Public and private communication with a quantum channel and a secret key

Min-Hsiu Hsieh*
ERATO–SORST Quantum Computation and Information Project, Japan Science and Technology Agency, 5-28-3 Hongo, Bunkyo-ku, Tokyo, 113–0033 Japan

Mark M. Wilde†
Electronic Systems Division, Science Applications International Corporation, 4001 North Fairfax Drive, Arlington, Virginia 22203, USA
(Received 17 April 2009; published 5 August 2009)

We consider using a secret key and a noisy quantum channel to generate noiseless public communication and noiseless private communication. The optimal protocol for this setting is the *publicly enhanced private father protocol*. This protocol exploits random coding techniques and "piggybacking" of public information along with secret-key-assisted private codes. The publicly enhanced private father protocol is a generalization of the secret-key-assisted protocol of Hsieh, Luo, and Brun and a generalization of a protocol for simultaneous communication of public and private information suggested by Devetak and Shor.

DOI: 10.1103/PhysRevA.80.022306 PACS number(s): 03.67.Hk, 03.67.Dd

I. INTRODUCTION

The qualitative connection between secrecy of information and the ability to maintain quantum correlations has long been a part of quantum information theory. The connection comes about from the observation that a maximally entangled ebit state, shared between two parties named Alice and Bob, has no correlations with the "rest of the universe"—in this sense, the ebit is *monogamous* [1]. We can represent the global state of the ebit and the rest of the universe as

$$\Phi^{AB} \otimes \sigma^{E},$$

where Alice and Bob share the ebit Φ^{AB}, and

$$\Phi^{AB} \equiv |\Phi\rangle\langle\Phi|^{AB},$$

$$|\Phi\rangle^{AB} \equiv \frac{1}{\sqrt{2}}(|0\rangle^{A}|0\rangle^{B} + |1\rangle^{A}|1\rangle^{B}),$$

and σ^{E} is some state of Eve, a third party representing the rest of the universe. Eve's state σ^{E} is independent of Alice and Bob's ebit. The relation to a secret key comes about when Alice and Bob perform local measurements of the ebit in the computational basis. The resulting state is

$$\bar{\Phi}^{AB} \otimes \sigma^{E},$$

where $\bar{\Phi}^{AB}$ is the maximally correlated state

$$\bar{\Phi}^{AB} \equiv \frac{1}{2}(|0\rangle\langle 0|^{A} \otimes |0\rangle\langle 0|^{B} + |1\rangle\langle 1|^{A} \otimes |1\rangle\langle 1|^{B}).$$

In this setting, the cryptographic setting, we consider Eve as a potential eavesdropper. She is no longer the rest of the universe, because some party now holds the purification of the dephased state $\bar{\Phi}^{AB}$.

The body of literature on the privacy–quantum-coherence connection has now grown substantially. Some of the original exploitations of this connection were the various quantum key distribution protocols [2–4]. These protocols establish a shared secret key with the help of a noisy quantum channel or noisy entanglement. The subsequent proofs [5,6] for the security of these protocols rely on the formal mathematical equivalence between entanglement distillation [7] and key distillation. Schumacher and Westmoreland explored the connection with an information-theoretical study [8]—they established a simple relation between the capacity of a quantum channel for transmitting quantum information and its utility for quantum key distribution. Collins and Popescu [9] and Gisin *et al.* [10] initiated the formal study of the connections between entanglement and secret key. Since then, researchers have determined a method for mapping an entangled state to a probability distribution with secret correlations [11] and have continued to extend existing quantum results [12] to analogous results for privacy [13].

The connection has also proven fruitful for quantum Shannon theory, where we study the capabilities of a large number of independent uses of a noisy quantum channel or a large number of copies of a noisy bipartite state. The first step in this direction was determining the capacity of a quantum channel for transmitting a private message or establishing a shared secret key [14,15]. Devetak further showed how *coherently* performing each step of a private protocol leads to a code that achieves the capacity of a quantum channel for transmitting quantum information [14]. Since these initial insights, we have seen how the seemingly different tasks of distilling secret key, distilling entanglement, transmitting private information, and transmitting quantum information all have connections [16]. Oppenheim *et al.* determined a merging protocol for private correlations [17], based on the quantum state merging protocol [18,19]. Additionally, the secret-key-assisted private capacity of a quantum channel [20] is analogous to its entanglement-assisted quantum capacity [21,22].

The connection is only qualitative because the Horodeckis and Oppenheim observed that there exist *bound entangled* states [23]. These bound entangled states are entangled, yet

*minhsiuh@gmail.com
†mark.m.wilde@saic.com

have no distillable entanglement (one cannot extract ebits from them), but they indeed have distillable secret key. The dynamic equivalent of this state is an entanglement binding channel [24–26]. This channel has no ability to transmit quantum information. The loss of the privacy-coherence connection here is not necessarily discomforting. In fact, it is more interesting because it leads to the "superactivation effect" [27]—the possibility of combining two zero-capacity channels to form a quantum channel with nonzero quantum capacity. Additionally, the private analog of this scenario exhibits some unexpected behavior [28].

In this paper, we continue along the privacy-coherence connection and detail the publicly enhanced private father protocol. This protocol exploits a secret key and a large number of independent uses of a noisy quantum channel to generate noiseless public communication and noiseless private communication. This protocol is the "public-private" analog of the classically enhanced father protocol [29], and might lead to further insights into the privacy-coherence connection. The publicly enhanced private father protocol combines the coding techniques of the suggested protocol in Sec. IV of Ref. [30] (originally proven for the classical wiretap channel [31]) with the recent secret-key-assisted private communication protocol [20].

We structure this work as follows: the next section establishes the definition of a noiseless public channel, a noiseless private channel, noiseless common randomness, and a perfect secret key. We then clarify a small point with the protocol for private communication [14,15]—specifically, we address the apparent ability of that protocol to transmit public information in addition to private information. Section IV describes the publicly enhanced private father protocol and states our main theorem (Theorem 1). This theorem gives the capacity region for the publicly enhanced private father protocol. We proceed with the proof of the corresponding converse theorem in Sec. V and the proof of the corresponding direct coding theorem in Sec. VI. Section VII shows that the suggested protocol from Ref. [30] is a child of the publicly enhanced private father protocol. We then conclude with some remaining open questions.

II. DEFINITIONS AND NOTATION

We first present the notion of a noiseless public channel, a noiseless private channel, and a noiseless secret key as resources. Our communication model includes one sender Alice, a receiver Bob, and an eavesdropper Eve. Alice chooses classical messages k from a set $[K]\equiv\{1,\ldots,K\}$. She encodes these messages as quantum states $\{|k\rangle\langle k|^A\}_{k\in[K]}$. We assume that each party is in a local, secret facility that does not leak information to the outside world. For example, Eve cannot gain any information about a state that Alice or Bob prepares locally. We consider two dynamic resources, public classical communication and private classical communication, and two static resources, common randomness and secret key.

A noiseless public channel $\mathrm{id}_{\mathrm{pub}}^{A\to B}$ from Alice to Bob implements the following map for $k\in[K]$:

$$\mathrm{id}_{\mathrm{pub}}^{A\to B}:|k\rangle\langle k|^A\to|k\rangle\langle k|^B\otimes\sum_{k'\in[K]}p_{K'|K}(k'|k)\rho_{k'}^E, \qquad (1)$$

where $p_{K'|K}(k'|k)$ is some conditional probability distribution and $\rho_{k'}^E$ is a state on Eve's system. The above definition of a noiseless public channel captures the idea that Bob receives the classical information perfectly, but Eve receives only partial information about Alice's message. Eve has perfect correlation with Alice's message if and only if her conditional distribution $p_{K'|K}(k'|k)$ is $\delta_{k',k}$ and her states $\rho_{k'}^E=|k'\rangle\langle k'|^E$ for all k'. We make no distinction between a noiseless public channel where Eve receives partial information and one where Eve receives perfect information because we are only concerned with the rate at which Alice can communicate to Bob—we are not concerned with the more general scenario of broadcast communication where Eve is an active party in the communication protocol [32]. We represent the noiseless public channel symbolically as the following resource:

$$[c\to c]_{\mathrm{pub}}.$$

The resource inequality framework [21] uses the notation $[c\to c]$ to represent one noiseless bit of classical communication. We require a symbol different from $[c\to c]$ because that symbol does not distinguish between public and private communication. For example, the superdense coding protocol [33] actually produces two private classical bits, but the notation $[c\to c]$ does not indicate this fact.

A noiseless private channel is the following map:

$$\mathrm{id}_{\mathrm{priv}}^{A\to B}:|k\rangle\langle k|^A\to|k\rangle\langle k|^B\otimes\sigma^E,$$

where σ^E is a constant state on Eve's system, independent of what Bob receives. A private channel appears as a special case of a public channel where random variable K' that represents Eve's knowledge is independent of random variable K. The definition in Eq. (1) reduces to that of a private channel if we set the probability distribution in Eq. (1) to $p_{K'|K}(k')$. But we define a private channel as the case when K' and K are independent. Otherwise, the channel is public. This difference is the distinguishing feature of a noiseless private channel. We represent the noiseless private channel symbolically as the following resource:

$$[c\to c]_{\mathrm{priv}}.$$

The above definitions of a public classical channel and private classical channel are inspired by definitions in Refs. [20,34].

Common randomness is the static analog of a noiseless public channel [35–37]. In fact, Alice can actually use a public channel to implement common randomness. Alice first prepares a local maximally mixed state π^A where

$$\pi^A\equiv\frac{1}{|K|}\sum_{k\in[K]}|k\rangle\langle k|^A.$$

She makes an exact copy of the random state locally to produce the following state:

$$\bar{\Phi}^{AA'}\equiv\frac{1}{|K|}\sum_{k\in[K]}|k\rangle\langle k|^A\otimes|k\rangle\langle k|^{A'}. \qquad (2)$$

She sends the A' system through the noiseless public channel. The resulting state represents common randomness shared between Alice and Bob, about which Eve may have partial information:

$$\frac{1}{|K|}\sum_{k\in[K]}|k\rangle\langle k|^A\otimes|k\rangle\langle k|^B\otimes\sum_{k'\in[K]}p_{K'|K}(k'|k)\rho^E_{k'}.$$

A noiseless secret key is the static analog of a noiseless private channel. Alice again prepares the state π^A and makes a copy of it to an A' system. She sends the A' system through a noiseless private channel, generating the following resource:

$$\frac{1}{K}\sum_{k\in[K]}|k\rangle\langle k|^A\otimes|k\rangle\langle k|^B\otimes\sigma^E=\bar{\Phi}^{AB}\otimes\sigma^E.$$

Alice and Bob share perfect common randomness, but this time, Eve has no knowledge of this common randomness. This resource is a secret key. A perfect secret-key resource has two requirements [38]:

(1) The key should have a uniform distribution.

(2) Eve possesses no correlations with the secret key.

We denote the resource of a shared secret key as follows:

$$[cc]_{\text{priv}}.$$

Note that a noiseless public channel alone cannot implement a noiseless private channel, and a noiseless private channel alone cannot implement a noiseless public channel. This relation is different from the corresponding relation between a noiseless quantum channel and a noiseless classical channel [39] because a noiseless quantum channel alone can implement a noiseless classical channel, but a noiseless classical channel alone cannot implement a noiseless quantum channel.

III. RELATIVE RESOURCE IN PRIVATE COMMUNICATION

We would like to clarify one point with the protocol for private communication [14,15] before proceeding to our main theorem. By inspecting the proof of the direct coding theorem in Ref. [14], one might think that Alice could actually transmit public information at an additional rate of $I(X;E)$. The following sentence from Ref. [14] may lead one to arrive at such a conclusion:

"By construction, Bob can perform a measurement that correctly identifies the pair (k,m), and hence k, with probability $\geq 1-\sqrt[4]{\epsilon}$."

But this conclusion is incorrect because the random variable M representing the "public" message m must have a uniform distribution. This random variable M serves the purpose of randomizing Eve's knowledge of the private message k [40]. The protocol would not operate as intended if random variable M had a distribution other than the uniform distribution. The size of the message set for the random variable M must be at least $2^{nI(X;E)}$. The rate $I(X;E)$ of randomization further confirms the role of the mutual information as the minimum amount of noise needed to destroy one's correlations with a random variable [41] (see Refs. [42,43] for further explorations of this idea). It is thus not surprising that the mutual information $I(X;E)$ arises in the protocol for private communication because Alice would like to destroy Eve's correlations with her private message k.

The resource inequality [21] for the protocol for private communication is as follows:

$$\langle\mathcal{N}\rangle\geq I(X;E)[c\rightarrow c:\pi]_{\text{pub}}+[I(X;B)-I(X;E)][c\rightarrow c]_{\text{priv}}, \tag{3}$$

where the mutual information quantities are with respect to the following classical-quantum state:

$$\sum_{x\in\mathcal{X}}p_X(x)|x\rangle\langle x|^X\otimes U^{A'\rightarrow BE}_{\mathcal{N}}(\sigma^{A'}_x),$$

corresponding to the channel input ensemble $\{p_X(x),\sigma^{A'}_x\}_{x\in\mathcal{X}}$. The meaning of the resource inequality is that Alice can transmit $nI(X;E)$ bits of public information (with the requirement that Alice's random variable has a uniform distribution) and $n[I(X;B)-I(X;E)]$ bits of private information by using a large number n of independent uses of the noisy quantum channel $\mathcal{N}$. The resource $[c\rightarrow c:\pi]_{\text{pub}}$ is not an absolute resource, but is rather a *relative resource* [21,44,45], meaning that the protocol only works properly if Alice's public variable has a uniform distribution, or equivalently, is equal to the maximally mixed state π. This public information must be completely random because Alice uses it to randomize Eve's knowledge of the private message.

The resource inequality in Eq. (3) leads to a simpler way of implementing the direct coding theorem of the secret-key-assisted private communication protocol [20]. Suppose that Alice has public information in a random variable M. If she combines this random variable with a secret key, the resulting random variable has a uniform distribution because the secret key randomizes the public variable. This variable can then serve as the input needed to implement the relative resource of public communication. Alice can transmit an extra $nI(X;E)$ bits of private information by combining this public communication with the secret-key resource, essentially implementing a one-time pad protocol [46,47]. We phrase the above argument with the theory of resource inequalities

$$\begin{aligned}
&\langle\mathcal{N}\rangle+I(X;E)[cc]_{\text{priv}}\\
&\quad\geq I(X;E)[c\rightarrow c:\pi]_{\text{pub}}+I(X;E)[cc]_{\text{priv}}\\
&\qquad+[I(X;B)-I(X;E)][c\rightarrow c]_{\text{priv}}\\
&\quad\geq I(X;E)[c\rightarrow c]_{\text{priv}}+[I(X;B)-I(X;E)][c\rightarrow c]_{\text{priv}}\\
&\quad=I(X;B)[c\rightarrow c]_{\text{priv}}.
\end{aligned}$$

This resource inequality is equivalent to that obtained in Ref. [20].

IV. PUBLIC AND PRIVATE TRANSMISSION WITH A SECRET KEY

We begin by defining our publicly enhanced private father protocol (PEPFP) for a quantum channel $\mathcal{N}^{A'\rightarrow B}$ from a sender Alice to a receiver Bob. The channel has an extension to an isometry $U^{A'\rightarrow BE}_{\mathcal{N}}$, defined on a bipartite quantum system BE, where Bob has access to system B and Eve has access to system E. Alice's task is to transmit, by some large number n uses of the channel $\mathcal{N}$, one of K public messages

and one of M private messages to Bob. The goal is for Bob to identify the messages with high probability and for Eve to receive no information about the private message. In addition, Alice and Bob have access to a private string (a secret key), picked uniformly at random from the set $[S]$, before the protocol begins.

An (n,R,P,R_S,ϵ) *secret-key-assisted private channel code* consists of six steps: preparation, encryption, channel coding, transmission, channel decoding, and decryption. We detail each of these steps below.

Preparation. Alice prepares a public message k in a register K and a private message m in a register M. Each of these has a uniform distribution

$$\pi^K \equiv \frac{1}{K}\sum_{k=1}^{K} |k\rangle\langle k|^K,$$

$$\pi^M \equiv \frac{1}{M}\sum_{m=1}^{M} |m\rangle\langle m|^M.$$

Alice also shares the maximally correlated secret-key state $\bar{\Phi}^{S_A S_B}$ with Bob

$$\bar{\Phi}^{S_A S_B} \equiv \frac{1}{S}\sum_{s=1}^{S} |s\rangle\langle s|^{S_A} \otimes |s\rangle\langle s|^{S_B}.$$

The overall state after preparation is

$$\pi^K \otimes \pi^M \otimes \bar{\Phi}^{S_A S_B}.$$

Encryption. Alice exploits an encryption map

$$f:[M]\times[S]\to[M].$$

The encryption map f computes an encrypted variable $f(m,s)$ that depends on the private message m and the secret-key s. Furthermore, the encryption map f satisfies the following conditions:

(1) For all $s_1,s_2\in[S]$ where $s_1\neq s_2$

$$f(m,s_1)\neq f(m,s_2).$$

(2) For all $m_1,m_2\in[M]$ where $m_1\neq m_2$

$$f(m_1,s)\neq f(m_2,s).$$

The encryption map f corresponds physically to a CPTP map $\mathcal{F}^{MS_A\to P}$. The state after the encryption map is

$$\mathcal{F}^{MS_A\to P}(\pi^K\otimes\pi^M\otimes\bar{\Phi}^{S_A S_B}) = \pi^K\otimes\frac{1}{MS}\sum_{m,s}|f(m,s)\rangle\langle f(m,s)|^P \otimes |s\rangle\langle s|^{S_B}.$$

Channel Encoding. Alice prepares the codeword state $\sigma^{A'^n}_{k,f(m,s)}$ based on the public message k and the encrypted message $f(m,s)$. This encoding corresponds physically to some CPTP map $\mathcal{E}^{KP\to A'^n}$. The state after the encoding map is

$$\frac{1}{KMS}\sum_{k,m,s}\sigma^{A'^n}_{k,f(m,s)}\otimes|s\rangle\langle s|^{S_B}.$$

Transmission. Alice sends the state $\sigma^{A'^n}_{k,f(m,s)}$ through the channel $U^{A'^n\to B^n E^n}_{\mathcal{N}}$, generating the state

$$\frac{1}{KMS}\sum_{k,m,s}\sigma^{B^n E^n}_{k,f(m,s)}\otimes|s\rangle\langle s|^{S_B},$$

where

$$\sigma^{B^n E^n}_{k,f(m,s)} \equiv U^{A'^n\to B^n E^n}_{\mathcal{N}}(\sigma^{A'^n}_{k,f(m,s)}).$$

Channel Decoding. Bob receives the above state from the channel and would like to decode the messages. He exploits a decoding positive-operator-valued measure (POVM) that acts on his system B^n. The elements of this POVM are

$$\{\Lambda^{B^n}_{k,f(m,s)}\}_{k\in[K],f(m,s)\in[M]}.$$

Bob places the measurement results k and $f(m,s)$ in the respective registers $\hat{K}$ and $\hat{P}$. The ideal output state after Bob's decoding operation is

$$\sum_{k,m,s}\sigma^{B^n E^n}_{k,f(m,s)}\otimes|s\rangle\langle s|^{S_B}\otimes|k\rangle\langle k|^{\hat{K}}\otimes|f(m,s)\rangle\langle f(m,s)|^{\hat{P}},$$

where it is understood that the normalization factor is $1/(KMS)$.

Decryption. The final step is for Bob to decrypt the encrypted message $f(m,s)$. He employs a decryption function g, where

$$g:[M]\times[S]\to[M].$$

The decryption function g satisfies the following property:

$$\forall s,m \quad g(f(m,s),s)=m.$$

This decryption function allows Bob to recover Alice's private message as $m=g(f(m,s),s)$ based on the encrypted message $f(m,s)$ and the secret-key s. Physically, this operation corresponds to a CPTP map $\mathcal{G}^{S_B\hat{P}\to\hat{M}}$. The state after this decryption map is

$$\frac{1}{KMS}\sum_{k,m,s}\sigma^{B^n E^n}_{k,f(m,s)}\otimes|s\rangle\langle s|^{S_B}\otimes|k\rangle\langle k|^{\hat{K}}\otimes|m\rangle\langle m|^{\hat{M}}.$$

Figure 1 depicts all of the above steps in a general publicly enhanced private father code.

The conditions for a good publicly enhanced secret-key-assisted private code are that Bob be able to decode the public message k and encrypted message $p=f(m,s)$ with high probability

$$\forall k,p \quad \mathrm{Tr}\{\Lambda^{B^n}_{k,p}\sigma^{B^n}_{k,p}\}\geq 1-\epsilon.$$

It is sufficient to consider the above criterion because Bob can determine the private message m with high probability if he can determine the encrypted message p with high probability. Also, the following inequality is our security criterion:

$$\forall k,m \quad \left\|\sum_s \sigma^{E^n}_{k,f(m,s)}\otimes|s\rangle\langle s|^{S_B}-\sigma^{E^n}_k\otimes\pi^{S_B}\right\|_1\leq\epsilon. \quad (4)$$

This criterion ensures that Eve's state is independent of the key and the private message m.

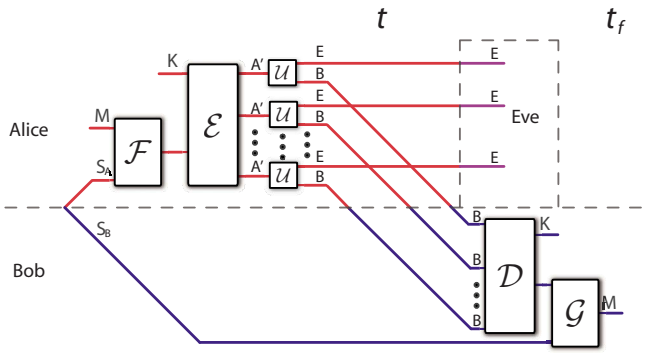

FIG. 1. (Color online) The above figure depicts all of the steps in a publicly enhanced private father code. Alice performs the encryption map $\mathcal{F}$ on her private variable M and her half S_A of the secret key. She then encodes her public variable K and the encrypted message with the encoding map $\mathcal{E}$. She transmits the encoded data over a large number of uses of the noisy channel $\mathcal{N}$. The isometric extension of the noisy quantum channel $\mathcal{N}$ is $U_{\mathcal{N}}$, and we give the full purification of the channel to Eve. Bob receives the outputs of the channel. He performs the decoding map $\mathcal{D}$ to recover the public variable K and the encrypted message. He combines the encrypted message with his half of the secret key and processes these two variables with the decryption map $\mathcal{G}$. He then recovers the private variable M. A good publicly enhanced private father code has the property that Bob can perfectly recover the public variable K and the private variable M while Eve learns nothing about the secret key or the private variable M.

A rate triple (R,P,R_S) is *achievable* if there exists an $(n,R-\delta,P-\delta,R_S+\delta,\epsilon)$ publicly enhanced private father code for any $\epsilon,\delta>0$ and sufficiently large n. The capacity region $C_{\text{PEPFP}}(\mathcal{N})$ is a three-dimensional region in the (R,P,R_S) space with all possible achievable rate triples (R,P,R_S).

Theorem 1. The capacity region $C(\mathcal{N})$ of a secret-key-assisted quantum channel $\mathcal{N}$ for simultaneously transmitting both public and private classical information is equal to the following expression:

$$C(\mathcal{N}) = \overline{\bigcup_{l=1}^{\infty} \frac{1}{l} C^{(1)}(\mathcal{N}^{\otimes l})}, \tag{5}$$

where the overbar indicates the closure of a set. The "one-shot" region $C^{(1)}(\mathcal{N})$ is the set of all $R,P,R_S \geq 0$, such that

$$R \leq I(X;B)_\sigma, \tag{6}$$

$$P \leq R_S + I(Y;B|X)_\sigma - I(Y;E|X)_\sigma, \tag{7}$$

$$P \leq I(Y;B|X)_\sigma. \tag{8}$$

The above entropic quantities are with respect to a "one-shot" quantum state σ^{XYBE}, where

$$\sigma^{XYBE} \equiv \sum_x p(x)|x\rangle\langle x|^X \otimes \rho_x^{YBE}, \tag{9}$$

and the states ρ_x^{YBE} are of the form

$$\rho_x^{YBE} = \sum_y p(y|x)|y\rangle\langle y|^Y \otimes U_{\mathcal{N}}^{A'\to BE}(\rho_{x,y}^{A'}), \tag{10}$$

for some density operator $\rho_{x,y}^{A'}$ and $U_{\mathcal{N}}^{A'\to BE}$ is an isometric extension of $\mathcal{N}$. It is sufficient to consider $|\mathcal{X}| \leq \min\{|A'|,|B|\}^2+1$ by the method in Ref. [48].

The proof of the above capacity theorem consists of two parts. The first part that we show is the *converse theorem*. The converse theorem shows that the rates in the above theorem are optimal—any given coding scheme that has asymptotically good performance cannot perform any better than the above rates. We prove the converse theorem in the next section. 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 limits given in the above theorem.

V. PROOF OF THE CONVERSE THEOREM

We outline the proof strategy of the converse before delving into its details. Consider that a noiseless public channel can generate common randomness and a noiseless private channel can generate a secret key. Let $K(\mathcal{N})$ denote the capacity of a quantum channel $\mathcal{N}$ for generating common randomness, generating a secret key, while consuming a secret key at respective rates (R,P,R_S). The capacity region $K(\mathcal{N})$ contains the capacity region $C(\mathcal{N})$ of Theorem 1 $(C(\mathcal{N}) \subseteq K(\mathcal{N}))$ because of the aforementioned one-way relation between a noiseless public channel and common randomness and that between a noiseless private channel and a secret key. It thus suffices to prove the converse for a secret-key-assisted common randomness generation and secret-key generation protocol. We consider the most general such protocol when proving the converse and show that the capacity region in Eqs. (6)–(8) bounds the capacity region $K(\mathcal{N})$. The result of the converse theorem is then that $K(\mathcal{N}) \subseteq C(\mathcal{N})$ and thus that $K(\mathcal{N}) = C(\mathcal{N})$.

Proof (Converse). Suppose Alice creates the maximally correlated state $\pi^{MM'_A}$ locally, where

$$\bar{\Phi}^{MM'_A} \equiv \frac{1}{M}\sum_{m=1}^{M} |m\rangle\langle m|^M \otimes |m\rangle\langle m|^{M'_A}.$$

(the protocol should be able to transmit the correlations in state $\bar{\Phi}^{MM'_A}$ with ϵ accuracy while keeping them secret). Alice shares the maximally correlated secret-key state $\bar{\Phi}^{S_AS_B}$ with Bob

$$\bar{\Phi}^{S_AS_B} \equiv \frac{1}{S}\sum_{s=1}^{S} |s\rangle\langle s|^{S_A} \otimes |s\rangle\langle s|^{S_B}.$$

Alice prepares a state $\bar{\Phi}^{KK'_A}$ for common randomness generation

$$\bar{\Phi}^{KK'_A} \equiv \frac{1}{K}\sum_{k=1}^{K} |k\rangle\langle k|^K \otimes |k\rangle\langle k|^{K'_A}.$$

Alice combines her states $\bar{\Phi}^{KK'_A}$, $\bar{\Phi}^{MM'_A}$, and $\bar{\Phi}^{S_AS_B}$. The most general encoding operation that she can perform on her three

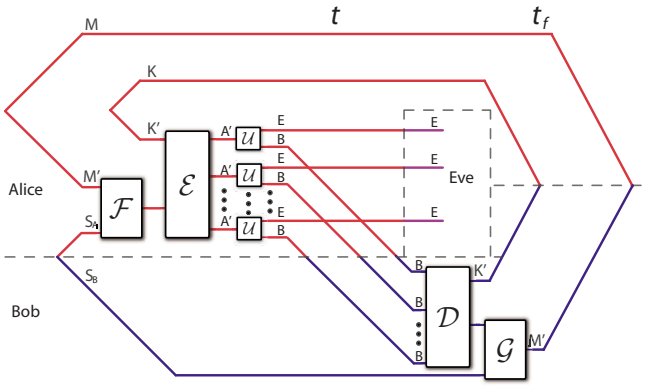

FIG. 2. (Color online) The above figure depicts the coding scenario that we consider for the converse theorem. It is similar to the protocol of Fig. 1 with the exception that the goal is for Alice and Bob to generate common randomness and a secret key, rather than transmitting public and private information, respectively.

registers K'_A, M'_A, and S_A is a conditional quantum encoder $\mathcal{E}^{K'_A M'_A S_A \to A'^n}$ consisting of a collection $\{\mathcal{E}_k^{M'_A S_A \to A'^n}\}_k$ of completely-positive and trace-preserving (CPTP) maps [29]. Each element $\mathcal{E}_k^{M'_A S_A \to A'^n}$ of the conditional quantum encoder consists of an encryption with the secret key and the mapping to channel codewords. Each element $\mathcal{E}_k^{M'_A S_A \to A'^n}$ produces the following state:

$$\omega_k^{MS_B A'^n} \equiv \mathcal{E}_k^{M'_A S_A \to A'^n}(\bar{\Phi}^{MM'_A} \otimes \bar{\Phi}^{S_A S_B}).$$

The average density operator over all public messages is then as follows:

$$\frac{1}{K}\sum_k |k\rangle\langle k|^K \otimes \omega_k^{MS_B A'^n}.$$

Alice sends the A'^n system through the noisy channel $U_{\mathcal{N}}^{A'^n \to B^n E^n}$, producing the following state:

$$\omega^{KMS_B B^n E^n} \equiv \frac{1}{K}\sum_k |k\rangle\langle k|^K \otimes U_{\mathcal{N}}^{A'^n \to B^n E^n}(\omega_k^{MS_B A'^n}).$$

Define the systems $Y \equiv MS_B$ and $X \equiv K$ so that the above state is a particular n^{th} extension of the state in the statement of the public-private secret-key-assisted capacity theorem. The above state is the state at time t in Fig. 2. Bob receives the above state and performs a decoding instrument $\mathcal{D}^{B^n S_B \to K'_B M'_B}$ [29] (each element $\mathcal{D}_k^{B^n S_B \to M'_B}$ of the instrument consists of a channel decoding and a decryption). The protocol ends at time t_f (depicted in Fig. 2). Let $(\omega')^{KMK'_B M'_B E^n}$ be the state at time t_f after Bob processes $\omega^{KMS_B B^n E^n}$ with the decoding instrument $\mathcal{D}^{B^n S_B \to K'_B M'_B}$.

Suppose that an $(n, R-\delta, P-\delta, R_S+\delta, \epsilon)$ secret-key-assisted protocol as given above exists. In particular, the following information-theoretic security conditions follow from the security criterion in Eq. (4):

$$I(M;E^n|K)_\omega \leq \epsilon, \tag{11}$$

$$I(S_B;E^n|K)_\omega \leq \epsilon, \tag{12}$$

by the application of the Alicki-Fannes inequality [49] and evaluating the conditional mutual information of the ideal state $\sigma_k^{E^n} \otimes \pi^{S_B}$ in Eq. (4). These conditions imply that Eve learns nothing about the secret correlations in system M and Eve learns nothing about the secret-key S_B (at time t) even if she knows the public variable K. We prove that the following bounds apply to the elements of the protocol's rate triple $(R-\delta, P-\delta, R_S+\delta)$:

$$R - \delta \leq \frac{I(X;B^n)_\omega}{n}, \tag{13}$$

$$P - \delta \leq \frac{I(Y;B^n|X)_\omega}{n}, \tag{14}$$

$$P - \delta \leq R_S + \frac{I(Y;B^n|X)_\omega - I(Y;E^n|X)_\omega}{n}, \tag{15}$$

$$R_S + \delta \geq \frac{I(Y;E^n|X)_\omega}{n}, \tag{16}$$

for any $\epsilon, \delta > 0$ and all sufficiently large n.

In the ideal case, the ideal private channel acts on system M to produce the maximally correlated and secret state $\pi^{MM'}$. So, for our case, the inequality

$$\|(\omega')^{MM'_B E^n} - \bar{\Phi}^{MM'_B} \otimes \sigma^{E^n}\|_1 \leq \epsilon \tag{17}$$

holds because the protocol is ϵ good for private communication. The state σ^{E^n} is some constant state on Eve's system.

The lower bound in Eq. (16) is the most straightforward to prove. Consider the following chain of inequalities:

$$\begin{aligned} n(R_S+\delta)+2\epsilon &\geq I(M;E^n|K)_\omega + I(S_B;E^n|K)_\omega + H(S_B|K)_\omega \\ &= H(M|K)_\omega + H(E^n|K) - H(ME^n|K)_\omega + I(S_B;E^n|K)_\omega + H(S_B|K)_\omega \geq H(M|S_BK)_\omega + H(E^n|S_BK) - H(ME^n|K)_\omega \\ &\quad + I(S_B;E^n|K)_\omega + H(S_B|K)_\omega \geq H(M|S_BK)_\omega + H(E^n|S_BK) - H(ME^nS_B|K)_\omega + I(S_B;E^n|K)_\omega + H(S_B|K)_\omega \\ &= I(M;E^n|S_BK)_\omega + I(S_B;E^n|K)_\omega = I(MS_B;E^n|K)_\omega = I(Y;E^n|X)_\omega. \end{aligned}$$

The first inequality follows by combining the equality $n(R_S+\delta)=H(S_B)=H(S_B|K)$ and the security criteria in Eqs. (11) and (12). The first equality follows from the definition of mutual information. The second inequality follows because $H(M)_\omega=H(M|S_BK)_\omega$ (M, S_B, and K are independent) and conditioning does not increase entropy $H(E^n|K) \geq H(E^n|S_BK)$. The third inequality follows because the addition of a classical system can increase entropy $H(ME^n|K)_\omega \leq H(ME^nS_B|K)_\omega$. The second equality follows from the definition of conditional mutual information. The third equality follows from the chain rule of mutual information, and the last equality follows from the definitions $Y \equiv MS_B$ and $X \equiv K$.

We next prove the upper bound in Eq. (14) on the private communication rate:

$$
\begin{aligned}
n(P-\delta) &= H(M) = I(M;M'_B)_{\omega'} + H(M|M'_B) \leq I(M;M'_BK)_{\omega'} + n\delta' \leq I(M;B^nS_BK)_\omega + n\delta' \\
&= I(M;B^nK|S_B)_\omega + n\delta' = H(M|S_B) + H(B^nK|S_B)_\omega - H(MB^nS_BK) + H(S_B) + n\delta' \\
&= H(MS_B|K) - H(S_B|K) + H(B^nK|S_B)_\omega - H(MB^nS_BK) + H(S_B|K) + n\delta' \\
&= H(MS_B|K) + H(B^nK|S_B)_\omega - H(MB^nS_BK) + n\delta' \leq H(MS_B|K) + H(B^n)_\omega - H(MB^nS_BK) + H(K) - H(K) + n\delta' \\
&= I(MS_B;B^n|K)_\omega + n\delta' = I(Y;B^n|X)_\omega + n\delta'.
\end{aligned}
$$

The first equality follows by evaluating the entropy for the state $\bar{\Phi}^M$ and noting that $H(M)=H(M|K)$. The second equality follows by standard entropic relations. The first inequality follows from Eq. (17), Fano's inequality [54], and conditioning does not increase entropy. The second inequality is from quantum data processing. The third equality follows from the chain rule for mutual information and $I(M;S_B)=0$ because M and S_B are independent. The fourth equality follows by expanding the conditional mutual information. The fifth and sixth equalities follow from standard entropic relations. The last inequality follows because conditioning does not increase entropy $H(B^nK|S_B)_\omega \leq H(B^nK)_\omega$. The fifth equality follows by the definition of mutual information, and the last equality follows from the definitions $Y \equiv MS_B$, $X \equiv K$, and $\delta' \equiv \frac{1}{n}+\epsilon P$.

The second bound in Eq. (15) on the private communication rate follows from adding the bound in Eq. (14) to the bound in Eq. (16).

We can use a proof by contradiction to get the bound on the public rate R. Suppose that we have secret key available at some rate $>I(X;E^n)_\omega/n$. Then one could combine the public communication at rate R with the extra secret key in a one-time pad protocol in order to generate private communication at a rate $R+P$. The resulting protocol consumes secret key at a rate greater than $I(YX;E^n)$ because

$$
\frac{I(Y;E^n|X)_\omega}{n} + \frac{I(X;E^n)_\omega}{n} = \frac{I(YX;E^n)}{n}.
$$

The state ω is of the form given by the secret-key-assisted capacity theorem [20]. The total amount of private communication that a secret-key-assisted protocol can generate cannot be any larger than $I(YX;B^n)/n$ [20]. The chain rule also applies to the mutual information $I(YX;B^n)/n$:

$$
\frac{I(Y;B^n|X)_\omega}{n} + \frac{I(X;B^n)_\omega}{n} = \frac{I(YX;B^n)}{n}.
$$

If the public rate R were to exceed $I(X;B^n)_\omega/n$, then this public rate would contradict the optimality of the secret-key-assisted protocol from Ref. [20]. Thus, the public rate R must obey the bound in Eq. (13). ■

VI. PROOF OF THE DIRECT CODING THEOREM

The direct coding theorem is the proof of the following *publicly enhanced private father protocol resource inequality* (See Refs. [22,21] for the theory of resource inequalities):

$$
\begin{aligned}
\langle \mathcal{N} \rangle + I(Y;E|X)_\sigma[cc]_{\text{priv}} \geq I(Y;B|X)_\sigma[c \to c]_{\text{priv}} \\
+ I(X;B)_\sigma[c \to c]_{\text{pub}}. \quad (18)
\end{aligned}
$$

The resource inequality has an interpretation as the following statement: for any $\epsilon, \delta > 0$ and sufficiently large n, there exists a protocol that consumes $nI(Y;E|X)_\sigma$ bits of secret key and n independent uses of the noisy quantum channel $\mathcal{N}$ to generate $nI(Y;B|X)_\sigma$ bits of private communication and $nI(X;B)_\sigma$ bits of public communication with ϵ probability of error. In addition, Eve's state is ϵ close to a state that is independent of the private message and the secret key. The entropic quantities are with respect to the state σ^{XYBE} in Eq. (9).

The proof of the direct coding theorem proceeds similarly to the proof of the direct coding theorem for the classically enhanced father protocol from Ref. [29]. There are some subtle differences between the two proofs, and we highlight only the parts of the proof that are different from the proof of the classically enhanced father protocol. The proof begins by showing how to construct a *random private father code*, similar to the notion of a random father code [29] or a random quantum code [14]. We present the *channel input density operator* for a random private father code and show that

it is possible to make it close to a tensor-product state. We then show how to associate a classical string to a random private father code by exploiting the "code pasting" technique from Ref. [30]. The proof proceeds by applying the Holevo-Schumacher-Westmoreland (HSW) theorem [50,51] to show that Bob can decode the public information first. Based on the public information, Bob decodes the private information. The details of the proof involve showing how the random publicly enhanced private father code has low probability of error for decoding the public information and the private information. Finally, we employ the standard techniques of derandomization and expurgation to show that there exists a particular publicly enhanced private father code that achieves the rates given in Theorem 1.

A. Random Private Coding

We first recall the secret-key-assisted private communication capacity theorem (also known as the private father capacity theorem) [20].

Theorem 2. The secret-key-assisted private channel capacity region $C_{SKP}(\mathcal{N})$ is given by

$$C_{\mathrm{SKP}}(\mathcal{N}) = \overline{\bigcup_{l=1}^{\infty} \frac{1}{l} \tilde{C}^{(1)}_{\mathrm{SKP}}(\mathcal{N}^{\otimes l})}, \tag{19}$$

where the overbar indicates the closure of a set, and $\tilde{C}^{(1)}_{\mathrm{SKP}}(\mathcal{N})$ is the set of all $R_S \geq 0$, $P \geq 0$ such that

$$P \leq I(Y;B)_\rho - I(Y;E)_\rho + R_S, \tag{20}$$

$$P \leq I(Y;B)_\rho, \tag{21}$$

where R_S is the secret-key consumption rate and ρ is a state of the form

$$\rho^{YBE} \equiv \sum_y p(y)|y\rangle\langle y|^Y \otimes U^{A' \to BE}_{\mathcal{N}}(\rho^{A'}_y), \tag{22}$$

for some ensemble $\{p(y), \rho^{A'}_y\}$ and $U^{A' \to BE}_{\mathcal{N}}$ is an isometric extension of $\mathcal{N}$.

The *channel input density operator* $\rho^{A'^n}(\mathcal{C})$ for a private father code $\mathcal{C} \equiv \{\rho^{A'^n}_m\}_{m \in [M]}$ is a uniform mixture of all the private code words $\rho^{A'^n}_m$ in code $\mathcal{C}$

$$\rho^{A'^n}(\mathcal{C}) \equiv \frac{1}{M} \sum_{m=1}^{M} \rho^{A'^n}_m.$$

We cannot say much about the channel input density operator $\rho^{A'^n}(\mathcal{C})$ for a particular private father code $\mathcal{C}$. But we can say something about the expected channel input density operator of a random private father code $\mathcal{C}$ (where $\mathcal{C}$ itself becomes a random variable).

Definition 1. A random private father code is an ensemble $\{p_{\mathcal{C}}, \mathcal{C}\}$ of codes where each code $\mathcal{C}$ occurs with probability $p_{\mathcal{C}}$. The expected channel input density operator $\bar{\rho}^{A'^n}$ is as follows:

$$\bar{\rho}^{A'^n} \equiv \mathbb{E}_{\mathcal{C}}\{\rho^{A'^n}(\mathcal{C})\}. \tag{23}$$

A random private father code is "ρ-like" if the expected channel input density operator is close to a tensor power of some state ρ

$$\|\bar{\rho}^{A'^n} - \rho^{\otimes n}\|_1 \leq \epsilon. \tag{24}$$

We now state a version of the direct coding theorem that applies to random private father codes. The proof shows that we can produce a random secret-key-assisted private code with an expected channel input density operator close to a tensor power state.

Proposition 3. For any $\epsilon, \delta > 0$ and all sufficiently large n, there exists a random $\rho^{A'}$-like secret-key-assisted private code for a channel $\mathcal{N}^{A' \to B}$ such that

$$\|\bar{\rho}^{A'^n} - (\rho^{A'})^{\otimes n}\|_1 \leq 2\epsilon + 4\sqrt[4]{\epsilon}, \tag{25}$$

where $\bar{\rho}^{A'^n}$ is defined in Eq. (23) and the state $\rho^{A'} \equiv \sum_y p(y)\rho^{A'}_y$. The random private code has private communication rate $I(Y;B)_\rho - \delta$ and secret-key consumption rate $I(Y;E)_\rho + \delta$. The entropic quantities are with respect to the state in Eq. (22).

The proof of Proposition 3 is an extension of the development in Appendix D of Ref. [30] and the development in Ref. [20].

Proof. Consider the density operator $\rho^{A'}$ where

$$\rho^{A'} = \sum_{y \in \mathcal{Y}} p(y)\rho^{A'}_y.$$

The nth extension of the above state as a tensor power state is as follows:

$$\rho^{A'^n} \equiv (\rho^{A'})^{\otimes n} = \sum_{y^n \in \mathcal{Y}^n} p^n(y^n)\rho^{A'^n}_{y^n},$$

where

$$\rho^{A'^n}_{y^n} \equiv \rho^{A'}_{y_1} \otimes \rho^{A'}_{y_2} \otimes \cdots \otimes \rho^{A'}_{y_n}.$$

We define the pruned distribution p'^n as follows:

$$p'^n(x^n) \equiv \begin{cases} p^n(y^n)/\sum_{y^n \in T^{Y^n}_\delta} p^n(y^n) & : y^n \in T^{Y^n}_\delta \\ 0 & : \text{else}, \end{cases}$$

where $T^{Y^n}_\delta$ denotes the δ typical set of sequences with length n. Let $\tilde{\rho}^{A'^n}$ denote the following "pruned state:"

$$\tilde{\rho}^{A'^n} \equiv \sum_{y^n \in T^{Y^n}_\delta} p'^n(y^n)\rho^{A'^n}_{y^n}. \tag{26}$$

For any $\epsilon > 0$ and sufficiently large n, the state $\rho^{A'^n}$ is close to $\tilde{\rho}'^n$ by the gentle measurement lemma [52] and because the probability [53] for sequences outside the typical set is small

$$\|\rho^{A'^n} - \tilde{\rho}^{A'^n}\|_1 \leq 2\epsilon.$$

For any density operator $\rho^{A'}$, it is possible to construct a secret-key-assisted private code that achieves the private

communication rate and secret-key consumption rate in Proposition 3.

Let $[M]$ denote a set of size $2^{n[I(Y;B)-c\delta]}$ for some constant c and let U_m denote $2^{n[I(Y;B)-c\delta]}$ random variables that we choose according to the pruned distribution $p'^n(y^n)$. The realizations u_m of the random variables U_m are sequences in $\mathcal{Y}^n$ and are the basis for constructing a secret-key-assisted private code $\mathcal{C}$ with the following code word ensemble:

$$\mathcal{C}=\{p'^n(u_m),\rho_{u_m}^{A^n}\}_m.$$

We then perform a decoding positive operator-valued measure with elements $\{\Lambda_m\}_{m\in[M]}$ and decryption map g, resulting in failure with probability $4\epsilon+20\sqrt{\epsilon}$ by the arguments in Ref. [20].

Suppose that we choose a particular secret-key-assisted private code $\mathcal{C}$ according to the above prescription. Its code density operator is

$$\rho^{A'^n}(\mathcal{C})=\frac{1}{M}\sum_{m=1}^{M}\rho_{u_m}^{A'^n}.$$

Suppose we now consider the secret-key-assisted private code chosen according to the above prescription as a *random* code $\mathcal{C}$ (where $\mathcal{C}$ is now a random variable). Let $\rho'^{A'^n}(\mathcal{C})$ be the channel input density operator for the random code before expurgation and $\rho^{A'^n}(\mathcal{C})$ its channel input density operator after expurgation

$$\rho'^{A'^n}(\mathcal{C})\equiv\frac{1}{M'}\sum_{m=1}^{M'}\rho_{U_m}^{A'^n},$$

$$\rho^{A'^n}(\mathcal{C})\equiv\frac{1}{M}\sum_{m=1}^{M}\rho_{U_m}^{A'^n},$$

where the primed variable M is the dimension before expurgation and the unprimed variable M' is that after expurgation (the corresponding rates are slightly different but identical for large n). Let $\bar{\rho}'^{A'^n}$ and $\bar{\rho}^{A'^n}$ denote the expectation of the above channel input density operators

$$\bar{\rho}'^{A'^n}\equiv\mathbb{E}_{\mathcal{C}}\{\rho'^{A'^n}(\mathcal{C})\},$$

$$\bar{\rho}^{A'^n}\equiv\mathbb{E}_{\mathcal{C}}\{\rho^{A'^n}(\mathcal{C})\}.$$

Choosing our code in the particular way that we did leads to an interesting consequence. The expectation of the density operator corresponding to Alice's codeword $\rho_{U_m}^{A'^n}$ is equal to the pruned state in Eq. (26)

$$\mathbb{E}_{\mathcal{C}}\{\rho_{U_m}^{A'^n}\}=\sum_{y^n}p'^n(y^n)\rho_{y^n}^{A'^n},$$

because we choose the code words $\rho_{y^n}^{A'^n}$ randomly according to the pruned distribution $p'^n(y^n)$. Then the expected channel input density operator $\bar{\rho}'^{A'^n}$ is as follows:

$$\bar{\rho}'^{A'^n}=\mathbb{E}_{\mathcal{C}}\{\rho'^{A'^n}(\mathcal{C})\},\tag{27}$$

$$=\frac{1}{M'}\sum_{m=1}^{M'}\mathbb{E}_{\mathcal{C}}\{\rho_{U_m}^{A'^n}\},\tag{28}$$

$$=\sum_{y^n}p'^n(y^n)\rho_{y^n}^{A'^n}.\tag{29}$$

Then we know that the following inequality holds for $\bar{\rho}'^{A'^n}$ and the tensor power state $\rho^{A'^n}$:

$$\|\bar{\rho}'^{A'^n}-\rho^{A'^n}\|_1\leq 2\epsilon\tag{30}$$

by the typical subspace theorem and the gentle measurement lemma. The expurgation of any secret-key-assisted private code $\mathcal{C}$ has a minimal effect on the resulting channel input density operator [30]

$$\|\rho'^{A'^n}(\mathcal{C})-\rho^{A'^n}(\mathcal{C})\|_1\leq 4\sqrt[4]{\epsilon}.$$

The above inequality implies that the following one holds for the expected channel input density operators $\bar{\rho}'^{A'^n}$ and $\bar{\rho}^{A'^n}$:

$$\|\bar{\rho}'^{A'^n}-\bar{\rho}^{A'^n}\|_1\leq 4\sqrt[4]{\epsilon},\tag{31}$$

because the trace distance is convex. The following inequality holds:

$$\|\bar{\rho}^{A'^n}-\rho^{A'^n}\|_1\leq 2\epsilon+4\sqrt[4]{\epsilon}\tag{32}$$

by applying the triangle inequality to Eqs. (30) and (31). Therefore, the random secret-key-assisted private code is ρ-like. ■

B. Associating a Random Private Code with a Classical String

Suppose that we have an ensemble $\{p(x),\rho_x\}_{x\in\mathcal{X}}$ of quantum states. The density operator ρ_x arises as the expected density operator of another ensemble $\{p(y|x),\rho_{x,y}\}$. Let $x^n\equiv x_1\cdots x_n$ denote a classical string generated by the density $p(x)$ where each symbol $x_i\in\mathcal{X}$. Then there is a density operator ρ_{x^n} corresponding to the string x^n where

$$\rho_{x^n}\equiv\bigotimes_{i=1}^{n}\rho_{x_i}.$$

Suppose that we label a random private code by the string x^n and let $\bar{\rho}_{x^n}^{A'^n}$ denote its expected channel input density operator.

Definition 2. A random private code is (ρ_{x^n})-like if the expected channel input density operator $\bar{\rho}_{x^n}^{A'^n}$ is close to the state ρ_{x^n}

$$\|\bar{\rho}_{x^n}^{A'^n}-\rho_{x^n}\|_1\leq\epsilon.$$

Proposition 4. Suppose we have an ensemble as above. Consider a quantum channel $\mathcal{N}^{A'\to B}$ with its isometric extension $U_{\mathcal{N}}^{A'\to BE}$. Then there exists a random (ρ_{x^n})-like secret-key-assisted private code for the channel $\mathcal{N}^{A'\to B}$ for any $\epsilon,\delta>0$, for all sufficiently large n, and for any classical string x^n in the typical set $T_\delta^{X^n}$ (Ref. [54] explains the idea of

the typical set). Its private communication rate is $I(Y;B|X)-c'\delta$, and its secret-key consumption rate is $I(Y;E|X)-c''\delta$ for some constants c',c'' where the entropic quantities are with respect to the state in Eq. (9). The state ρ_x is the restriction of the following state:

$$\rho_x^{YA'} = \sum_y p(y|x)|y\rangle\langle y|^Y \otimes \rho_{x,y}^{A'}$$

to the A' system.

Proof (Proposition 4). The proof of this theorem proceeds exactly as the proof of Proposition 3 in Ref. [29] and the proof of Proposition 5 in Ref. [30]. ■

C. Publicly enhanced secret-key-assisted private code

Proposition 5. (HSW Coding Theorem [50,51]) Consider an input ensemble $\{p(x),\rho_x^{A'}\}$ that gives rise to a classical-quantum state σ^{XB}, where

$$\sigma^{XB} \equiv \sum_{x\in\mathcal{X}} p(x)|x\rangle\langle x|^X \otimes \mathcal{N}^{A'\to B}(\rho_x^{A'}).$$

Let $R=I(X;B)_\sigma-c'\delta$ for any $\delta>0$ and for some constant c'. Then for all $\epsilon>0$ and for all sufficiently large n, there exists a classical encoding map

$$h:[2^{nR}] \to T_\delta^{X^n},$$

and a decoding POVM

$$\{\Lambda_k^{B^n}\}_{k\in[2^{nR}]},$$

that allows Bob to decode any classical message $k\in[2^{nR}]$ with high probability

$$\mathrm{Tr}\{\tau_k^{B^n}\Lambda_k^{B^n}\} \geq 1-\epsilon.$$

The density operators $\tau_k^{B^n}$ are the channel outputs

$$\tau_k^{B^n} \equiv \mathcal{N}^{A'^n\to B^n}(\rho_{h(k)}^{A'^n}), \tag{33}$$

and the channel input states $\rho_{x^n}^{A'^n}$ are a tensor product of states in the ensemble

$$\rho_{x^n}^{A'^n} \equiv \bigotimes_{i=1}^n \rho_{x_i}^{A'}.$$

We are now in a position to prove the direct coding part of the publicly enhanced private father capacity theorem. The proof is similar to that in Refs. [30,29].

Proof (Direct Coding Theorem). Define the public message set $[2^{nR}]$, the classical encoding map h, the channel output states $\tau_k^{B^n}$, and the decoding POVM $\{\Lambda_k^{B^n}\}_{k\in 2^{nR}}$ as in Proposition 5. We label each public message $k\in[2^{nR}]$ where $R=I(X;B)-c'\delta$.

Invoking Proposition 4, there exists a random $(\rho_{h(k)}^{A'^n})$-like private code $\mathcal{C}_k$ with probability density $p_{\mathcal{C}_k}$ because each input to the channel $\rho_{h(k)}^{A'^n}$ is a tensor product of an ensemble $\{p(x),\rho_x^{A'}\}$. The random private code $\mathcal{C}_k$ has encryption-decryption pair $(f_{\mathcal{C}_k},g_{\mathcal{C}_k})$ and encoding-decoding pair $(\mathcal{E}_{\mathcal{C}_k},\mathcal{D}_{\mathcal{C}_k})$ for each of its realizations. We label the combined operations simply as the pair $(\mathcal{E}_{\mathcal{C}_k}^{MS_A\to A'^n},\mathcal{D}_{\mathcal{C}_k}^{B^nS_B\to M})$. It transmits $n[I(Y;B|X)+c'\delta]$ private bits, provided Alice and Bob share at least $n[I(Y;E|X)+c''\delta]$ secret-key bits.

Let $\mathcal{C}$ denote the *random publicly enhanced secret-key-assisted private code* that is the collection of random private codes $\{\mathcal{C}_k\}_{k\in[2^{nR}]}$. We first prove that the expectation of the error probability for public message k is small. The expectation is with respect to the random private code $\mathcal{C}_k$. Let $\tau_{\mathcal{C}_k}^{B^n}$ denote the *channel output density operator* corresponding to the private code $\mathcal{C}_k$

$$\tau_{\mathcal{C}_k}^{B^n} \equiv \mathrm{Tr}_{S_B}\{\mathcal{N}^{A'^n\to B^n}[\mathcal{E}_{\mathcal{C}_k}^{MS_A\to A'^n}(\pi^M\otimes\bar{\Phi}^{S_AS_B})]\}.$$

Let $\bar{\tau}_k^{B^n}$ denote the *expected channel output density operator* of the random father code $\mathcal{C}_k$

$$\bar{\tau}_k^{B^n} \equiv \mathbb{E}_{\mathcal{C}_k}\{\tau_{\mathcal{C}_k}^{B^n}\} = \sum_{\mathcal{C}_k} p_{\mathcal{C}_k}\tau_{\mathcal{C}_k}^{B^n}.$$

The following inequality holds:

$$\|\bar{\rho}_{h(k)}^{A'^n} - \rho_{h(k)}^{A'^n}\|_1 \leq |\mathcal{X}|\epsilon$$

because the random private code $\mathcal{C}_k$ is $(\rho_{h(k)}^{A'^n})$-like. Then the expected channel output density operator $\bar{\tau}_k^{B^n}$ is close to the tensor product state $\tau_k^{B^n}$ in Eq. (33)

$$\|\bar{\tau}_k^{B^n} - \tau_k^{B^n}\|_1 \leq |\mathcal{X}|\epsilon, \tag{34}$$

because the trace distance is monotone under the quantum operation $\mathcal{N}^{A'^n\to B^n}$. It follows that the POVM element $\Lambda_k^{B^n}$ has a high probability of detecting the expected channel output density operator $\bar{\tau}_k^{B^n}$

$$\mathrm{Tr}\{\Lambda_k^{B^n}\bar{\tau}_k^{B^n}\} \geq \mathrm{Tr}\{\Lambda_k^{B^n}\tau_k^{B^n}\} - \|\bar{\tau}_k^{B^n}-\tau_k^{B^n}\|_1 \geq 1-\epsilon-|\mathcal{X}|\epsilon. \tag{35}$$

The first inequality follows from the following lemma that holds for any two quantum states ρ and σ and a positive operator Π where $0\leq\Pi\leq I$:

$$\mathrm{Tr}\{\Pi\rho\} \geq \mathrm{Tr}\{\Pi\sigma\} - \|\rho-\sigma\|_1.$$

The second inequality follows from Proposition 5 and Eq. (34). Let $p_{e,\mathrm{pub}}(\mathcal{C}_k)$ denote the public message error probability for each public message k of the publicly enhanced father code $\mathcal{C}$

$$p_{e,\mathrm{pub}}(\mathcal{C}_k) \equiv 1-\Pr\{K'=k|K=k\}.$$

Then by the above definition, and Eq. (35), it holds that the expectation of the error probability $p_{e,\mathrm{pub}}(\mathcal{C}_k)$ for public message k with respect to the random private code $\mathcal{C}_k$ is low

$$\mathbb{E}_{\mathcal{C}_k}\{p_{e,\mathrm{pub}}(\mathcal{C}_k)\} = 1-\mathrm{Tr}\{\Lambda_k^{B^n}\bar{\tau}_k^{B^n}\}, \tag{36}$$

$$\leq (1+|\mathcal{X}|)\epsilon. \tag{37}$$

We now show that the private error is small. Input the state $\pi^M \otimes \bar{\Phi}^{S_A S_B}$ to the encoder $\mathcal{E}_{\mathcal{C}_k}^{MS_A \to A'^n}$, followed by the channel $\mathcal{N}^{A'^n \to B^n}$. The resulting state is an extension $\Omega_{\mathcal{C}_k}^{S_B B^n}$ of $\tau_{\mathcal{C}_k}^{B^n}$

$$\Omega_{\mathcal{C}_k}^{S_B B^n} \equiv \mathcal{N}^{A'^n \to B^n}[\mathcal{E}_{\mathcal{C}_k}^{MS_A \to A'^n}(\pi^M \otimes \bar{\Phi}^{S_A S_B})].$$

Let $\bar{\Omega}_k^{S_B B^n}$ denote the expectation of $\Omega_{\mathcal{C}_k}^{S_B B^n}$ with respect to the random code $\mathcal{C}_k$

$$\bar{\Omega}_k^{S_B B^n} \equiv \mathbb{E}_{\mathcal{C}_k}\{\Omega_{\mathcal{C}_k}^{S_B B^n}\}.$$

It follows that $\bar{\Omega}_k^{S_B B^n}$ is an extension of $\bar{\tau}_k^{B^n}$. The following inequality follows from Eq. (35):

$$\mathrm{Tr}\{\bar{\Omega}_k^{S_B B^n} \Lambda_k^{B^n}\} \geq 1 - (1 + |\mathcal{X}|)\epsilon. \tag{38}$$

The above inequality is then sufficient for us to apply a modified version of the gentle measurement lemma (see Appendix C of Ref. [29]) so that the following inequality holds:

$$\mathbb{E}_{\mathcal{C}_k}\{\| \sqrt{\Lambda_k^{B^n}} \Omega_{\mathcal{C}_k}^{S_B B^n} \sqrt{\Lambda_k^{B^n}} - \Omega_{\mathcal{C}_k}^{S_B B^n} \|_1\} \leq \sqrt{8(1 + |\mathcal{X}|)\epsilon}. \tag{39}$$

We define a decoding instrument $\mathcal{D}_{\mathcal{C}}^{B^n S_B \to KM}$ for the random publicly enhanced private father code $\mathcal{C}$ as follows [29,55]:

$$\mathcal{D}_{\mathcal{C}}^{B^n S_B \to KM}(\rho^{B^n S_B}) \equiv \sum_k \mathcal{D}_{\mathcal{C}_k}^{B^n S_B \to M}(\sqrt{\Lambda_k^{B^n}} \rho^{B^n S_B} \sqrt{\Lambda_k^{B^n}}) \otimes |k\rangle\langle k|^K,$$

where $\mathcal{D}_{\mathcal{C}_k}^{B^n S_B \to M}$ is the decoder for the private father code $\mathcal{C}_k$ and each map $\mathcal{D}_{\mathcal{C}_k}^{B^n S_B \to M}(\sqrt{\Lambda_k^{B^n}} \rho^{B^n S_B} \sqrt{\Lambda_k^{B^n}})$ is trace reducing. The induced quantum operation corresponding to this instrument is as follows:

$$\mathcal{D}_{\mathcal{C}}^{B^n S_B \to M}(\rho) = \mathrm{Tr}_K\{\mathcal{D}_{\mathcal{C}}^{B^n S_B \to KM}(\rho)\}.$$

Monotonicity of the trace distance gives an inequality for the trace-reducing maps of the quantum decoding instrument

$$\begin{aligned}&\mathbb{E}_{\mathcal{C}_k}\{\| \mathcal{D}_{\mathcal{C}_k}^{B^n S_B \to M}(\sqrt{\Lambda_k^{B^n}} \Omega_{\mathcal{C}_k}^{S_B B^n} \sqrt{\Lambda_k^{B^n}}) - \mathcal{D}_{\mathcal{C}_k}^{B^n S_B \to M}(\Omega_{\mathcal{C}_k}^{S_B B^n}) \|_1\} \\ &\quad \leq \sqrt{8(1 + |\mathcal{X}|)\epsilon}. \end{aligned} \tag{40}$$

The following inequality also holds:

$$\begin{aligned}&\mathbb{E}_{\mathcal{C}_k}\{\| \mathcal{D}_{\mathcal{C}}^{B^n S_B \to M}(\Omega_{\mathcal{C}_k}^{S_B B^n}) - \mathcal{D}_{\mathcal{C}_k}^{B^n S_B \to M}(\sqrt{\Lambda_k^{B^n}} \Omega_{\mathcal{C}_k}^{S_B B^n} \sqrt{\Lambda_k^{B^n}}) \|_1\} \\ &\quad \leq \mathbb{E}_{\mathcal{C}_k}\left\{ \sum_{k' \neq k} \| \mathcal{D}_{\mathcal{C}_{k'}}^{B^n S_B \to M}(\sqrt{\Lambda_{k'}^{B^n}} \Omega_{\mathcal{C}_k}^{S_B B^n} \sqrt{\Lambda_{k'}^{B^n}}) \|_1 \right\} \\ &\quad = \mathbb{E}_{\mathcal{C}_k}\left\{ \sum_{k' \neq k} \| \sqrt{\Lambda_{k'}^{B^n}} \Omega_{\mathcal{C}_k}^{S_B B^n} \sqrt{\Lambda_{k'}^{B^n}} \|_1 \right\} \\ &\quad = \mathbb{E}_{\mathcal{C}_k}\left\{ \sum_{k' \neq k} \mathrm{Tr}\{\Lambda_{k'}^{B^n} \Omega_{\mathcal{C}_k}^{S_B B^n}\} \right\} \\ &\quad = 1 - \mathrm{Tr}\{\Lambda_k^{B^n} \bar{\Omega}_k^{S_B B^n}\} \\ &\quad \leq (1 + |\mathcal{X}|)\epsilon. \end{aligned} \tag{41}$$

The first inequality follows by definitions and the triangle inequality. The first equality follows because the trace distance is invariant under isometry. The second equality follows because the operator $\Lambda_k^{B^n} \Omega_{\mathcal{C}_k}^{S_B B^n}$ is positive. The third equality follows from some algebra, and the second inequality follows from Eq. (35). The private communication for all public messages k and codes $\mathcal{C}_k$ is good

$$\| \mathcal{D}_{\mathcal{C}_k}^{B^n S_B \to M}(\Omega_{\mathcal{C}_k}^{S_B B^n}) - \pi^M \|_1 \leq \epsilon,$$

because each code $\mathcal{C}_k$ in the random private father code is good for private communication. It then follows that:

$$\mathbb{E}_{\mathcal{C}_k}\{\| \mathcal{D}_{\mathcal{C}_k}^{B^n S_B \to M}(\Omega_{\mathcal{C}_k}^{S_B B^n}) - \pi^M \|_1\} \leq \epsilon. \tag{42}$$

Application of the triangle inequality to Eqs. (42), (41), and (40) gives the following bound on the expected private error probability:

$$\mathbb{E}_{\mathcal{C}_k}\{p_{e,\mathrm{priv}}(\mathcal{C}_k)\} \leq \epsilon', \tag{43}$$

where

$$\epsilon' \equiv (1 + |\mathcal{X}|)\epsilon + \sqrt{8(1 + |\mathcal{X}|)\epsilon} + 2\sqrt{\epsilon},$$

and where we define the private error $p_{e,\mathrm{priv}}(\mathcal{C}_k)$ of the code $\mathcal{C}_k$ as follows:

$$p_{e,\mathrm{priv}}(\mathcal{C}_k) \equiv \| \mathcal{D}_{\mathcal{C}}^{S_B \to M}(\Omega_{\mathcal{C}_k}^{S_B B^n}) - \pi^M \|_1.$$

The above random publicly enhanced secret-key-assisted private code relies on Alice and Bob having access to a source of common randomness. We now show that they can eliminate the need for common randomness and select a good publicly enhanced secret-key-assisted private code $\mathcal{C}$ that has a low public error $p_{e,\mathrm{pub}}(\mathcal{C}_k)$ and low private error $p_{e,\mathrm{priv}}(\mathcal{C}_k)$ for all public messages in a large subset of $[2^{nR}]$. By the bounds in Eqs. (36) and (43), the following bound holds for the expectation of the averaged summed error probabilities:

$$\mathbb{E}_{\mathcal{C}_k}\left\{ \frac{1}{2^{nR}} \sum_k p_{e,\mathrm{pub}}(\mathcal{C}_k) + p_{e,\mathrm{priv}}(\mathcal{C}_k) \right\} \leq \epsilon' + (1 + |\mathcal{X}|)\epsilon.$$

If the above bound holds for the expectation over all random codes, it follows that there exists a particular publicly enhanced private father code $\mathcal{C} = \{\mathcal{C}_k\}_{k \in [2^{nR}]}$ with the following bound on its averaged summed error probabilities:

$$\frac{1}{2^{nR}} \sum_k p_{e,\mathrm{pub}}(\mathcal{C}_k) + p_{e,\mathrm{priv}}(\mathcal{C}_k) \leq \epsilon' + (1 + |\mathcal{X}|)\epsilon.$$

We fix the code $\mathcal{C}$ and expurgate the worst half of the private father codes—those private father codes with public messages k that have the highest value of $p_{e,\mathrm{pub}}(\mathcal{C}_k) + p_{e,\mathrm{priv}}(\mathcal{C}_k)$. This derandomization and expurgation yields a publicly enhanced private father code that has each public error $p_{e,\mathrm{pub}}(\mathcal{C}_k)$ and each private error $p_{e,\mathrm{priv}}(\mathcal{C}_k)$ upper bounded by $2(\epsilon' + (1 + |\mathcal{X}|)\epsilon)$ for the remaining public messages k. This expurgation decreases the public rate by an asymptotically negligible factor of $\frac{1}{n}$. ■

VII. CHILD PROTOCOLS

Two simple protocols for the public-private setting are *secret-key distribution* and the *one-time pad* [46,47]. Secret-

key distribution is a protocol where Alice creates the state $\bar{\Phi}^{AA'}$ locally and sends the system A' through a noiseless private channel. The protocol creates a secret key and corresponds to the following resource inequality:

$$[c \to c]_{\text{priv}} \geq [cc]_{\text{priv}}.$$

The one-time pad protocol exploits a secret key and a noiseless public channel to create a noiseless private channel. It admits the following resource inequality:

$$[c \to c]_{\text{pub}} + [cc]_{\text{priv}} \geq [c \to c]_{\text{priv}}.$$

We now consider some protocols that are child protocols of the publicly enhanced private father protocol. Consider the resource inequality in Eq. (18). We can combine the protocol with secret-key distribution, and we recover the protocol suggested in Sec. IV of Ref. [30]:

$$\begin{aligned}
&\langle \mathcal{N} \rangle + I(Y;E|X)_\sigma [cc]_{\text{priv}} \\
&\quad \geq I(Y;B|X)_\sigma [c \to c]_{\text{priv}} + I(X;B)_\sigma [c \to c]_{\text{pub}}. \\
&\geq [I(Y;B|X)_\sigma - I(Y;E|X)_\sigma][c \to c]_{\text{priv}} + I(Y;E|X)_\sigma [c \to c]_{\text{priv}} \\
&\quad + I(X;B)_\sigma [c \to c]_{\text{pub}} \geq [I(Y;B|X)_\sigma - I(Y;E|X)_\sigma][c \to c]_{\text{priv}} \\
&\quad + I(Y;E|X)_\sigma [cc]_{\text{priv}} + I(X;B)_\sigma [c \to c]_{\text{pub}}.
\end{aligned}$$

By cancellation of the secret-key term, we are left with the following resource inequality:

$$\begin{aligned}
\langle \mathcal{N} \rangle + o[cc]_{\text{priv}} \geq (I(Y;B|X)_\sigma - I(Y;E|X)_\sigma)[c \to c]_{\text{priv}} \\
+ I(X;B)_\sigma [c \to c]_{\text{pub}},
\end{aligned}$$

where $o[cc]_{\text{priv}}$ represents a sublinear amount of secret-key consumption.

We can combine the publicly enhanced private father protocol with the one-time pad

$$\begin{aligned}
&\langle \mathcal{N} \rangle + I(Y;E|X)_\sigma [cc]_{\text{priv}} + I(X;B)_\sigma [cc]_{\text{priv}} \\
&\quad \geq I(Y;B|X)_\sigma [c \to c]_{\text{priv}} + I(X;B)_\sigma [c \to c]_{\text{pub}} \\
&\quad + I(X;B)_\sigma [cc]_{\text{priv}}, \qquad (44)
\end{aligned}$$

$$\begin{aligned}
&\geq I(Y;B|X)_\sigma [c \to c]_{\text{priv}} + I(X;B)_\sigma [c \to c]_{\text{priv}} \\
&= I(XY;B)_\sigma [c \to c]_{\text{priv}}. \qquad (45)
\end{aligned}$$

This protocol is one for secret-key-assisted transmission of private information. It is not an efficient protocol because the optimal secret-key-assisted protocol [20] implements the following resource inequality:

$$\langle \mathcal{N} \rangle + I(XY;E)_\sigma [cc]_{\text{priv}} \geq I(XY;B)_\sigma [c \to c]_{\text{priv}}.$$

For a channel with nonzero private capacity so that $I(X;B)_\sigma - I(X;E)_\sigma > 0$, the protocol in Eq. (45) is not efficient because it uses more secret key than necessary. This inefficiency is similar to the inefficiency that we found for combining the classically enhanced father protocol with teleportation (see Sec. VII of Ref. [29]). It is not surprising that this inefficiency occurs because the publicly enhanced private father protocol is the public-private analog of the classically enhanced father protocol and the one-time pad protocol is the public-private analog of the teleportation protocol [9].

VIII. CONCLUSION

We have presented an optimal protocol, the publicly enhanced private father protocol, that exploits a secret key and a large number of independent uses of a noisy quantum to transmit public and private information. Several protocols in the literature are now special cases of this protocol.

Some open questions remain. It remains to determine the capacity regions of a multiple-access quantum channel [48,56] and a broadcast channel [32] for transmitting public and private information while consuming a secret key. One might also consider the five-dimensional region corresponding to the scenario where Alice and Bob consume secret key, entanglement, and a noisy quantum channel to produce quantum communication, public classical communication, and private classical communication. This scenario might give more insight into the privacy/coherence correspondence. It remains open to determine the full triple tradeoff for the use of a quantum channel in connection with public communication, private communication, and secret key. We have made initial progress on this problem by exploiting techniques developed in Ref. [39]. Before completing this work, we need to determine a publicly assisted private mother protocol, the analog of the classically assisted mother protocol in Refs. [21,39]. This protocol should then allow us to determine the full triple tradeoff for both the dynamic setting and the static setting.

ACKNOWLEDGMENTS

The authors thank Igor Devetak for a private discussion regarding the issue in Sec. III with the protocol for private communication. M.M.W acknowledges partial support from an internal research and development grant (Grant No. SAIC-1669) of Science Applications International Corporation.

[1] B. Terhal, IBM J. Res. Dev. **48**, 71 (2004).
[2] C. H. Bennett and G. Brassard, *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, New York, 1984), pp. 175–179.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[5] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[6] Z. Luo and I. Devetak, Phys. Rev. A **75**, 010303(R) (2007).

[7] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[8] B. Schumacher and M. D. Westmoreland, Phys. Rev. Lett. **80**, 5695 (1998).
[9] D. Collins and S. Popescu, Phys. Rev. A **65**, 032321 (2002).
[10] N. Gisin, R. Renner, and S. Wolf, Algorithmica **34**, 389 (2002).
[11] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[12] T. S. Cubitt, F. Verstraete, W. Dür, and J. I. Cirac, Phys. Rev. Lett. **91**, 037902 (2003).
[13] J. Bae, T. Cubitt, and A. Acín, Phys. Rev. A **79**, 032304 (2009).
[14] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[15] N. Cai, A. Winter, and R. W. Yeung, Probl. Inf. Transm. **40**, 318 (2004).
[16] I. Devetak and A. Winter, Proc. R. Soc. London, Ser. A **461**, 207 (2005).
[17] J. Oppenheim, R. Spekkens, and A. Winter, e-print arXiv:quant-ph/0511247 (unpublished).
[18] M. Horodecki, J. Oppenheim, A. Winter, Nature (London) **436**, 673 (2005).
[19] M. Horodecki, J. Oppenheim, and A. Winter, Commun. Math. Phys. **269**, 107 (2006).
[20] M.-H. Hsieh, Z. Luo, and T. Brun, Phys. Rev. A **78**, 042306 (2008).
[21] I. Devetak, A. W. Harrow, and A. Winter, IEEE Trans. Inf. Theory **54**, 4587 (2008).
[22] I. Devetak, A. W. Harrow, and A. J. Winter, Phys. Rev. Lett. **93**, 230504 (2004).
[23] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Phys. Rev. Lett. **94**, 160502 (2005).
[24] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, Phys. Rev. Lett. **100**, 110502 (2008).
[25] P. Horodecki, M. Horodecki, and R. Horodecki, J. Mod. Opt. **47**, 347 (2000).
[26] K. Horodecki, M. Horodecki, P. Horodecki, D. Leung, and J. Oppenheim, IEEE Trans. Inf. Theory **54**, 2604 (2008).
[27] G. Smith and J. Yard, Science **321**, 1812 (2008).
[28] G. Smith and J. A. Smolin, Phys. Rev. Lett. **102**, 010501 (2009).
[29] M.-H. Hsieh and M. M. Wilde, e-print arXiv:0811.4227.
[30] I. Devetak and P. W. Shor, Commun. Math. Phys. **256**, 287 (2005).
[31] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).
[32] J. Yard, P. Hayden, and I. Devetak, e-print arXiv:quant-ph/0603098.
[33] C. H. Bennett and S. J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1992).
[34] D. Leung and G. Smith, e-print arXiv:0810.4931, Commun. Math. Phys. (to be published).
[35] R. Ahlswede and I. Csiszár, IEEE Trans. Inf. Theory **39**, 1121 (1993).
[36] R. Ahlswede and I. Csiszár, IEEE Trans. Inf. Theory **44**, 225 (1998).
[37] I. Devetak and A. Winter, IEEE Trans. Inf. Theory **50**, 3138 (2003).
[38] R. Renner, Ph.D. thesis, ETH Zurich, 2005.
[39] M.-H. Hsieh and M. M. Wilde, e-print arXiv:0901.3038.
[40] I. Devetak (private communication).
[41] B. Groisman, S. Popescu, and A. Winter, Phys. Rev. A **72**, 032317 (2005).
[42] F. Buscemi, e-print arXiv:0807.3594.
[43] F. Buscemi, e-print arXiv:0901.4506.
[44] I. Devetak, Phys. Rev. Lett. **97**, 140503 (2006).
[45] A. Abeyesinghe, Ph.D. thesis, California Institute of Technology, (2006).
[46] G. S. Vernam, Journal of the IEEE **55**, 109 (1926).
[47] C. E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).
[48] J. Yard, P. Hayden, and I. Devetak, IEEE Trans. Inf. Theory **54**, 3091 (2008).
[49] R. Alicki and M. Fannes, J. Phys. A **37**, L55 (2004).
[50] A. S. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
[51] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **56**, 131 (1997).
[52] A. Winter, IEEE Trans. Inf. Theory **45**(7), 2481 (1999).
[53] A. Winter, Ph.D. thesis, Universität Bielefeld, 1999.
[54] T. M. Cover and J. A. Thomas, *Elements of Information Theory* Series in Telecommunication (John Wiley and Sons, New York, 1991).
[55] J. Yard, Ph.D. thesis, Stanford University, 2005; e-print arXiv:quant-ph/0506050.
[56] M.-H. Hsieh, I. Devetak, and A. Winter, IEEE Trans. Inf. Theory **54**, 3078 (2008).