes that are robust to noise in shared entanglement. Finally, the channel-state coding protocol leads to a Smith-Yard superactivation, where we can generate entanglement using a zero-capacity erasure channel and a non-distillable bound entangled state.**

***Index Terms*—channel-state coding protocol, superactivation, mother protocol, father protocol**

I. Introduction

Quantum Shannon theory is the study of the ultimate capability of a noisy quantum system to preserve correlations [1], [2]. A noisy quantum channel possesses various capacities: its quantum capacity governs its ability to transmit quantum information [3], [4], [5], its classical capacity governs its ability for noiseless classical communication [6], [7], and its private capacity governs its ability for noiseless private communication [5], [8]. A noisy bipartite state possesses various distillation yields. Its distillable entanglement determines the amount of maximal entanglement that we can recover from it [9], [10], [11]. Its distillable secret key determines its private correlations [10], [11], and its distillable common randomness determines its classical correlations [12].

In their pioneering unification of quantum Shannon theory [13], [1], Devetak *et al*. formulated the mother and father protocols. The mother protocol exploits a noisy bipartite state and noiseless quantum communication to establish noiseless entanglement between two parties. The father protocol exploits a noisy quantum channel and noiseless entanglement to transmit noiseless quantum information from a sender to a receiver. Since this work, various authors have unified quantum Shannon theory in other ways [14], [15], [16], [17].

In this paper, we introduce a new protocol, the *channel-state coding protocol*, that exploits both a noisy bipartite state and a noisy quantum channel to establish noiseless entanglement between two parties. In the operation of the independent and identically distributed (IID) version of the protocol, we assume that the sender and receiver use the channel and the state *the same number of times*. One might think that the optimal strategy is one of the following three strategies:

1) Distill entanglement from the state and generate entanglement with a quantum channel code. The total entanglement generated is then the sum of the distilled entanglement and the entanglement generated from the channel.
2) Distill entanglement and perform the father protocol if enough entanglement is available. The amount of entanglement generated is the net amount that the father protocol can generate.
3) Perform quantum channel coding and follow with the mother protocol if enough quantum communication is available. The amount of entanglement generated is the net amount that the mother protocol can generate.

It turns out that none of the above strategies is the best strategy. The channel-state coding protocol is the best strategy here and instead encodes both the input to the quantum channel and a share of the noisy bipartite state.

The existence of the channel-state coding protocol has some interesting ramifications. First, it addresses a practical concern for the theory of entanglement-assisted coding [18], where a sender exploits noiseless entanglement and a noisy quantum channel to transmit quantum information. It is conjectured, but not yet demonstrated, that the performance of an entanglement-assisted code decreases dramatically if the entanglement is not perfect. The channel-state coding protocol demonstrates that another strategy other than entanglement-assisted coding is appropriate for this situation. In fact, the motivation for the channel-state coding protocol was the discovery of an entanglement-assisted code that corrects errors on both the sender's transmitted qubits and the receiver's share of the entanglement [19]. Secondly, the mother and father protocols now arise as a special case of the channel-state coding protocol. The mother arises when the quantum channel that connects sender to receiver is a perfect quantum channel. The father arises when the shared entanglement between sender and receiver is perfect. Finally, it leads to another instance of the superactivation effect [20], [21], [22]. Specifically, we can apply the Smith-Yard superactivation [20] to show that it is possible to establish entanglement using a quantum channel with zero capacity and a noisy bipartite state with zero distillable entanglement.

We structure this paper as follows. We first outline a general channel-state coding protocol. Section III gives the proof of the channel-state coding capacity theorem. This theorem determines the ultimate rate at which a noisy quantum channel

Mark M. Wilde was with the Electronic Systems Division, Science Applications International Corporation, 4001 North Fairfax Drive, Arlington, Virginia, USA 22203 when conducting this research, but is now a postdoctoral fellow with the School of Computer Science at McGill University. Min-Hsiu Hsieh is with the ERATO-SORST Quantum Computation and Information Project, Japan Science and Technology Agency 5-28-3, Hongo, Bunkyo-ku, Tokyo, Japan(E-mail: mark.wilde@mcgill.ca and minhsiuh@gmail.com)

978-1-4244-7892-7/10/$26.00 ©2010 IEEE

and a noisy state can generate maximal entanglement. We then show how a special case of this protocol, doing quantum channel coding and entanglement distillation, is inferior to the channel-state coding protocol. Section V shows how the father and mother protocol are special cases of the channel-state coding protocol. We then show how it is possible to obtain a Smith-Yard-like superactivation in the channel-state coding protocol and conclude with some observations and open questions.

II. Channel-State Coding Protocol

We begin by defining our channel-state coding protocol for a quantum channel $\mathcal{N}^{A_1'\rightarrow B_1}$ and a noisy bipartite state $\rho^{A_2B_2}$. The noisy quantum channel $\mathcal{N}^{A_1'\rightarrow B_1}$ connects a sender Alice to a receiver Bob, and Alice and Bob share the noisy state $\rho^{A_2B_2}$ before the protocol begins. The channel has an extension to an isometry $U_{\mathcal{N}}^{A_1'\rightarrow B_1E_1}$, defined on a bipartite quantum system B_1E_1. Bob has access to system B_1 and Eve has access to system E_1. The noisy state admits a purification $\psi^{A_2B_2E_2}$ where Eve shares a purifying system E_2.

We appeal to the asymptotic setting where Alice and Bob have access to n independent uses of the channel $\mathcal{N}^{A_1'\rightarrow B_1}$ and n copies of the bipartite state $\rho^{A_2B_2}$ (where n is as large as we need it to be). We denote the n independent uses of the channel as

$$\mathcal{N}^{A_1'^n\rightarrow B_1^n}\equiv(\mathcal{N}^{A_1'\rightarrow B_1})^{\otimes n},$$

and the n copies of the bipartite state $\rho^{A_2B_2}$ as

$$\rho^{A_2^nB_2^n}\equiv(\rho^{A_2B_2})^{\otimes n}.$$

Let $U_{\mathcal{N}}^{A_1'^n\rightarrow B_1^nE_1^n}$ and $\psi^{A_2^nB_2^nE_2^n}$ similarly denote the n^{th} extensions of the respective isometry $U_{\mathcal{N}}^{A_1'\rightarrow B_1E_1}$ and purification $\psi^{A_2B_2E_2}$.

Alice's task is to generate noiseless entanglement between her and Bob by using the channel $\mathcal{N}^{A_1'^n\rightarrow B_1^n}$ and the noisy state $\rho^{A_2^nB_2^n}$. At the end of the protocol, the generated entanglement should be close to the following state:

$$|\Phi\rangle^{AB}\equiv\frac{1}{\sqrt{D}}\sum_{i=1}^{D}|i\rangle^{A}|i\rangle^{B},\qquad(1)$$

where D indicates the amount of entanglement generated so that the rate of entanglement generation is $R\equiv\log(D)/n$. We allow the free use of a forward classical channel from Alice to Bob.

An (n,R,ϵ) *channel-state code* consists of three steps: preparation, transmission, and channel decoding. We detail each of these steps below.

Preparation. Alice possesses her share of the noisy bipartite state $\rho^{A_2^nB_2^n}$ with purification $\psi^{A_2^nB_2^nE_2^n}$. Alice employs a preparation map $\mathcal{P}^{A_2^n\rightarrow A_1^nA_2^nA_1'^n}$ that prepares the following state for input to the channel:

$$\omega^{A_1^nA_2^nA_1'^nB_2^nE_2^n}\equiv\mathcal{P}^{A_2^n\rightarrow A_1^nA_2^nA_1'^n}(\psi^{A_2^nB_2^nE_2^n}),$$

where A_1^n and A_2^n are systems with the same respective dimension as the input to the channel and Alice's share of the state.

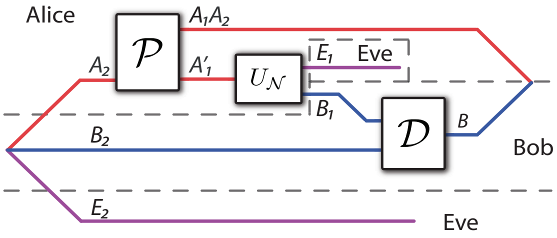

Fig. 1. (Color online) The most general protocol for generating entanglement with a noisy state $\rho^{A_2B_2}$ and a noisy channel $\mathcal{N}^{A_1'\rightarrow B_1}$. It is implicit in the above diagrams that the systems A_1, A_1', B_1, E_1, A_2, B_2, E_2 are actually the respective n-copy systems A_1^n, $A_1'^n$, B_1^n, E_1^n, A_2^n, B_2^n, E_2^n. A good protocol generates the maximally-entangled state Φ^{AB} shared between Alice and Bob.

Transmission. Alice sends the $A_1'^n$ system of the state $\omega^{A_1^nA_2^nA_1'^nB_2^nE_2^n}$ through the channel $U_{\mathcal{N}}^{A_1'^n\rightarrow B_1^nE_1^n}$. This transmission generates the state

$$\omega^{A_1^nA_2^nB_1^nE_1^nB_2^nE_2^n}\equiv U_{\mathcal{N}}^{A_1'^n\rightarrow B_1^nE_1^n}(\omega^{A_1^nA_2^nA_1'^nB_2^nE_2^n}).\qquad(2)$$

Channel Decoding. Bob receives the above state from the channel and performs a decoding map $\mathcal{D}^{B_1^nB_2^n\rightarrow B}$ resulting in the state

$$(\omega')^{A_1^nA_2^nBE_1^nE_2^n}\equiv\mathcal{D}^{B_1^nB_2^n\rightarrow B}(\omega^{A_1^nA_2^nB_1^nE_1^nB_2^nE_2^n}).\qquad(3)$$

The ideal state after Bob's decoding map is close in trace distance to the following product state:

$$\Phi^{AB}\otimes\sigma^{E_1^nE_2^n},$$

where Φ^{AB} is the state in (1), the subspaces of the systems $A_1^nA_2^n$ in which the entanglement is encoded are isomorphic to system A (Alice can perform some isometry to map between these spaces), and $\sigma^{E_1^nE_2^n}$ is some constant state on Eve's systems $E_1^nE_2^n$. The criterion for a successful channel-state code is that

$$\left\|(\omega')^{A_1^nA_2^nBE_1^nE_2^n}-\Phi^{AB}\otimes\sigma^{E_1^nE_2^n}\right\|_1\leq\epsilon,$$

where $\epsilon>0$. Figure 1 depicts all of the above steps in a general channel-state coding protocol.

III. The Channel-State Capacity Theorem

A rate R is *achievable* if there exists an $(n,R-\delta,\epsilon)$ channel-state code for any $\epsilon,\delta>0$ and sufficiently large n.

Theorem 1: The entanglement generation capacity $E(\mathcal{N}\otimes\rho)$ of a quantum channel $\mathcal{N}$ and a bipartite state ρ is

$$E(\mathcal{N}\otimes\rho)=\lim_{l\rightarrow\infty}\frac{1}{l}E^{(1)}(\mathcal{N}^{\otimes l}\otimes\rho^{\otimes l}),\qquad(4)$$

where the "one-shot" capacity $E^{(1)}(\mathcal{N}\otimes\rho)$ is

$$E^{(1)}(\mathcal{N}\otimes\rho)=\max_{\mathcal{P}}I\left(A_1A_2\rangle B_1B_2\right)_{\omega}.\qquad(5)$$

The maximization is over all preparations $\mathcal{P}^{A_2\rightarrow A_1A_2A_1'}$ and the coherent information $I\left(A_1A_2\rangle B_1B_2\right)_{\omega}$ is with respect to the following state:

$$\mathcal{N}^{A_1'\rightarrow B_1}(\mathcal{P}^{A_2\rightarrow A_1A_2A_1'}(\rho^{A_2B_2})).\qquad(6)$$

The proof of the above capacity theorem consists of two parts. The first part that we prove is the *converse theorem*. The multi-letter converse theorem states that the capacity in the above theorem is optimal—any given coding scheme that has asymptotically good performance cannot perform any better than the rate in (4). The second part that we prove is the *direct coding theorem*. The proof of the direct coding theorem gives a coding scheme that achieves the capacity in (4).

Converse: We provide an upper bound on the entanglement generation rate R of a general channel-state coding protocol that allows the help of classical communication. Consider the following chain of inequalities:

$$\begin{aligned} nR &= I\left(A\rangle B\right)_{\Phi} \\ &= I\left(A_1^n A_2^n\rangle B\right)_{\Phi} \\ &\leq I\left(A_1^n A_2^n\rangle B\right)_{\omega'} + \epsilon' \\ &\leq I\left(A_1^n A_2^n\rangle B_1^n B_2^n\right)_{\omega} + \epsilon'. \end{aligned}$$

The first and second equalities result from evaluating the coherent information of the state Φ^{AB} and realizing that the system A and the subspace of $A_1^n A_2^n$ where Alice encodes the entanglement are isomorphic. The maximally entangled state Φ^{AB} and $(\omega')^{A_1^n A_2^n B}$ in (3) are ϵ-close for a good code. Noting this fact, the first inequality results from an application of the Alicki-Fannes' inequality [23] where $\epsilon' \equiv 4\epsilon \log D + 2H(\epsilon)$, $H(\epsilon)$ is the binary entropy function, and $\lim_{\epsilon \to 0} H(\epsilon) = 0$. The last inequality results from quantum data processing [24], where we evaluate the coherent information with respect to the state $\omega^{A_1^n A_2^n B_1^n E_1^n B_2^n E_2^n}$ in (2). The converse theorem holds because the state $\omega^{A_1^n A_2^n B_1^n E_1^n B_2^n E_2^n}$ is a state of the form (6). ■

We can phrase the direct coding theorem as a resource inequality [1]:

$$\langle \mathcal{N} \otimes \rho \rangle + I\left(A_1 A_2; E_1 E_2\right)_{\omega} [c \to c] \geq I\left(A_1 A_2\rangle B_1 B_2\right)_{\omega} [qq]\,. \tag{7}$$

The above resource inequality is an asymptotic statement of achievability. Suppose Alice has access to n independent uses of the noisy quantum channel $\mathcal{N}$, n shares of n respective copies of the noisy bipartite state ρ, and $nI\left(A_1 A_2; E_1 E_2\right)_{\omega}$ bits of classical communication. Then she can reliably generate $nI\left(A_1 A_2\rangle B_1 B_2\right)_{\omega}$ ebits of entanglement with Bob. The entropic quantities are with respect to the state

$$\mathcal{N}^{A_1' \to B_1}(\mathcal{P}^{A_2 \to A_1 A_2 A_1'}(\rho^{A_2 B_2})),$$

where $\mathcal{P}^{A_2 \to A_1 A_2 A_1'}$ is a preparation operation equivalent to appending the state $\rho^{A_2 B_2}$ with a state $\phi^{A_1 A_1'}$ and performing an isometric encoding $\mathcal{E}^{A_1' A_2 \to A_1' A_2}$ so that

$$\mathcal{P}^{A_2 \to A_1 A_2 A_1'}(\rho^{A_2 B_2}) = \mathcal{E}^{A_1' A_2 \to A_1' A_2}(\phi^{A_1 A_1'} \otimes \rho^{A_2 B_2}).$$

We are specifically counting the classical communication cost in the above resource inequality and show how the amount in (7) arises in the proof of the theorem.

The proof of the direct coding theorem exploits the observations and coding techniques from Refs. [25], [14]. We refer the reader to these papers for details of carrying out the proof.

We first establish some notation and concepts for the proof. Alice has many uses of the channel $\mathcal{N}^{A_1' \to B_1}$ available, and we label this channel as $\mathcal{N}_1^{A_1' \to B_1}$ (with a subscript "1") for reasons that become clear later. Let $U_{\mathcal{N}_1}^{A_1' \to B_1 E_1}$ denote an isometric extension of the channel $\mathcal{N}_1^{A_1' \to B_1}$. Suppose Alice prepares the state $\phi^{A_1 A_1'}$ on the systems $A_1 A_1'$. Sending the A_1' system of the state $\phi^{A_1 A_1'}$ through the channel $U_{\mathcal{N}_1}^{A_1' \to B_1 E_1}$ gives rise to a state $\phi^{A_1 B_1 E_1}$ where

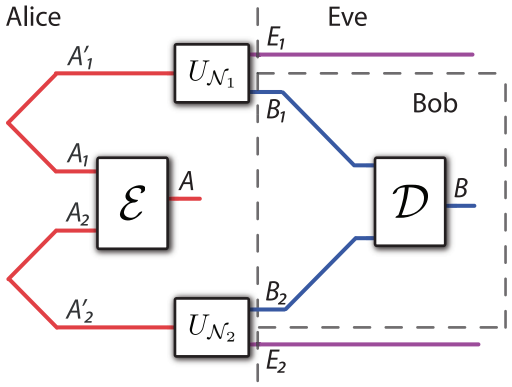

Fig. 2. (Color online) A coding scheme for the channel-state protocol.

$$\phi^{A_1 B_1 E_1} \equiv U_{\mathcal{N}_1}^{A_1' \to B_1 E_1}(\phi^{A_1 A_1'}).$$

The nth extensions of the above states, channel, and isometric extension are respectively as follows: $\phi^{A_1^n A_1'^n}$, $\phi^{A_1^n B_1^n E_1^n}$, $\mathcal{N}_1^{A_1'^n \to B_1^n}$, and $U_{\mathcal{N}_1}^{A_1'^n \to B_1^n E_1^n}$.

Alice also has access to her share A_2^n of the state $\rho^{A_2^n B_2^n}$. There is another, more useful way of thinking about this shared state. Let us first consider a purification $\psi^{A_2 B_2 E_2}$ of the state $\rho^{A_2 B_2}$. We can think of the purification $\psi^{A_2 B_2 E_2}$ as arising from sending a state $\psi^{A_2 A_2'}$ through a channel $\mathcal{N}_2^{A_2' \to B_2}$ with isometric extension $U_{\mathcal{N}_2}^{A_2' \to B_2}$:

$$\psi^{A_2 B_2 E_2} = U_{\mathcal{N}_2}^{A_2' \to B_2}(\psi^{A_2 A_2'}).$$

The tensor power state $\psi^{A_2^n B_2^n E_2^n}$ arises from sending n copies of the state $\psi^{A_2 A_2'}$ through the tensor power channel $U_{\mathcal{N}_2}^{A_2'^n \to B_2^n E_2^n}$. So, it is physically equivalent to say that Alice has access to the system A_2^n of the state $\psi^{A_2^n A_2'^n}$ before the $A_2'^n$ system is transmitted through the channel $U_{\mathcal{N}_2}^{A_2'^n \to B_2^n E_2^n}$, but she does not have access to system $A_2'^n$.

Alice prepares the state $\phi^{A_1^n A_1'^n}$ alongside the state $\psi^{A_2^n A_2'^n}$. She performs an initial entangling, isometric encoder $\mathcal{E}^{A_1' A_2 \to A_1' A_2}$ on each copy $\phi^{A_1 A_1'} \otimes \psi^{A_2 A_2'}$ of the state, so that the overall encoding is a tensor power that we denote by

$$\mathcal{E}^{A_1'^n A_2^n \to A_1'^n A_2^n}(\phi^{A_1^n A_1'^n} \otimes \psi^{A_2^n A_2'^n}).$$

She performs a *typical subspace* measurement of the systems $A_1^n A_2^n$ followed by a *type* measurement of the systems [25], [14], ensuring that the systems $A_1^n A_2^n$ and $A_1'^n A_2'^n$ are maximally entangled. She performs a random unitary U, selected from the Haar measure, on the systems $A_1^n A_2^n$. This unitary is equivalent to applying the unitary U^T to the systems $A_1'^n A_2'^n$ because the systems $A_1^n A_2^n$ and $A_1'^n A_2'^n$ are maximally entangled [14]. She then performs a projective measurement

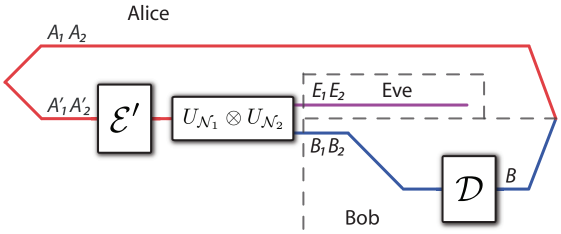

Fig. 3. (Color online) Reduction of the coding scenario in Figure 2 to entanglement generation for the product channel $U_{\mathcal{N}_1} \otimes U_{\mathcal{N}_2}$.

of the systems $A_1^n A_2^n$ onto a subspace $S \subseteq A_1^n A_2^n$ of size $|S|$. This last measurement projects the systems $A_1'^n A_2'^n$ onto a subspace $S' \subseteq A_1'^n A_2'^n$, where the subspace S' is isomorphic to the subspace S and the state on SS' is maximally entangled [25]. Let $\mathcal{E}$ denote these encoding operations on systems $A_1^n A_2^n$, and let $\mathcal{E}'$ denote the equivalent operations occurring on systems $A_1'^n A_2'^n$. Figure 2 gives a picture of this protocol, and Figure 3 gives a picture of a protocol that is formally equivalent to the one in Figure 2. She sends Bob the result of the type measurement (requiring only a sublinear amount of classical communication), and she sends the result of the second projective measurement, requiring $nI\left(A_1A_2; E_1E_2\right)$ bits of classical communication [10], [11], so that he knows in which subspace the entanglement is encoded.

We now can exploit the simplified proof of the quantum coding theorem (Theorem 1 of Ref. [25]). Bob can perform a reliable decoding (resulting from a decoupling of Bob's outputs $B_1^n B_2^n$ from Eve's outputs $E_1^n E_2^n$) if the size $|S|$ of the subspace S is not too large [25]: $|S| < 2^{n(H(B_1B_2) - H(E_1E_2))}$. The rate of this code is

$$\begin{aligned}\frac{\log|S|}{n} &< H\left(B_1B_2\right) - H\left(E_1E_2\right) \\ &= H\left(B_1B_2\right) - H\left(A_1A_2B_1B_2\right) \\ &= I\left(A_1A_2\rangle B_1B_2\right).\end{aligned}$$

We can maximize over all input states $\phi^{A_1A_1'}$ and isometric encoders $\mathcal{E}^{A_1'A_2 \to A_1'A_2}$ to have a code that achieves the one-shot capacity:

$$\max_{\phi,\mathcal{E}} I\left(A_1A_2\rangle B_1B_2\right),$$

where the coherent information is with respect to the following state:

$$\mathcal{N}^{A_1' \to B_1}(\mathcal{E}^{A_1'A_2 \to A_1'A_2}(\phi^{A_1A_1'} \otimes \rho^{A_2B_2})).$$

The maximization with respect to input states and encoders is equivalent to performing a maximization over isometric preparations.

This code achieves the one-shot capacity in (5). We can then block the channels and states together to give a superchannel $\mathcal{N}^{A_1'^l \to B_1^l}$ and superstate $\rho^{A_2^lB_2^l}$. Applying the above proof to this scenario gives a code that achieves the capacity in Theorem 1.

IV. Special Case

We can restrict the above protocol to obtain a special case. Suppose Alice prepares a state $\Phi^{A_1^nA_1'}$ and limits the preparation to be of the form $\mathcal{E}^{A_1' \to A'^n} \otimes \Lambda^{A_2^n}$, where the map $\mathcal{E}^{A_1' \to A'^n}$ is a quantum channel encoding and the map $\Lambda^{A_2^n}$ is a quantum instrument [2] for entanglement distillation. Bob's decoding consists of an operation $\mathcal{D}^{B_1^n \to B_1'} \otimes \Lambda^{B_2^n}$, where the map $\mathcal{D}^{B_1^n \to B_1'}$ is a quantum channel decoding and the map $\Lambda^{B_2^n}$ is a map that uses the classical information sent by Alice. This protocol uses the forward classical channel for entanglement distillation [9] and uses the quantum channel for channel coding the system A_1' only. The one-shot entanglement generation capacity for this restricted scenario is

$$E^{(1)}(\mathcal{N} \otimes \rho) = \max_{\phi^{A_1A_1'}} I\left(A_1\rangle B_1\right) + I\left(A_2\rangle B_2\right)$$

and is equal to the sum of the entanglement generation capacity with the entanglement distillation capacity. This protocol is not optimal because it is less than or equal to the one-shot capacity in (4).

V. Resource Inequalities

We discuss some resource inequalities that follow from the channel-state resource inequality in (7). We can generate a "fully quantum" resource inequality, by applying rule I from Ref. [1] to the resource inequality in (7). We can apply rule I because the communicated classical information is coherently decoupled. The resulting resource inequality resembles the mother resource inequality:

$$\langle\mathcal{N} \otimes \rho\rangle + \frac{1}{2}I\left(A_1A_2; E_1E_2\right)_\omega [q \to q] \geq \frac{1}{2}I\left(A_1A_2; B_1B_2\right)_\omega [qq].$$

There is also a sense in which the mother and father protocol in Refs. [13], [1] arise as special cases of the channel-state coding protocol. First, suppose that the state $\rho^{\otimes n}$ is equivalent to a rate E maximally entangled state $\Phi^{A_2^nB_2^n}$ with nE ebits of entanglement where $E \geq I\left(A_1; E_1\right)/2$. Then, it is best to act with the father protocol. The resource inequality is equivalent to that for the father protocol (modulo some classical communication):

$$\langle\mathcal{N}\rangle + \frac{1}{2}I\left(A_1; E_1\right)[qq] \geq \frac{1}{2}I\left(A_1; B_1\right)[q \to q].$$

Another special case of this protocol is the mother protocol. Suppose that the channel $\mathcal{N}$ is a noiseless qubit channel $\mathrm{id}^{A_1 \to B_1}$ of rate Q where $Q \geq I\left(A_2; E_2\right)/2$. Then the resource inequality is equivalent to that for the mother protocol:

$$\langle\rho\rangle + \frac{1}{2}I\left(A_2; E_2\right)[q \to q] \geq \frac{1}{2}I\left(A_2; B_2\right)[qq].$$

VI. Superactivation

We now discuss how the channel-state coding protocol can lead to a superactivation effect. The main finding in Ref. [20] was the following inequality:

$$\frac{1}{2}P\left(\mathcal{N}\right) \leq Q\left(\mathcal{N} \otimes \mathcal{A}\right),$$

where $P\left(\mathcal{N}\right)$ denotes the private capacity of a channel $\mathcal{N}$ [5], [8] and $Q\left(\mathcal{N} \otimes \mathcal{A}\right)$ denotes the joint quantum capacity of the channel $\mathcal{N}$ and a symmetric channel $\mathcal{A}$ (a symmetric channel is one that behaves the same under interchange of its receiver and its environment, and thus has zero quantum capacity by a no-cloning argument [26]). Smith and Yard showed that an entanglement-binding channel $\mathcal{N}$ [27] , one that has zero quantum capacity but non-zero private capacity, and a 50% erasure channel [28], an example of a symmetric channel, can combine to have a non-zero quantum capacity.

Devetak showed that the secret key generation capacity $K(\mathcal{N})$ of quantum channel $\mathcal{N}$ is equal to its privacy capacity $P(\mathcal{N})$, and he also showed that its entanglement generation capacity $E(\mathcal{N})$ is equal to its quantum capacity $Q(\mathcal{N})$ [5]. Thus, it is possible to translate the above Smith-Yard inequality as follows:

$$\frac{1}{2}K(\mathcal{N}) \leq E(\mathcal{N} \otimes \mathcal{A}).$$

The question now is whether we can have the following inequality for a noisy bipartite state ρ^{AB} and a noisy erasure channel $\mathcal{A}$:

$$\frac{1}{2}K(\rho) \leq E(\rho \otimes \mathcal{A}). \tag{8}$$

An example of the above inequality for our scenario follows directly from the example of Smith and Yard in the appendix of Ref. [20]. Suppose that we have the state $|\rho\rangle^{XAC}$ on page 3 of the Supplementary Materials in Ref. [20]. Let us relabel this state as $|\rho\rangle^{XA_2C}$. Sending the A_2 system through an entanglement-binding channel gives a state $|\rho\rangle^{XB_2E_2C}$. Discarding the C system leads to a state ρ on XB_2, where Alice possesses X and Bob possesses B_2. Alice and Bob can distill some secret key from this state ($K(\rho) > 0$), but cannot distill any maximal entanglement ($E(\rho) = 0$). Suppose now that the state is $|\rho\rangle^{XB_2E_2C}$. Alice can send the C system through a 50% erasure channel. By the same proof method in Ref. [20], it is possible to show the inequality in (8) for this particular setup. The key to this modification of the Smith-Yard proof is that there is entanglement between Alice's systems X and C, implying that an entangling encoder in the channel-state coding protocol outperforms a strategy such as the one in Section IV, which is not able to generate any entanglement for this state. Thus, we have a superactivation effect occurring for the channel-state coding protocol.

VII. Conclusion

We have introduced a new protocol, the channel-state coding protocol, that combines a noisy quantum channel with a noisy quantum state to generate entanglement. This protocol performs well when entanglement is not perfect and should aid in the effort to examine entanglement-assisted codes with imperfect entanglement. The channel-state coding protocol also exhibits the superactivation effect, where a state with no distillable entanglement and a zero-capacity quantum channel can generate maximal entanglement. An open task is to construct a protocol that achieves quantum communication rather than mere entanglement generation.

M.M.W. thanks Andreas Winter for useful discussions and acknowledges research grant SAIC-1669, the National Research Foundation & Ministry of Education, Singapore, and the Centre for Quantum Technologies.

References

[1] I. Devetak, A. W. Harrow, and A. Winter, "A resource framework for quantum Shannon theory," *IEEE Transactions on Information Theory*, vol. 54, no. 10, pp. 4587–4618, October 2008.

[2] J. Yard, "Simultaneous classical-quantum capacities of quantum multiple access channels," Ph.D. dissertation, Stanford University, Stanford, CA, 2005, quant-ph/0506050.

[3] S. Lloyd, "The capacity of a noisy quantum channel," *Physical Review A*, vol. 55, pp. 1613–1622, 1997.

[4] P. W. Shor, "The quantum channel capacity and coherent information," MSRI workshop on quantum computation, 2002.

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

[6] A. S. Holevo, "The capacity of the quantum channel with general signal states." *IEEE Transactions on Information Theory*, vol. 44, pp. 269–273, 1998.

[7] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Physical Review A*, vol. 56, pp. 131–138, 1997.

[8] 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, 2004.

[9] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wooters, "Mixed state entanglement and quantum error correction," *Physical Review A*, vol. 54, pp. 3824–3851, 1996.

[10] I. Devetak and A. Winter, "Relating quantum privacy and quantum coherence: an operational approach," *Physical Review Letters*, vol. 93, p. 080501, 2004.

[11] ——, "Distillation of secret key and entanglement from quantum states," *Proceedings of the Royal Society A*, vol. 461, pp. 207–235, 2005.

[12] ——, "Distilling common randomness from bipartite quantum states," *IEEE Transactions on Information Theory*, vol. 50, pp. 3138–3151, 2003.

[13] I. Devetak, A. W. Harrow, and A. J. Winter, "A family of quantum protocols," *Physical Review Letters*, vol. 93, p. 239503, 2004.

[14] A. Abeyesinghe, I. Devetak, P. Hayden, and A. Winter, "The mother of all protocols: Restructuring quantum information's family tree," quant-ph/0606225, 2006.

[15] J. Oppenheim, "State redistribution as merging: introducing the coherent relay," *arXiv:0805.1065*, 2008.

[16] M.-H. Hsieh and M. M. Wilde, "Trading classical communication, quantum communication, and entanglement in quantum Shannon theory," arXiv:0901.3038, January 2009.

[17] M. M. Wilde and M.-H. Hsieh, "The quantum dynamic capacity formula of a quantum channel," April 2010, arXiv:1004.0458.

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

[19] B. Shaw, M. M. Wilde, O. Oreshkov, I. Kremsky, and D. Lidar, "Encoding one logical qubit into six physical qubits," *Physical Review A*, vol. 78, p. 012337, 2008.

[20] G. Smith and J. Yard, "Quantum communication with zero-capacity channels," *Science*, vol. 321, pp. 1812–1815, September 2008.

[21] P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Superactivation of bound entanglement," *Physical Review Letters*, vol. 90, no. 10, p. 107901, March 2003.

[22] K. Li, A. Winter, X. Zou, and G. Guo, "Nonadditivity of the private classical capacity of a quantum channel," *arXiv:0903.4308*, 2009.

[23] R. Alicki and M. Fannes, "Continuity of quantum conditional information," *Journal of Physics A: Mathematical and General*, vol. 37, no. 5, pp. L55–L57, 2004.

[24] B. Schumacher and M. A. Nielsen, "Quantum data processing and error correction," *Physical Review A*, vol. 54, pp. 2629–2635, 1996.

[25] P. Hayden, M. Horodecki, A. Winter, and J. Yard, "A decoupling approach to the quantum capacity," *Open Systems & Information Dynamics*, vol. 15, pp. 7 – 19, March 2008.

[26] G. Smith, J. A. Smolin, and A. Winter, "The quantum capacity with symmetric side channels," *IEEE Transactions on Information Theory*, vol. 54, no. 9, pp. 4208–4217, 2008.

[27] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "Secure key from bound entanglement," *Physical Review Letters*, vol. 94, no. 16, p. 160502, April 2005.

[28] M. Grassl, T. Beth, and T. Pellizzari, "Codes for the quantum erasure channel," *Physical Review A*, vol. 56, no. 1, pp. 33–38, July 1997.