Secure Communication with Unreliable Entanglement Assistance: Interception and Loss

Meir Lederman, *Student Member, IEEE*, and Uzi Pereg, *Member, IEEE*

***Abstract*—Secure communication is considered with unreliable entanglement assistance, due to one of two reasons: Interception or loss. We consider two corresponding models. In the first model, Eve may intercept the entanglement resource. In the second model, Eve is passive, and the resource may dissipate to the environment beyond her reach. The operational principle of communication with unreliable entanglement assistance is to adapt the transmission rate to the availability of entanglement assistance, without resorting to feedback and repetition. For the passive model, we derive a multi-letter secrecy capacity formula for general channels, subject to a maximal error criterion and semantic security. For the interception model, we derive achievable rates, and a multi-letter formula for the special class of degraded channels. As an example, we consider the erasure channel and the amplitude damping channel. In the erasure channel, time division is optimal and we derive single-letter formulas for both models. In the amplitude damping channel, under interception, time division is not necessarily possible, and the boundary of our achievable region is disconnected. In the passive model, our rate region outperforms time division.**

***Index Terms*—Quantum communication, secrecy capacity, wiretap channel, entanglement assistance, semantic security.**

I. Introduction

Security poses a pivotal challenge in modern communications [1]. QKD protocols are designed to generate a key for subsequent encryption [2]. Physical layer security complements the cryptographic approach, and leverages the inherent disturbance of the physical channel to ensure security without relying on a key [3–6]. A quantum wiretap channel is modeled as a linear map $\mathcal{N}_{A\to BE}$, where the sender, Alice, transmits A, a receiver, Bob, obtains B, and a malicious third-party, Eve, holds E. The goal is for Alice to reliably send a message to Bob, while Eve gets negligible information.

Entanglement resources are useful in many applications, including physical-layer security [7, 8], and can significantly increase throughput [9, 10]. Unfortunately, it is a fragile resource [11]. In order to generate entanglement assistance in optical communication, the transmitter first prepares an entangled pair locally, and then transmits half of it [12]. Since photons are easily lost to the environment [13], current implementations incorporate a back channel to notify the transmitter in case of a failure, with numerous repetitions. This approach has clear disadvantages and may even result in system collapse. However, ensuring resilience and reliability is critical for developing future communication networks [14].

Communication with unreliable entanglement assistance was recently introduced in [15] as a setup where a back channel and repetition are not required. Instead, the rate is adapted to the availability of entanglement assistance. The principle of operation ensures reliability by design. Uncertain cooperation was originally studied in classical multi-user information theory [16], motivated by the engineering aspects of modern networks. The quantum model involves a point-to-point quantum channel and unreliable correlations [15, 17].

The secrecy capacity of a quantum wiretap channel has been investigated in various settings [18–20]. Cai et al. [21] and Devetak [22] considered the unassisted setting. Qi et al. [9] considered secure communication with entanglement assistance. In principle, pre-shared entanglement can be utilized to generate a joint key. However, Qi et al. [9] assume that Eve can also access Bob's resource. While this assumption may seem to contradict the no-cloning theorem, we provide an operational meaning below.

Here, we consider two security settings of a quantum wiretap channel with unreliable entanglement assistance. Before communication begins, the legitimate parties try to generate entanglement assistance. To this end, Alice prepares an entangled pair locally and transmits one particle. The particle may fail to reach Bob due to one of two reasons:

1) *Interception:* While the particle travels from the transmitter, Eve tries to steal it.
2) *Loss:* The particle is lost to the environment. Yet, Eve is passive and does not gain access to the resource.

In the optimistic case, Alice and Bob generate entanglement successfully prior to the transmission of information. Hence, Bob can decode the information while using the entangled resource, which is not available to Eve. However, in the pessimistic case, Bob must decode without it. Nonetheless, secrecy needs to be maintained, whether Bob, Eve, or a neutral environment hold the entangled resource.

Consider the following approach. Alice encodes two messages at rates R and R', unaware of whether Bob holds the entanglement resource or not. Whereas, Bob and Eve know whether the resource is in their possession. In practice, this is realized through heralded entanglement generation [15, Remark 2]. If the entangled resource is not available to Bob, then he decodes the first message alone; hence, the transmission rate is R. Whereas, given entanglement assistance, Bob decodes both messages, hence the overall rate is $R+R'$. The rate R is thus associated with information that is guaranteed to be sent, while R' with the excess information that entanglement

Parts of this work will be presented in the International Symposium on Information Theory (ISIT 2024) and were submitted to the Information Theory Workshop (ITW 2024).

assistance provides. In this manner, we adapt the transmission rate to the availability of entanglement assistance.

We establish an achievable rate region for communication with unreliable entanglement assistance under interception, and a multi-letter capacity formula under passive eavesdropper, both subject to a maximal error criterion and semantic security. In addition, we derive a multi-letter capacity formula also for the interception model for the class of degraded wiretap channels. To demonstrate our results, we consider the erasure channel and the amplitude damping channel. For the erasure channel, we show that time-division is optimal and we derive single-letter formulas for both models. For the amplitude damping channel, in the interception model, we encounter a phenomenon that is somewhat rare in network information theory [23]: Time sharing is impossible and the boundary of our achievable region is disconnected. In the passive model, our achievable region outperforms time division.

The paper is organized as follows. In Section II, we provide definitions and description for both models. In Section III, we give a brief review of related work. Our results are presented in Sections IV-VI. The achievability proof for the inner bound is given in Section VII, and the proof for the regularized characterization in Section VIII. Section IX is dedicated to summary and discussion.

II. Notations and Coding Definitions

A. Basic Definitions

We use the following notation conventions: Calligraphic letters $\mathcal{X},\mathcal{Y},\mathcal{Z},\dots$ denote finite sets. Uppercase letters $X,Y,Z,\dots$ represent random variables, while lowercase $x,y,z,\dots$ stand for their values. We use $x^j=(x_1,x_2,\dots,x_j)$ for a sequence of letters from the alphabet $\mathcal{X}$, and $[i:j]$ for the index set $\{i,i+1,\dots,j\}$ where $j>i$.

A quantum state is described by a density operator ρ on a Hilbert space $\mathcal{H}$. We denote the set of all density operators by $\mathscr{S}(\mathcal{H})$. The von Neumann entropy is defined as $H(\rho)\equiv-\mathrm{Tr}[\rho\log(\rho)]$. Given a bipartite state $\rho_{AB}\in\mathscr{S}(\mathcal{H}_A\otimes\mathcal{H}_B)$, the quantum mutual information is $I(A;B)_\rho=H(\rho_A)+H(\rho_B)-H(\rho_{AB})$. The conditional quantum entropy is defined by $H(A|B)_\rho=H(\rho_{AB})-H(\rho_B)$, and the quantum conditional mutual information is defined accordingly.

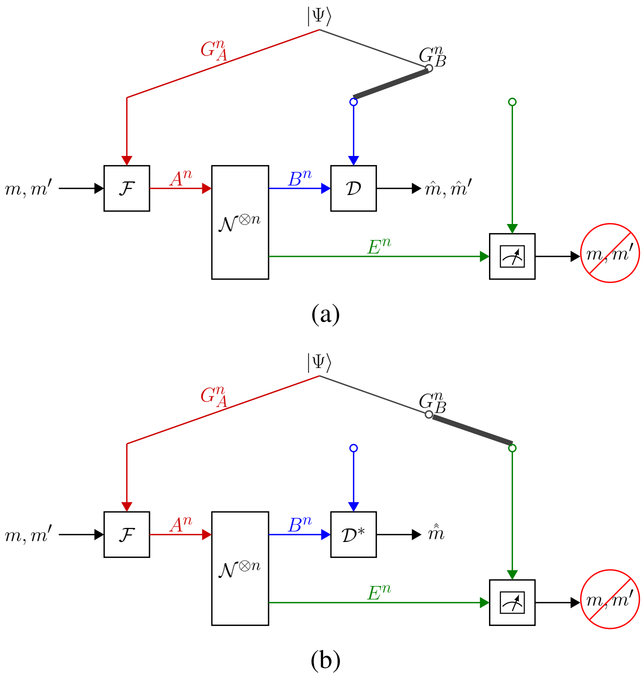
A quantum channel $\mathcal{L}_{A\to B}:\mathscr{S}(\mathcal{H}_A)\to\mathscr{S}(\mathcal{H}_B)$ is a linear completely-positive and trace-preserving (CPTP) map.

B. Wiretap Channel

A quantum wiretap channel $\mathcal{N}_{A\to BE}:\mathscr{S}(\mathcal{H}_A)\to\mathscr{S}(\mathcal{H}_B\otimes\mathcal{H}_E)$ maps a state at the sender's system to a joint state of the legitimate receiver and eavesdropper's systems. The sender, receiver, and eavesdropper are often referred to as Alice, Bob and Eve, respectively.

We denote the marginal channel, from Alice to Bob, by $\mathcal{L}_{A\to B}$, and the other marginal, from Alice to Eve, by $\overline{\mathcal{L}}_{A\to E}$. The marginal channels are also referred to as the main channel and the eavesdropper's channel, respectively. The quantum wiretap channel $\mathcal{N}_{A\to BE}$ is called *degraded* if there exists a degrading channel $\mathcal{P}_{B\to E}$ such that

$$\overline{\mathcal{L}}_{A\to E}=\mathcal{P}_{B\to E}\circ\mathcal{L}_{A\to B}\,. \tag{1}$$



(a)

(b)

Fig. 1. Interception illustration with an imaginary switch. As Eve may steal the resource, there are two scenarios: (a) "Left": Bob decodes both m and m'. (b) "Right": Bob decodes m alone.

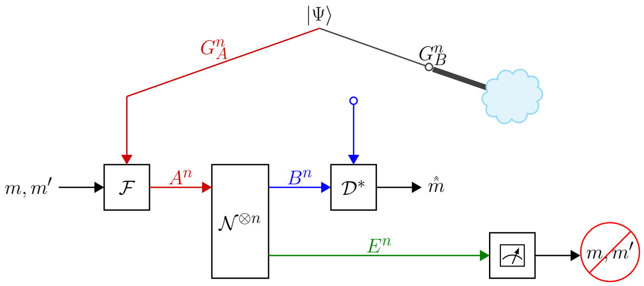


Fig. 2. Passive eavesdropper. The resource may get lost to the environment.

We assume that the channel is memoryless, i.e., if Alice sends a sequence of input systems $A^n\equiv(A_1,\dots,A_n)$, then the channel input ρ_{A^n} undergoes the tensor-product mapping $\mathcal{N}_{A\to BE}^{\otimes n}$.

C. Coding with Unreliable Assistance

Before communication begins, the legitimate parties try to generate entanglement assistance. In the optimistic case, Alice and Bob have entanglement resources, G_A^n and G_B^n, respectively (see Figure 1(a)). However, G_B^n is not necessarily available to Bob, due to either interception or loss.

In the communication phase, Alice sends n inputs through a memoryless quantum wiretap channel $\mathcal{N}_{A\to BE}$, while she is unaware of whether Bob has the entanglement resource.

Nevertheless, based on the common use of heralded entanglement generation in practical systems [24], we assume that Bob knows whether he has the assistance or not.

Definition 1. A $(2^{nR}, 2^{nR'}, n)$ code with unreliable entanglement assistance consists of the following:

- Two message sets $[1:2^{nR}]$ and $[1:2^{nR'}]$,
- a pure entangled state $\Psi_{G_A^n, G_B^n}$,
- a collection of encoding maps $\{\mathcal{F}^{(m,m')}_{G_A^n \to A^n}\}$, and
- two POVMs, $\mathcal{D}_{B^n G_B^n} = \{D_{m,m'}\}$ and $\mathcal{D}^*_{B^n} = \{D^*_m\}$.

The scheme is depicted in Figure 1. Alice holds G_A^n. She chooses two messages m and m', encodes by

$$\rho^{m,m'}_{A^n G_B^n} = (\mathcal{F}^{(m,m')}_{G_A^n \to A^n} \otimes \mathrm{id})(\Psi_{G_A^n G_B^n}) \tag{2}$$

and transmits A^n. The channel output is $\rho^{m,m'}_{B^n E^n G_B^n} = (\mathcal{N}^{\otimes n}_{A\to BE} \otimes \mathrm{id})(\rho^{m,m'}_{A^n G_B^n})$. Bob receives B^n. Depending on the availability of the entanglement assistance, Bob decides whether to decode both messages or only one. If G_B^n is available, Bob performs $\mathcal{D}_{B^n G_B^n}$ to recover both messages. Otherwise, Bob measures $\mathcal{D}^*_{B^n}$ and estimates m alone.

Remark 1. Our model considers two extreme scenarios, i.e., the entanglement resources are either entirely available to Bob or not at all. In digital communications, this strategy aligns with a *hard decision* approach [25]. Indeed, the decoder in our setting makes a hard decision on whether the entanglement resources are viable. This approach fundamentally differs from noisy entanglement models that ensure reliability with respect to the average state [26].

Remark 2. We observe that guaranteed information could have correlation with the receiver's entanglement resource. Indeed, the guaranteed information m needs to be encoded in such a manner that Bob could recover it even in the absence of the entanglement resource, see Figure 1(b), 2. Nevertheless, Alice encodes *her* resource G_A^n using an encoding map that depends on both m and m' (see (2)). As a result, the encoding operation may induce correlation between the guaranteed information m and the entangled resource G_B^n. We will see the consequences of this observation on the rate region formula in Section IV below, see Remarks 6 and 7.

We have two maximum error criteria: In the presence of entanglement assistance,

$$P_{e,\max}(\Psi, \mathcal{F}, \mathcal{D}) = \max_{m,m'} \left[1 - \mathrm{Tr}(D_{m,m'}\, \rho^{m,m'}_{B^n G_B^n})\right] ,$$

and without entanglement assistance,

$$P^*_{e,\max}(\Psi, \mathcal{F}, \mathcal{D}^*) = \max_{m} \left[1 - \mathrm{Tr}(D^*_m\, \rho^{m,m'}_{B^n})\right] . \tag{3}$$

Notice that both include m and m', since Alice does not know whether the assistance is available to Bob or not.

We consider two security settings.

D. Security Under Interception

Suppose that Eve may steal the entanglement resource G_B^n. In the pessimistic case, Eve intercepts the entanglement resource, and Bob decodes without it. In other words, Alice and *Eve* share the entanglement, instead of Bob. See Figure 1(b).

Semantic security requires that Eve cannot gain any information on Alice's message, regardless of the message distribution. Hence, the state of Eve's resources needs to be close to a *constant state* that does not depend on Alice's messages. Formally, define the security level under interception, with respect to a constant state $\theta_{E^n G_B^n}$, by

$$\Delta_{\mathrm{SI}}(\Psi, \mathcal{F}, \theta_{E^n G_B^n}) = \max_{m,m'} \frac{1}{2} \left\| \rho^{m,m'}_{E^n G_B^n} - \theta_{E^n G_B^n} \right\|_1 . \tag{4}$$

Notice that we include the entangled resource G_B^n in the indistinguishability criterion due to the pessimistic case above.

Definition 2. A $(2^{nR}, 2^{nR'}, n, \epsilon, \delta)$ code with unreliable entanglement assistance and security under interception satisfies $\max\left(P_{e,\max}(\Psi, \mathcal{F}, \ \mathcal{D}), P^*_{e,\max}(\Psi, \mathcal{F}, \mathcal{D}^*)\right) \leq \epsilon$, and there exists $\theta_{E^n G_B^n}$ such that $\Delta_{\mathrm{SI}}(\Psi, \mathcal{F}, \theta_{E^n G_B^n}) \leq \delta$. A rate pair (R, R') is called achievable if $\forall\ \epsilon, \delta > 0$ and large n, there is a $(2^{nR}, 2^{nR'}, n, \epsilon, \delta)$ code. The capacity region $\mathcal{C}_{\text{SI-EA}^*}(\mathcal{N})$ with unreliable entanglement assistance and security under interception is the closure of the set of all such pairs.

Remark 3. A straightforward method to leverage entanglement assistance is to generate a shared key, and then encode the information using the one-time pad protocol. However, this strategy poses a security risk in our case. If Eve intercepts the entanglement resource, then she will get a hold of Alice's key, resulting in a failure and a breach of security.

Remark 4. Eve's interception has severe consequences on entanglement-assisted communication. For example, suppose that Alice uses the superdense coding protocol to encode two classical bits, and then transmits her qubit via a quantum erasure channel. Consider the event that Bob receives an erasure, hence Eve receives the transmitted qubit. Nevertheless, without the entanglement resource, there is no leakage, because each qubit by itself has no correlation with Alice's messages. On the other hand, if Eve has both qubits, then she can use the superdense decoder in order to recover Alice's bits.

E. Passive Eavesdropper

The passive model assumes that Eve does not gain access to the resource G_B^n. In the pessimistic case, the entanglement resource is lost to the environment, and neither Bob nor Eve can benefit from it. See Figure 2. The security level is now

$$\Delta_{\mathrm{PE}}(\Psi, \mathcal{F}, \theta_{E^n}) = \max_{m,m'} \frac{1}{2} \left\| \rho^{m,m'}_{E^n} - \theta_{E^n} \right\|_1 \tag{5}$$

(cf. (4)). The security requirement for the passive model can thus be viewed as a relaxation of the one we had in the interception model. The capacity region $\mathcal{C}_{\text{PE-EA}^*}(\mathcal{N})$ is defined accordingly.

III. Previous Work

We provide a brief review of known results with and without secrecy, and with different levels of entanglement assistance. We denote the corresponding capacities as in Figure 3. Specifically, we denote the non-secure capacities, without entanglement assistance, with reliable entanglement assistance, and with unreliable entanglement assistance, by

	Unsecure	Interception
No assistance	$C_0(\mathcal{L})$	$C_{\text{S}}(\mathscr{N})$
Reliable Assistance	$C_{\text{EA}}(\mathcal{L})$	$C_{\text{SI-EA}}(\mathcal{N})$
Unreliable Assistance	$\mathcal{C}_{\text{EA}^*}(\mathcal{L})$	$\mathcal{C}_{\text{SI-EA}^*}(\mathcal{N})$

Fig. 3. Notation of channel capacities with and without secrecy, and with different levels of entanglement assistance. The first column corresponds to communication without a secrecy requirement, and the second column comprises secrecy capacities under interception.

$C_0(\mathcal{L})$, $C_{\text{EA}}(\mathcal{N})$, and $\mathcal{C}_{\text{EA}^*}(\mathcal{L})$, respectively. Similarly, we denote the secrecy capacities with interception by $C_{\text{S}}(\mathcal{N})$, $C_{\text{SI-EA}}(\mathcal{N})$, and $\mathcal{C}_{\text{SI-EA}^*}(\mathcal{N})$, respectively.

A. Unsecure Communication

At first, we consider communication over a quantum channel $\mathcal{L}_{A\to B}$, without a secrecy requirement. We review the capacity results without assistance, with reliable entanglement assistance, and with unreliable entanglement assistance.

1) No Assistance: Suppose that Alice and Bob do not share entanglement a priori. The Holevo information of the channel is defined as

$$\chi(\mathcal{L}) \equiv \max_{p_X(x),|\psi_A^x\rangle} I(X;B)_\omega \,, \tag{6}$$

where the maximization is over the ensemble of quantum input states $\{p_X(x), |\psi_A^x\rangle\}_{x\in\mathcal{X}}$, and

$$\omega_{XB} \equiv \sum_{x\in\mathcal{X}} p_X(x)\, |x\rangle\langle x| \otimes \mathcal{L}(|\psi_A^x\rangle\langle\psi_A^x|) \tag{7}$$

with $|\mathcal{X}| \leq \dim(\mathcal{H}_A)^2$.

Theorem 1 (see [27, 28]). The capacity of a quantum channel $\mathcal{L}_{A\to B}$ without secrecy and without assistance satisfies

$$C(\mathcal{L}) = \lim_{n\to\infty} \frac{1}{n}\chi(\mathcal{N}^{\otimes n}) \,. \tag{8}$$

2) Reliable Assistance: Consider entanglement-assisted communication, where it is assumed that the entanglement assistance is reliable with certainty. Let

$$I_{\text{EA}}(\mathcal{L}) = \max_{|\phi_{GA}\rangle} I(G;B)_\omega \,, \tag{9}$$

where the maximum is over all bipartite states $|\phi_{GA}\rangle$, and

$$\omega_{GB} = (\text{id}\otimes\mathcal{L})(|\phi_{GA}\rangle\langle\phi_{GA}|) \,, \tag{10}$$

with $\dim(\mathcal{H}_G) \leq \dim(\mathcal{H}_A)$. The system G in (10) can be interpreted as Bob's entanglement resource.

Theorem 2 (see [29]). The capacity of a quantum channel $\mathcal{L}_{A\to B}$ without secrecy and with (reliable) entanglement assistance is given by

$$C_{\text{EA}}(\mathcal{N}) = I_{\text{EA}}(\mathcal{L}) \,. \tag{11}$$

3) Unreliable Assistance: We move to communication with *unreliable* entanglement assistance [15], as presented in Subsection II-C, but without a secrecy requirement. Recall that Alice sends two messages, a guaranteed message at rate R and excess message at rate R', hence the performance is characterized by rate regions. Define

$$\mathcal{R}_{\text{EA}^*}(\mathcal{L}) = \bigcup_{p_X,\varphi_{G_1G_2},\mathcal{F}^{(x)}} \left\{ \begin{array}{rl} (R,R') \,:\, R \leq & I(X;B)_\omega \\ R' \leq & I(G_2;B|X)_\omega \end{array} \right\} , \tag{12}$$

where the union is over all auxiliary variables $X \sim p_X$, bipartite states $\varphi_{G_1G_2}$, and encoding channels $\mathcal{F}_{G_1\to A}^{(x)}$, with

$$\omega_{XG_2A} = \sum_{x\in\mathcal{X}} p_X(x)\, |x\rangle\langle x| \otimes (\text{id}\otimes\mathcal{F}_{G_1\to A}^{(x)})(\varphi_{G_2G_1}) \tag{13}$$

and

$$\omega_{XG_2B} = (\text{id}\otimes\mathcal{L}_{A\to B})(\omega_{XG_2A}) \,. \tag{14}$$

Theorem 3 (see [15]). The capacity region of a quantum channel $\mathcal{L}_{A\to B}$ with *unreliable* entanglement assistance satisfies

$$\mathcal{C}_{\text{EA}^*}(\mathcal{L}) = \bigcup_{n=1}^{\infty} \frac{1}{n}\mathcal{R}_{\text{EA}^*}(\mathcal{L}^{\otimes n}) \,. \tag{15}$$

B. Secure Communication

Consider a quantum wiretap channel $\mathcal{N}_{A\to BE}$. Here, we review the fundamental secrecy capacity results, without assistance and with reliable entanglement assistance. Secure communication with unreliable entanglement assistance will be addressed in the results section.

1) No Assistance: Suppose that Alice and Bob do not share entanglement a priori. The private information of the quantum wiretap channel is defined by

$$I_{\text{S}}(\mathcal{N}) \equiv \max_{p_X(x),\omega_A^x} [I(X;B)_\omega - I(X;E)_\omega] \,, \tag{16}$$

where the maximization is over the ensemble of quantum input states $\{p_X(x), \omega_A^x\}_{x\in\mathcal{X}}$, and

$$\omega_{XBE} \equiv \sum_{x\in\mathcal{X}} p_X(x)\, |x\rangle\langle x| \otimes \mathcal{N}_{A\to BE}(\omega_A^x) \,, \tag{17}$$

with $|\mathcal{X}| \leq \dim(\mathcal{H}_A)^2 + 1$.

Theorem 4 (see [21, 22]). The secrecy capacity of a quantum wiretap channel $\mathcal{N}_{A\to BE}$ without assistance is given by

$$C_{\text{S}}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} I_{\text{S}}(\mathcal{N}^{\otimes n}) \tag{18}$$

Furthermore, if the channel is degraded, then

$$\mathcal{C}_{\text{S}}(\mathcal{N}) = I_{\text{S}}(\mathcal{N}) \,. \tag{19}$$

A single-letter formula for the secrecy capacity remains an open problem for a general quantum wiretap channel. The secrecy capacity and the private information are both known to be super additive [30, 31].

2) Reliable Assistance: Qi et al. [9] consider secure communication under the assumption that the entanglement assistance is reliable and available to Bob, and yet, Eve could access the same resource. Define

$$I_{\text{SI-EA}}(\mathcal{N}) = \max_{\varphi_{AG}} [I(G;B)_\omega - I(G;E)_\omega] \,, \tag{20}$$

where the maximum is over all bipartite states φ_{AG}, and

$$\omega_{GBE} \equiv (\text{id} \otimes \mathcal{N}_{A\to BE})(\varphi_{GA}) \,. \tag{21}$$

Theorem 5 (see [9]). The secrecy capacity of a quantum wiretap channel $\mathcal{N}_{A\to BE}$ with (reliable) entanglement assistance is bounded by

$$C_{\text{SI-EA}}(\mathcal{N}) \geq I_{\text{SI-EA}}(\mathcal{N}) \,. \tag{22}$$

Furthermore, if the channel is degraded, then

$$\mathcal{C}_{\text{SI-EA}}(\mathcal{N}) = I_{\text{SI-EA}}(\mathcal{N}) \,. \tag{23}$$

A single-letter formula for the entanglement-assisted secrecy capacity is an open problem as well.

Remark 5. Qi et al. [9] assume that Eve can also access Bob's resource. While this assumption may seem to contradict the no-cloning theorem, our interception model provides an operational meaning to their setting.

IV. Results – Interception

We consider communication with unreliable entanglement assistance and semantic security. Recall that Alice does not know whether the entanglement resource has reached Bob's location, hence she encodes two messages, at rates R and R' (see the code definition in Section II-C). If entanglement assistance is available to Bob, he recovers both messages. Yet, in the interception model, if Eve has stolen the resource, then he recovers the first message alone. Nonetheless, we require the information to be secret from Eve in both scenarios (see security requirement in Section II-D).

A. Inner Bound

First, we establish an achievable secrecy rate region. Let $\mathcal{N}_{A\to BE}$ be a quantum wiretap channel. Define

$$\mathcal{R}_{\text{SI-EA*}}(\mathcal{N}) \equiv \bigcup_{p_X, \varphi_{G_1G_2}, \mathcal{F}^{(x)}} \left\{ \begin{array}{rl} (R,R') : & R \leq [I(X;B)_\omega - I(X;EG_2)_\omega]_+ \\ & R' \leq [I(G_2;B|X)_\omega - I(G_2;E|X)_\omega]_+ \end{array} \right\} \tag{24}$$

where $[x]_+ \equiv \max(x,0)$. The union is over all auxiliary variables $X \sim p_X$, bipartite states $\varphi_{G_1G_2}$, and encoding channels $\mathcal{F}^{(x)}_{G_1\to A}$, hence

$$\omega_{XG_2A} \equiv \sum_{x\in\mathcal{X}} p_X(x) \, |x\rangle\langle x| \otimes (\text{id} \otimes \mathcal{F}^{(x)}_{G_1\to A})(\varphi_{G_2G_1}) \,, \tag{25}$$

$$\omega_{XG_2BE} \equiv (\text{id} \otimes \text{id} \otimes \mathcal{N}_{A\to BE})(\omega_{XG_2A}) \,, \tag{26}$$

Remark 6. While the setting resembles layered secrecy broadcast models [32, 33], the analysis is much more involved, and the formulas have a different form. Specifically, instead of the mutual information term $I(X;E)_\omega$ in the private information formula, we now have $I(X;EG_2)_\omega$ that includes the receiver's entanglement resource, cf. (16) and (24).

Remark 7. Based on the model description, it may seem at a first glance as if X should not be correlated with G_2, since the guaranteed information needs to be recovered in the absence of the entanglement resource. However, as pointed out in Remark 2, Alice's encoding may induce correlation between the guaranteed information and the receiver's resource. Similarly, in the rate region formula, the application of the encoding channel $\mathcal{F}^{(x)}_{G_1\to A}$ could create correlation between X and G_2 (see (25)).

Our main result is given in the theorem below.

Theorem 6. The region $\mathcal{R}_{\text{SI-EA*}}(\mathcal{N})$ is achievable with unreliable entanglement assistance and semantic security under *interception*. That is, the capacity region is bounded by

$$\mathcal{C}_{\text{SI-EA*}}(\mathcal{N}) \supseteq \mathcal{R}_{\text{SI-EA*}}(\mathcal{N}) \tag{27}$$

The proof of Theorem 6 is given in Section VII. We modify the quantum superposition coding (SPC) scheme in [15] by inserting local randomness elements that are used in the encoding, one for each message, in order to confuse Eve. In the analysis, we use the quantum covering lemma [34] in a non-standard manner. In addition, our proof modifies the methods of Cai [35, 36], originally applied to multiple-access channels (without secrecy), using random message permutations.

Remark 8. In the coding scheme described in Section II-C, we specified that Bob applies one of two distinct POVMs, depending on who holds the entanglement resource — Bob or Eve. If Bob has entanglement assistance, then he performs $\mathcal{D}_{B^n G_B^n} = \{D_{m,m'}\}$ to decode both m and m'. Otherwise, if Eve has sabotaged his assistance, Bob performs $\mathcal{D}^*_{B^n} = \{D^*_m\}$ to decode m alone. Nonetheless, the quantum SPC scheme [15] employs a sequential decoder. On the first stage, Bob performs a measurement to obtain an estimate for the guaranteed message m. Then, Bob moves on to the second stage. In the presence of the entanglement resource, Bob performs a second measurement to estimate the excess message m', and in the absence of his resource, he aborts. The gentle measurement lemma [37, 38] guarantees that there is no collapse after the first measurement, i.e., the output state remains nearly unchanged.

	Unsecure	Interception	Passive Eavesdropper
No assistance	$C_0(\mathcal{L})$	$C_{\text{S}}(\mathscr{N})$	$C_{\text{S}}(\mathscr{N})$
Reliable Assistance	$C_{\text{EA}}(\mathcal{L})$	$C_{\text{SI-EA}}(\mathcal{N})$	$C_{\text{PE-EA}}(\mathcal{N})$
Unreliable Assistance	$\mathcal{C}_{\text{EA}*}(\mathcal{L})$	$\mathcal{C}_{\text{SI-EA}*}(\mathcal{N})$	$\mathcal{C}_{\text{PE-EA}*}(\mathcal{N})$

Fig. 4. Notation of channel capacities without secrecy, with interception and with passive eavesdropper, with different levels of entanglement assistance.

B. Regularized Capacity Formula

For the class of degraded channels, we establish a multi-letter capacity formula.

Theorem 7. Let $\mathcal{N}_{A\to BE}$ be a degraded quantum wiretap channel. The capacity region with unreliable entanglement assistance and semantic security under interception satisfies

$$\mathcal{C}_{\text{SI}}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n}\mathcal{R}_{\text{SI}}(\mathcal{N}^{\otimes n}) \tag{28}$$

The proof of Theorem 7 is given in Section VIII.

V. Results – Passive Eavesdropper

Here, we consider the model of a passive eavesdropper, where Eve cannot intercept the assistance. The entangled resource is unreliable as it may get lost to the environment. We denote the secrecy capacities without assistance, with reliable assistance, and with unreliable assistance with passive eavesdropper, by $C_{\text{S}}(\mathcal{N})$, $C_{\text{PE-EA}}(\mathcal{N})$, and $\mathcal{C}_{\text{PE-EA}*}(\mathcal{N})$, respectively, as shown in the right column in Figure 4.

Define

$$\mathcal{R}_{\text{PE-EA}*}(\mathcal{N}) \equiv \bigcup_{p_X,\varphi_{G_1G_2},\mathcal{F}^{(x)}} \left\{ \begin{array}{rl} (R,R')\,:\; R\leq & [I(X;B)_\omega - I(X;E)_\omega]_+ \\ R'\leq & I(G_2;B|X)_\omega \end{array} \right\} \tag{29}$$

where ω_{XG_2BE} is as in (26). Our main result for the passive model is given below.

Theorem 8. The region $\mathcal{R}_{\text{PE-EA}*}(\mathcal{N})$ is achievable with unreliable entanglement assistance and a passive eavesdropper. That is, the capacity region is bounded by

$$\mathcal{C}_{\text{PE-EA}*}(\mathcal{N}) \supseteq \mathcal{R}_{\text{PE-EA}*}(\mathcal{N})\,. \tag{30}$$

Furthermore, the capacity region with unreliable entanglement assistance and a passive eavesdropper satisfies

$$\mathcal{C}_{\text{PE-EA}*}(\mathcal{N}) = \bigcup_{n=1}^{\infty} \frac{1}{n}\mathcal{R}_{\text{PE-EA}*}(\mathcal{N}^{\otimes n}) \tag{31}$$

Notice that here we have a regularized formula for a general wiretap channel, and not just degraded channels (cf. Theorem 7 and Theorem 8).

The analysis follows similar steps as for Theorem 6, in Sections VII-VIII, with the following differences. Since the assistance remains secure from the eavesdropper in the passive model, Alice and Bob can use the entanglement resources in order to secure a shared secret key. Hence, we can achieve perfect secrecy for the excess message m' through one-time pad encryption. The assumption that the wiretap channel is degraded is not needed in the derivation of the multi-letter formula, as the bound on R' does not involve Eve's output E. The details are omitted.

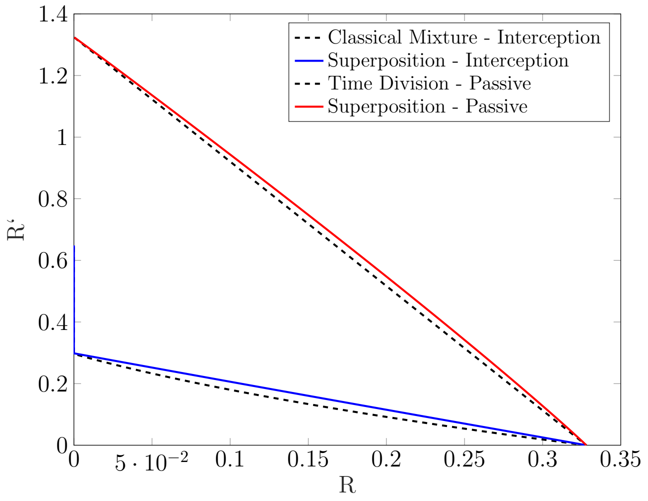


Fig. 5. Achievable rate regions for the amplitude damping channel with unreliable entanglement assistance and semantic security, for $\gamma = 0.3$

Remark 9. Consider the first row in Figure 4. Without any assistance, there is no meaning to the distinction between the interception and passive models. Therefore, we denote both secrecy capacities as $C_{\text{S}}(\mathcal{N})$. See the middle and last columns in the third rows. The basic results on $C_{\text{S}}(\mathcal{N})$ were briefly reviewed in III-B1.

Remark 10. We now consider the second row in Figure 4.If entanglement assistance is guaranteed, then security with a passive eavesdropper is straightforward in the sense that the entanglement between Alice and Bob can be used in order to secure a shared secret key and apply the one-time pad protocol to achieve perfect secrecy. Thus, the secrecy capacity is the same as if there is no security requirement, i.e., $C_{\text{PE-EA}}(\mathcal{N}) = C_{\text{EA}}(\mathcal{N})$.

VI. Examples

A. Amplitude Damping Channel

Consider the amplitude damping channel, specified by the input-output relation: $\mathcal{L}_{A\to B}(\rho) = K_0\rho K_0^\dagger + K_1\rho K_1^\dagger$, with

$K_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}\,|1\rangle\langle 1|$ and $K_1 = \sqrt{\gamma}\,|0\rangle\langle 1|$, with $\gamma \in \left[0, \frac{1}{2}\right]$. The amplitude damping channel has a Stinespring representation, such that the complementary channel, from Alice to Eve, is an amplitude damping channel as well, with a parameter $(1-\gamma)$ [39, Sec. II-A]. The amplitude damping channel is degraded. The classical secrecy capacity of the channel, without assistance, is the same as its quantum capacity, and it is given by $C_{\text{S}}(\mathcal{N}) = \max_{q\in[0,1]} h_2((1-\gamma)q) - h_2(\gamma q)$ (see [39, Eq.(36)]). The entanglement-assisted capacity, without secrecy, is given by $C_{\text{EA}}(\mathcal{L}) = \max_{p\in[0,1]} h_2(p) + h_2((1-\gamma)p) - h_2(\gamma p)$ (see [39, Eq. (38)]), and it can be achieved with a state of the form $|\phi_{G_1G_2}\rangle = \sqrt{1-p}\,|0\rangle \otimes |0\rangle + \sqrt{p}\,|1\rangle \otimes |1\rangle$.

We numerically compute achievable regions for each setting, using the following ensemble. Define $|u_\beta\rangle = \sqrt{1-\beta}\,|0\rangle\,|0\rangle + \sqrt{\beta}\,|\phi_{R'}\rangle$, and set $|\phi_{G_1G_2}\rangle = \frac{1}{\|u_\beta\|}\,|u_\beta\rangle$, $p_X = (1-q, q)$, and $\mathcal{F}^{(x)}(\rho) = \Sigma_X^x \rho \Sigma_X^x$, $x \in \{0,1\}$, where Σ_X is the Pauli bit-flip operator. We note that $\beta = 0$ yields the optimal choice without assistance, whereas $\beta = 1$ is optimal when entanglement assistance is available reliably.

The resulting achievable regions, for the interception and passive models, are indicated by the solid lines in Figure 5, in blue and red, respectively. For comparison, the dashed lines indicate the regions that are achieved through a classical mixture of optimal strategies, for communication with and without entanglement assistance. In the interception model, time division is impossible because the use of entanglement can lead to a leakage of guaranteed information. As can be seen in Figure 5, the point $(R, R') = (0, 0.648)$ is disconnected from the set of boundary points for which $R > 0$. In the passive model, on the other hand, we see that our coding scheme outperforms time division.

B. Erasure Channel

Consider the qubit erasure channel, specified by $\mathcal{L}_{A\to B}(\rho) = (1-\epsilon)\rho + \epsilon\,|e\rangle\langle e|$, $\epsilon \in \left[0, \frac{1}{2}\right]$, where $|e\rangle$ is an erasure state that is orthogonal to the qubit space. The channel has the following isometric extension,

$$\mathcal{N}_{A\to BE}(\rho) = V\rho V^\dagger \tag{32}$$

where the isometry $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_E$ is given by $V = \sqrt{1-\epsilon}\mathbb{1}_{A\to B} \otimes |e\rangle_E + \sqrt{\epsilon}\mathbb{1}_{A\to E} \otimes |e\rangle_B$. The erasure channel is degraded as well.

Theorem 9. Time division is optimal for the qubit erasure channel with unreliable entanglement assistance and security under interception, i.e,

$$\mathcal{C}_{\text{SI-EA*}}(\mathcal{N}) = \bigcup_{0\le\lambda\le 1} \left\{ \begin{array}{rl} (R, R') : R \le & (1-\lambda)(1-2\epsilon) \\ R' \le & 2\lambda(1-2\epsilon) \end{array} \right\}. \tag{33}$$

Proof. Achievability follows by a classical mixture of the optimal strategies, with and without entanglement assistance. That is, set $|\phi_{G_1G_2}\rangle$ to be an EPR state, $p_X = (1-\lambda, \lambda)$, and $\mathcal{F}^{(x)}(\rho)$ as in the previous example. To show the converse part, let $(R, R') \in \frac{1}{n}\mathcal{R}_{\text{SI-EA*}}(\mathcal{N}^{\otimes n})$, and let Z be an erasure flag. Since there are isometries mapping B^n and E^n to B^nZ and E^nZ, respectively, we have

$$\begin{aligned} R &\le \frac{1}{n}(I(X; B^n)_\omega - I(X; E^nG_2^n)_\omega) \\ &= \frac{1}{n}(I(X; B^n|Z)_\omega - I(X; E^nG_2^n|Z)_\omega) \\ &= \frac{1}{n}((1-\epsilon)I(X; A^n)_\omega - \epsilon I(X; A^nG_2^n)_\omega) \\ &\le \frac{1}{n}(1-2\epsilon)I(X; A^n)_\omega \\ &\le (1-2\epsilon)\left(1 - \frac{1}{n}H(A^n|X)_\omega\right) \end{aligned} \tag{34}$$

and similarly,

$$\begin{aligned} R' &\le \frac{1}{n}(1-2\epsilon)I(G_2^n; A^n|X)_\omega \\ &\le \frac{1}{n}(1-2\epsilon)2H(A^n|X)_\omega \end{aligned} \tag{35}$$

since $I(A; B)_\rho \le 2H(A)_\rho$ in general. The converse part follows by defining $\lambda \equiv \frac{1}{n}H(A^n|X)_\omega$. □

Following the same arguments, we obtain a similar result in the passive model.

Corollary 10. Time division is optimal for the qubit erasure channel with unreliable entanglement assistance and a passive eavesdropper, i.e,

$$\mathcal{C}_{\text{PE-EA*}}(\mathcal{N}) = \bigcup_{0\le\lambda\le 1} \left\{ \begin{array}{rl} (R, R') : R \le & (1-\lambda)(1-2\epsilon) \\ R' \le & 2\lambda(1-\epsilon) \end{array} \right\}. \tag{36}$$

VII. Proof of Theorem 6

Consider secure communication with unreliable entanglement assistance under interception. We show that every secrecy rate pair (R, R') in the interior of $\mathcal{R}_{\text{SI}}(\mathcal{N})$ is achievable. Suppose Alice wishes to send a pair of messages, $(m, m') \in [1 : 2^{nR}] \times [1 : 2^{nR'}]$. In the optimistic case, entanglement is successfully generated prior to the transmission of information, hence Bob can decode while using the entangled resource, which is not available to Eve. However, in the pessimistic case in this model, Eve intercepts the resource, in which case, Bob must decode without it. The coding scheme modifies the quantum SPC construction from [15]. Here, we insert local randomness elements, which will be denoted in the analysis as k, k', and are used in the encoding of each message in order to confuse Eve. Our secrecy analysis relies on the quantum covering lemma [34], as stated below. The quantum covering lemma can be viewed as a direct consequence of quantum channel resolvability [40, Appendix B], [41]. For semantic security, our proof modifies the methods of Cai [35, 36], originally applied to multiple-access channels (without secrecy), using random message permutations.

Lemma 11 (see [34]). let $\{p_X(x), \sigma_x\}_{x\in\mathcal{X}}$ be an ensemble, with a mean state $\sigma \equiv \sum_{x\in\mathcal{X}} p_X(x)\sigma_x$. Furthermore, suppose that there is a code projector Π and codeword projectors $\{\Pi_x\}_{x\in\mathcal{X}}$, that satisfy for every $\epsilon > 0$:

$$\mathrm{Tr}\{\Pi\sigma_x\} \geq 1-\epsilon, \qquad \mathrm{Tr}\{\Pi_x\sigma_x\} \geq 1-\epsilon \tag{37}$$

$$\mathrm{Tr}\{\Pi\} \leq \mathsf{D}, \qquad \Pi_x\sigma_x\Pi_x \leq \frac{1}{\mathsf{d}}\Pi_x \tag{38}$$

where $0 < \mathsf{d} < \mathsf{D}$. Consider a random codebook that $\mathscr{C} \equiv \{X(k)\}_{k\in\mathcal{K}}$ that consists of $|\mathcal{K}|$ independent and identically distributed codewords, $\sim p_X$. Then,

$$\Pr\left\{\left\|\frac{1}{|\mathcal{K}|}\sum_{k\in\mathcal{K}}\sigma_{X(k)}-\sigma\right\|_1 > \epsilon+4\sqrt{\epsilon}+24\sqrt[4]{\epsilon}\right\}$$
$$\leq 1-2\mathsf{D}\exp\left\{-\frac{\epsilon^3}{4\ln 2}\frac{|\mathcal{K}|\mathsf{d}}{\mathsf{D}}\right\}. \tag{39}$$

Before we state the proof, we make the following observations. First, we note that pure states $|\phi_{G_1G_2}\rangle$ are sufficient to exhaust the union in the rate region formula in (24), since G_1 can be extended to include a purifying reference system. In addition, we can restrict the proof to isometric encoding maps, $F^{(x)}_{G_1\to A}$ for $x\in\mathcal{X}$, by similar arguments as in [15]. To see this, consider using a collection of encoding channels, $\mathcal{F}^{(x)}_{G_1\to A'}$ for $x\in\mathcal{X}$, for transmission via $\widehat{\mathcal{N}}_{A'\to BE}$. Every quantum channel $\mathcal{F}^{(x)}_{G_1\to A'}$ has a Stinespring representation, with an isometry $F^{(x)}_{G_1\to A'A_0}$. Since it is an encoding map, we may think of A_0 as Alice's ancilla. Then, let $A\equiv(A',A_0)$ be the augmented channel input. We are effectively coding over the channel $\mathcal{N}_{A\to BE}$, where $\mathcal{N}_{A\to BE}(\rho_{A'A_0}) = \widehat{\mathcal{N}}_{A'\to BE}(\mathrm{Tr}_{A_0}(\rho_{A'A_0}))$, using the isometric map $F^{(x)}_{G_1\to A}$. From this point, we will focus on the quantum wiretap channel $\mathcal{N}_{A\to BE}$ and use the isometric encoding map $F^{(x)}_{G_1\to A}$.

A. Notation

We introduce the following notation. For every $x\in\mathcal{X}$, consider the input state

$$\left|\psi^x_{AG_2}\right\rangle = (F^{(x)}_{G_1\to A}\otimes\mathbb{1})\left|\phi_{G_1G_2}\right\rangle, \tag{40}$$

which results in the output

$$\omega^x_{BEG_2} = (\mathcal{N}_{A\to BE}\otimes\mathrm{id})(\psi^x_{AG_2}). \tag{41}$$

Then, consider a Schmidt decomposition,

$$\left|\psi^x_{AG_2}\right\rangle = \sum_{y\in\mathcal{Y}}\sqrt{p_{Y|X}(y|x)}\left|\xi_{y|x}\right\rangle\otimes\left|\xi'_{y|x}\right\rangle \tag{42}$$

where $p_{Y|X}$ is a conditional probability distribution. We will often use the notation $\left|\psi^{x^n}\right\rangle = \bigotimes_{i=1}^n|\psi^{x_i}\rangle$.

Next, let us define a unitary operator that will be useful in the definition of our encoder. Denote the Heisenberg-Weyl operators, on a qudit of dimension d, by

$$\Sigma(a,b) = \Sigma_X^a\Sigma_Z^b\,,\ \text{for } a,b\in\{0,\ldots,d-1\}, \tag{43}$$

where $\Sigma_X = \sum_{k=0}^{d-1}|k+1 \mod d\rangle\langle k|$ and $\Sigma_Z = \sum_{k=0}^{d-1}\exp\left\{\frac{2\pi ik}{d}\right\}|k\rangle\langle k|$.

Let $x^n\in\mathcal{X}^n$ be a given sequence. For every conditional type t on $\mathcal{Y}^n$ given x^n, we will apply an operator of the form $(-1)^{c_t}\Sigma(a_t,b_t)$ for $a_t,b_t\in\{0,\ldots,d_t-1\}$ and $c_t\in\{0,1\}$, where d_t is the size of the corresponding conditional type class. Then, define the unitary

$$U(\gamma) = \bigoplus_t(-1)^{c_t}\Sigma(a_t,b_t) \tag{44}$$

corresponding to a vector $\gamma = ((a_t,b_t,c_t)_t)$, where the direct sum is over all conditional types. Furthermore, let Γ_{x^n} denote the set of all such vectors γ.

B. Code Construction

We now describe the construction of a secrecy code with unreliable entanglement assistance. Let $|\phi_{G_1G_2}\rangle^{\otimes n}$ be the assistance that Alice and Bob would like to share. We also let R_0 and R'_0 denote the rates of the Alice's local random elements, where $0<R_0<R$ and $0<R'_0<R'$.

1) Classical Codebook Generation: Select $2^{n(R+R_0)}$ sequences independently at random,

$$\left\{x^n(m,k)\right\}_{m\in[1:2^{nR}]\,,\,k\in[1:2^{nR_0}]} \tag{45}$$

each i.i.d. $\sim p_X$. Then, for every m and k, select $2^{n(R'+R'_0)}$ conditionally independent sequences at random,

$$\left\{\gamma(m',k'|x^n(m,k)\right\}_{m'\in[1:2^{nR'}]\,,\,k'\in[1:2^{nR'_0}]} \tag{46}$$

each uniformly distributed over $\Gamma_{x^n(m,k)}$. The codebooks are publicly revealed, to Alice, Bob, and Eve.

2) Encoding: Alice chooses a message pair (m,m'). To ensure secrecy, Alice further selects local randomness elements, k and k', chosen uniformly at random, from $[1:2^{nR_0}]$ and $[1:2^{nR'_0}]$, respectively. To encode the first message m, she applies the encoding map

$$F^{(x^n)}_{G_1^n\to A^n} = \bigotimes_{i=1}^n F^{(x_i)}_{G_1\to A}\,,\ \text{with } x^n\equiv x^n(m,k)\,, \tag{47}$$

on her share of the entangled state $|\phi_{G_1G_2}\rangle^{\otimes n}$. The resulting input state is $\left|\psi^{x^n}_{A^nG_2^n}\right\rangle$ (see (40)).

To encode the excess message m', she applies the unitary $U(\gamma)$, with $\gamma\equiv\gamma(m',k'|x^n)$. This yields the input state

$$\left|\chi^{\gamma,x^n}_{A^nG_2^n}\right\rangle = (U(\gamma)\otimes\mathbb{1})\left|\psi^{x^n}_{A^nG_2^n}\right\rangle. \tag{48}$$

Alice transmits A^n through n uses of the wiretap channel $\mathcal{N}_{A\to BE}$. The output is

$$\rho^{\gamma,x^n}_{B^nE^nG_2^n} = (\mathcal{N}^{\otimes n}_{A\to BE}\otimes\mathrm{id})(\chi^{\gamma,x^n}_{A^nG_2^n}). \tag{49}$$

3) Decoding: Bob has two decoding strategies. If Bob holds the entangled resource G_2^n, then he decodes both messages, m and m'. However, if Eve has stolen G_2^n, then Bob decodes the message m alone. Specifically, Bob decodes in two steps. First, he performs a measurement, using a POVM $\{\Lambda_{m,k}\}$, which will be described later, in order to estimate the message m. If he has access to the entanglement resource G_2^n, then he continues to decode the message m' using a second POVM $\{\Upsilon_{m',k'}\}$, which will also be described later.

C. Error Analysis

We now analyze the probability for erroneous decoding by Bob, for the guaranteed message and the excess message. Let $\alpha > 0$ be arbitrarily small. Using the schmidt decomposition in (42), we have

$$\left|\psi^{x^n}_{A^n G_2^n}\right\rangle = \sum_{y^n \in \mathcal{Y}^n} \sqrt{P_{Y^n|x^n}(y^n|x^n)} \left|\xi_{y^n|x^n}\right\rangle \otimes \left|\xi'_{y^n|x^n}\right\rangle$$

for $x^n \in \mathcal{X}^n$. Following similar arguments as in [15], we can also write this as

$$\left|\psi^{x^n}_{A^n G_2^n}\right\rangle = \sum_t \sqrt{p(t|x^n)} \left|\Phi_t\right\rangle \tag{50}$$

where the sum is over all conditional types on $\mathcal{Y}^n$ given x^n, with $p(t|x^n)$ denoting the probability that a random sequence $Y^n \sim p^n_{Y|X}(\cdot|x^n)$ belongs to the conditional type class of t, and $|\Phi_t\rangle = \sum_{y^n \in T_n(t|x^n)} \left|\xi_{y^n|x^n}\right\rangle \otimes \left|\xi'_{y^n|x^n}\right\rangle$ is a maximally entangled state on the product of typical subspaces (see [15, Eq. (71)]). Using the ricochet property $(U \otimes \text{id}) |\Phi_{AB}\rangle = (\text{id} \otimes U^T) |\Phi_{AB}\rangle$, we can then reflect the unitary operation to the entangled resource at the receiver along with the environment:

$$\left|\chi^{\gamma, x^n}_{A^n G_2^n}\right\rangle = (\mathbb{1} \otimes U^T(\gamma)) \left|\psi^{x^n}_{A^n G_2^n}\right\rangle . \tag{51}$$

Thus, we can write the output state as follows:

$$\begin{aligned}
\rho^{\gamma, x^n}_{B^n E^n G_2^n} &= (\mathcal{N}^{\otimes n}_{A \to BE} \otimes \text{id})(\chi^{\gamma, x^n}_{A^n G_2^n}) \\
&= (\mathcal{N}^{\otimes n}_{A \to BE} \otimes \text{id})((\mathbb{1} \otimes U^T(\gamma)) \psi^{x^n}_{A^n G_2^n} (\mathbb{1} \otimes U^*(\gamma))) \\
&= (\mathbb{1} \otimes U^T(\gamma)) \left[(\mathcal{N}^{\otimes n}_{A \to BE} \otimes \text{id})(\psi^{x^n}_{A^n G_2^n})\right] (\mathbb{1} \otimes U^*(\gamma)) \\
&= (\mathbb{1} \otimes U^T(\gamma)) \omega^{x^n}_{B^n E^n G_2^n} (\mathbb{1} \otimes U^*(\gamma))
\end{aligned} \tag{52}$$

where $\omega^x_{BEG_2}$ is as in (41).

Next, we analyze the error probability in each scenario.

1) Eve has stolen the resource: We begin with the pessimistic case, where Bob does not have the entangled resource G_2^n, as it was stolen by Eve. Bob's reduced state is given by

$$\begin{aligned}
\rho^{\gamma, x^n}_{B^n} &= \text{Tr}_{E^n G_2^n}((\mathbb{1} \otimes U^T(\gamma)) \omega^{x^n}_{B^n E^n G_2^n} (\mathbb{1} \otimes U^*(\gamma))) \\
&= \omega^{x^n}_{B^n}
\end{aligned} \tag{53}$$

The second equality follows from trace cyclicity, as $U^* U^T = \mathbb{1}$. Observe that the state does not depend on γ. That is, the reduced output state is not affected by the encoding of m'. Therefore, based on the HSW Theorem [27, 28], there exists a decoding POVM $\mathcal{D}^*_{B^n} = \{\Lambda_{m,k}\}$ such that

$$\mathbb{E}\left[\frac{1}{2^{n(R+R')}} \sum_{m,m'} P_e^{*(n)}(\Psi, \mathcal{F}, \mathcal{D}^* | m, m')\right] \leq \alpha. \tag{54}$$

for sufficiently large n, provided that

$$R + R_0 < I(X;B)_\omega - \epsilon_1 . \tag{55}$$

2) Bob has entanglement assistance: We move to the optimistic case, where Eve has failed to intercept G_2^n, hence Bob holds the entangled resource. Based on the analysis above, Bob's first measurement recovers the correct guaranteed message m, with a high probability. In general, upon performing a measurement, it may lead to a state collapse. Denote the post-measurement state, after the first measurement, by $\tilde{\rho}^{\gamma, x^n}_{B^n G_2^n}$. According to the gentle measuring lemma [37, 38], this state is close in trace distance to the original state, before the measurement took place, as

$$\frac{1}{2}\left\|\tilde{\rho}^{\gamma, x^n}_{B^n E^n G_2^n} - \rho^{\gamma, x^n}_{B^n E^n G_2^n}\right\| \leq 2^{-n\frac{1}{2}(I(X;B)_\omega - R - R_0 - \epsilon_1)} , \tag{56}$$

which tends to zero if (55) holds. Hence, we may focus our error analysis on the original state, before the measurement:

$$\begin{aligned}
\rho^{\gamma, x^n}_{B^n G_2^n} &= \text{Tr}_{E^n}(\rho^{\gamma, x^n}_{B^n E^n G_2^n}) \\
&= \text{Tr}_{E^n}((\mathbb{1} \otimes U^T(\gamma)) \omega^{x^n}_{B^n E^n G_2^n} (\mathbb{1} \otimes U^*(\gamma))) \\
&= (\mathbb{1} \otimes U^T(\gamma)) \omega^{x^n}_{B^n G_2^n} (\mathbb{1} \otimes U^*(\gamma))
\end{aligned} \tag{57}$$

where $\gamma \equiv \gamma(m', k'|x^n)$, and $\omega^{x^n}_{B^n G_2^n} = \text{Tr}_{E^n}(\omega^{x^n}_{B^n E^n G_2^n})$. Based on the same arguments as without secrecy [15], there exists a POVM $\{\Upsilon_{m',k'|x^n}\}$ such that the expected error probability is bounded by

$$\mathbb{E}\left[\frac{1}{2^{n(R+R')}} \sum_{m,m'} P_e(\Psi, \mathcal{F}, \mathcal{D} | m, m')\right] \leq \alpha \tag{58}$$

for sufficiently large n, provided that

$$R' + R'_0 < I(G_2; B|X)_\omega - \epsilon_2 . \tag{59}$$

D. Secrecy Analysis

We note that secrecy is required whether Eve has intercepted Bob's entanglement resource G_2^n or not.

Consider Eve's joint state, including both her output and the entanglement resource, which could be in her possession. Similarly, as before, we express Eve's joint state as

$$\rho^{\gamma, x^n}_{E^n G_2^n} = (\mathbb{1} \otimes U^T(\gamma)) \omega^{x^n}_{E^n G_2^n} (\mathbb{1} \otimes U^*(\gamma)) \tag{60}$$

where $\omega^{x^n}_{E^n G_2^n} = \text{Tr}_{B^n}(\omega^{x^n}_{B^n E^n G_2^n})$ (see (41)).

Next, we analyze the secrecy for each of Alice's messages. Denote

$$\begin{aligned}
\Delta_{m'|m,k}(\mathscr{C}) &= \frac{1}{2}\left\|\frac{1}{2^{nR'_0}} \sum_{k'=1}^{2^{nR'_0}} \rho^{\gamma(m',k'|x^n), x^n}_{E^n G_2^n} - \zeta^{x^n}_{E^n G_2^n}\right\|_1 , \\
\Delta^*_m(\mathscr{C}) &= \frac{1}{2}\left\|\frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \omega^{x^n}_{E^n G_2^n} - \omega^{\otimes n}_{EG_2}\right\|_1 ,
\end{aligned} \tag{61}$$

with $x^n \equiv x^n(m,k)$, and $\zeta^{x^n}_{E^n G_2^n} = \frac{1}{|\Gamma_{x^n}|} \sum_{\gamma \in \Gamma_{x^n}} \rho^{\gamma, x^n}_{E^n G_2^n}$.

1) Guaranteed information indistinguishability bound: We apply the quantum covering lemma [34], Lemma 11, with the ensemble below,

$$\{p_{X^n}(x^n), \omega^{x^n}_{E^n G_2^n}\}_{x^n \in \mathcal{X}^n} \,, \tag{62}$$

and the following typical projectors, $\Pi = \Pi^{(n)}_{\delta}(\omega_{E^n G_2^n})$ and $\Pi_{x^n} = \Pi^{(n)}_{\delta}(\omega_{E^n G_2^n}|x^n)$. In the Supplementary, we show that the conditions of Lemma 11 are met for every m. Thus,

$$\Pr\left(\Delta^*_m(\mathscr{C}) > e^{-\frac{\lambda}{2}n}\right) \leq \exp\Big\{-2^{n(R_0 - I(X;EG_2)_\omega - \epsilon_4)}\Big\} \,. \tag{63}$$

for sufficiently large n. The last bound tends to zero in a double exponential rate, provided that

$$R_0 > I(X;EG_2)_\omega + \epsilon_4 \,. \tag{64}$$

2) Excess information indistinguishability bound: Let $x^n \equiv x^n(m,k)$ be fixed. Consider the uniform ensemble,

$$\left\{ p(\gamma|x^n) = \frac{1}{|\Gamma_{x^n}|}, \rho^{\gamma,x^n}_{E^n G_2^n} \right\}_{\gamma \in \Gamma_{x^n}} \,. \tag{65}$$

Using the quantum covering lemma, Lemma 11 we show that Alice's encoding simulates the average state,

$$\zeta^{x^n}_{E^n G_2^n} = \frac{1}{|\Gamma_{x^n}|} \sum_{\gamma \in \Gamma_{x^n}} \rho^{\gamma,x^n}_{E^n G_2^n} \tag{66}$$

using the code projectors $\Pi = \Pi^{(n)}_{\delta}(\omega_{E^n}|x^n) \otimes \Pi^{(n)}_{\delta}(\omega_{G_2^n}|x^n)$ and $\Pi_\gamma = (I \otimes U^T(\gamma))\Pi^{(n)}_{\delta}(\omega_{E^n G_2^n}|x^n)(I \otimes U^*(\gamma))$.

By Lemma 11, for every $m' \in [1:2^{nR'}]$ and sufficiently large n,

$$\Pr\left(\Delta_{m'|m,k}(\mathscr{C}) > e^{-\frac{\mu}{2}n}\right) \leq \exp\Big\{-2^{n(R_0' - I(G_2;E|X)_\omega - \epsilon_5)}\Big\} \tag{67}$$

which tends to zero in a double exponential rate, provided that

$$R_0' > I(E;G_2|X)_\omega + \epsilon_5 \,. \tag{68}$$

E. De-randomization

We now show that there exists a deterministic codebook under the requirements of average error probabilities and maximal indistinguishability. Consider the following error events,

$$\mathcal{A}_1 = \{\frac{1}{2^{n(R+R')}} \sum_{m,m'} P_e(\mathscr{C}|m,m') > \sqrt{\alpha}\} \,, \tag{69}$$

$$\mathcal{A}_2 = \{\frac{1}{2^{n(R+R')}} \sum_{m,m'} P_e^*(\mathscr{C}|m,m') > \sqrt{\alpha}\} \,, \tag{70}$$

$$\mathcal{B} = \{\exists (m,m') : \frac{1}{2}\left\|\rho^{m,m'}_{E^n G_B^n} - \omega^{\otimes n}_{EG_2}\right\|_1 > \delta\} \,. \tag{71}$$

By the union bound,

$$\Pr(\mathcal{A}_0 \cup \mathcal{A}_1 \cup \mathcal{B}) \leq \Pr(\mathcal{A}_0) + \Pr(\mathcal{A}_1) + \Pr(\mathcal{B}) \,. \tag{72}$$

By Markov's inequality, $\Pr(\mathcal{A}_j) \leq \sqrt{\alpha}$ (see (54), (58)). As for the last term, by the triangle inequality,

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{m,m'}_{E^n G_B^n} - \omega^{\otimes n}_{EG_2}\right\|_1 \\
&= \frac{1}{2}\left\| \frac{1}{2^{n(R_0+R_0')}} \sum_{k=1}^{2^{nR_0}} \sum_{k'=1}^{2^{nR_0'}} \rho^{\gamma(m',k'|x^n),x^n}_{E^n G_B^n} - \omega^{\otimes n}_{EG_2} \right\|_1 \\
&\leq \frac{1}{2}\left\| \frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \left(\frac{1}{2^{nR_0'}} \sum_{k'=1}^{2^{nR_0'}} \rho^{\gamma(m',k'|x^n),x^n}_{E^n G_B^n} - \zeta^{x^n}_{E^n G_2^n} \right) \right\|_1 \\
&+ \frac{1}{2}\left\| \frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \zeta^{x^n}_{E^n G_2^n} - \omega^{\otimes n}_{EG_2} \right\|_1 \\
&\leq \frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \Delta_{m'|m,k}(\mathscr{C}) \\
&+ \frac{1}{2}\left\| \frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \zeta^{x^n(m,k)}_{E^n G_2^n} - \omega^{\otimes n}_{EG_2} \right\|_1 \,.
\end{aligned} \tag{73}$$

If we were to remove the encoding of γ, then Eve's output would have been $\omega^{x^n}_{E^n G_2^n}$, instead of $\zeta^{x}_{E^n G_2^n}$. Therefore, by trace monotonicity under quantum operations, the last trace norm is bounded by $\Delta^*_m(\mathscr{C})$ (see (61)). Thus,

$$\begin{aligned}
&\Pr(\mathcal{B}) = \Pr\left(\frac{1}{2}\left\|\rho^{m,m'}_{E^n G_B^n} - \omega^{\otimes n}_{EG_2}\right\|_1 > \delta \right) \\
&\leq \Pr\left(\frac{1}{2^{nR_0}} \sum_{k=1}^{2^{nR_0}} \Delta_{m'|m,k}(\mathscr{C}) \geq \frac{\delta}{2} \right) + \Pr\left(\Delta^*_m(\mathscr{C}) > \frac{\delta}{2} \right) \\
&\leq \Pr\left(\exists k : \Delta_{m'|m,k}(\mathscr{C}) \geq \frac{\delta}{2} \right) + \exp\left\{-2^{n\epsilon_6}\right\} \\
&\leq \exp\left\{-2^{n\epsilon_7}\right\}
\end{aligned} \tag{74}$$

for some $\epsilon_7 > 0$ and sufficiently large n. We deduce that there exists a deterministic codebook $\mathscr{C}$ such that the message-average error and indistinguishability tend to zero, if

$$\begin{aligned}
R &< I(X;B)_\omega - I(X;EG_2)_\omega - \epsilon_1 - \epsilon_4 \,, \\
R' &< I(G_2;B|X)_\omega - I(G_2;E|X)_\omega - \epsilon_2 - \epsilon_5 \,.
\end{aligned}$$

F. Semantic Security

We now complete the analysis for the maximum criteria. The proof modifies the methods of Cai [35, 36], originally applied to multiple-access channels.

1) Guaranteed information (expurgation): Consider the semi-average error probability,

$$e(m) \equiv \frac{1}{2^{nR'}} \sum_{m'=1}^{2^{nR'}} P_e(\mathscr{C}|m,m') \,. \tag{75}$$

Based on the analysis above, the average of $\{e(m)\}_{m=1}^{2^{nR}}$ is bounded by $\alpha^{1/2}$. Therefore, at most a fraction of $\eta = \alpha^{1/4}$ of the messages m have $e(m) > \eta$. Then, we can expurgate the worst $\eta \cdot 2^{nR}$ messages, and the corresponding codewords. The guaranteed rate of the expurgated code is

$R - \frac{1}{n}\log\big((1-\eta)^{-1}\big)$, which tends to R as $n \to \infty$. Denote the expurgated message set by $\mathcal{M}_{\text{exp}}$.

2) Excess information (message permutation): We now construct a new code to satisfy the maximum criteria. The transmission consists of two stages. In the first stage, Alice selects a uniform "key" $L \in [1 : n^2]$. Assuming $R' > 0$, Alice can send L with negligible rate loss, such that the message-average error probabilities vanish. In the second stage, Alice chooses a permutation π_L on the message set $[1 : 2^{nR'}]$, and encodes the message pair $(m_0, m_0') = (m, \pi_L(m'))$ using the codebook $\mathscr{C}$. Bob obtains an estimate, $\hat{L}$ and $(\hat{m}_0, \hat{m}_0')$, and then declares his estimation for the original messages as $\hat{m} = \hat{m}_0$ and $\hat{m}' = \pi_{\hat{L}}^{-1}(\hat{m}_0')$.

Based on our previous analysis, the message-average error probability in the first stage is bounded by

$$\Pr\Big(\hat{L} \neq L\Big) = \frac{1}{n^2}\sum_{\ell=1}^{n^2} P_e(\mathscr{C}|1, \ell) \leq \sqrt{\alpha} \tag{76}$$

Now, consider the second block. Let $\Pi_1, \ldots, \Pi_{n^2}$ be an i.i.d. sequence of random permutations, uniformly distributed on the permutation group on the excess message set $[1 : 2^{nR'}]$. Denote the random codebook by $\Pi(\mathscr{C})$. For a given m',

$$\Pr(\Pi_{\ell'}(m') = \bar{m}') = \frac{(2^{nR'} - 1)!}{(2^{nR'})!} = \frac{1}{2^{nR'}} \tag{77}$$

for all $\bar{m}' \in [1 : 2^{nR'}]$ and $\ell' \in [1 : n^2]$. Thus, for every message pair $(m, m') \in \mathcal{M}_{\text{exp}} \times [1 : 2^{nR'}]$,

$$\begin{aligned}
&\mathbb{E}\left[P_e^{(n)}(\Pi(\mathscr{C})|m, m')\right] \\
&= \sum_{\bar{m}'} \Pr(\Pi_{\ell'}(m') = \bar{m}') P_e^{(n)}(\mathscr{C}|m, \bar{m}') \\
&= \frac{1}{2^{nR'}}\sum_{\bar{m}'} P_e^{(n)}(\mathscr{C}|m, \bar{m}') = e(m) \leq \lambda\,.
\end{aligned} \tag{78}$$

Now, by the Chernoff bound [35, Lemma 3.1],

$$\Pr\left(\frac{1}{n^2}\sum_{l'=1}^{n^2} P_e^{(n)}(\Pi(\mathscr{C})|m.m') > 4\lambda\right) < e^{-\lambda n^2}\,. \tag{79}$$

Therefore, the probability that, for some (m, m'), $\frac{1}{n^2}\sum_{l'=1}^{n^2} P_e^{(n)}(\Pi(\mathscr{C})|m, m') > 4\lambda$, tends to zero in a super-exponential rate by the union bound. We deduce that there exists a realization $(\pi_1, \ldots, \pi_{n^2})$ such that

$$P_e^{(n)}(\pi(\mathscr{C})|m, m') = \frac{1}{n^2}\sum_{\ell'=1}^{n^2} P_e^{(n)}(\pi_{\ell'}(\mathscr{C})|m, m') \leq 4\lambda \tag{80}$$

for all $(m, m') \in \mathcal{M}_{\text{exp}} \times [1 : 2^{nR'}]$. □

VIII. Proof of Theorem 7

Consider a degraded wiretap channel. Suppose Alice and Bob would like to share the entangled resource $\Psi_{G_A^n G_B^n}$, yet Bob's share may be stolen by Eve. In our model, there are two scenarios. Namely, either Bob holds the entanglement resource G_B^n, or Eve, depending on whether Eve has succeeded in her attempt to steal the resource. Alice first prepares a classical maximally correlated state,

$$\begin{aligned}
\pi_{KMK'M'} = &\left(\frac{1}{2^{nR}}\sum_{m=1}^{2^{nR}} |m\rangle\!\langle m|_M \otimes |m\rangle\!\langle m|_K\right) \\
&\otimes \left(\frac{1}{2^{nR'}}\sum_{m'=1}^{2^{nR'}} |m'\rangle\!\langle m'|_{M'} \otimes |m'\rangle\!\langle m'|_{K'}\right)
\end{aligned} \tag{81}$$

where M, K, M', and K' are classical registers, such that M and K are in perfect (classical) correlation, and so are M' and K'. Bob needs to recover the value of M in both cases, whether he holds the resource or Eve. Whereas, Bob need only recover M', if he holds the resource. Security requires that both M and M' are hidden from Eve, whether she intercepted G_B^n or not.

Alice applies an encoding map $\mathcal{F}_{MM'G_A^n \to A^n}$ on MM' and her share of entanglement, G_A^n. Hence, the input state is

$$\sigma_{KK'A^nG_B^n} = \mathcal{F}_{MM'G_A^n \to A^n}(\pi_{KMK'M'} \otimes \Psi_{G_A^n G_B^n})\,, \tag{82}$$

and transmits A^n through n channel uses, hence the output

$$\omega_{KK'B^nE^nG_B^n} = \mathcal{N}_{A\to BE}^{\otimes n}(\psi_{KK'A^nG_B^n})\,. \tag{83}$$

If the entanglement resource is available to Bob, then he applies a decoding channel $\mathcal{D}_{B^nG_B^n \to \hat{M}\hat{M}'}$, creating

$$\rho_{KK'\hat{M}\hat{M}'E^n} = \mathcal{D}_{B^nG_B^n \to \hat{M}\hat{M}'}(\omega_{KK'B^nG_B^nE^n})\,. \tag{84}$$

If Eve has stolen the entanglement resource, then Bob applies a decoding channel $\mathcal{D}^*_{B^n \to \tilde{M}}$, hence

$$\rho^*_{KK'\tilde{M}E^n} = \mathcal{D}^*_{B^n \to \tilde{M}}(\omega_{KK'B^nG_B^nE^n})\,. \tag{85}$$

Consider a sequence of $(2^{nR}, 2^{nR'}, n)$ codes, with vanishing errors and leakage, i.e.,

$$\frac{1}{2}\big\|\rho_{K\hat{M}K'\hat{M}'} - \pi_{KMK'M'}\big\|_1 \leq \alpha_n\,, \tag{86}$$

$$\frac{1}{2}\big\|\rho^*_{K\tilde{M}} - \pi_{KM}\big\|_1 \leq \alpha_n^*\,, \tag{87}$$

and

$$I(KK'; E^nG_B^n)_\omega \leq \beta_n \tag{88}$$

where α_n, α_n^*, and β_n tend to zero as $n \to \infty$. Eq. (88) represents a weaker form of secrecy, yet this is sufficient for the converse part. Based on entropy continuity,

$$\Big|I(K; M)_\pi - I(K; \hat{M})_{\rho^*}\Big| \leq n\varepsilon_n^* \tag{89}$$

$$\Big|I(K; M'|K)_\pi - I(K; \hat{M}'|K)_\rho\Big| \leq n\varepsilon_n \tag{90}$$

where $\varepsilon_n, \varepsilon_n^* \to 0$ when $n \to \infty$ (see [15, App.C, part B])

Consider the scenario where Bob receives B^n alone, while Eve gets both E^n and G_B^n. Now,

$$\begin{aligned}
nR &= I(K; M)_\pi \\
&\leq I(K; \hat{M})_{\rho^*} + n\epsilon_n^* \\
&\leq I(K; B^n)_\omega + n\epsilon_n^* \\
&\leq I(K; B^n)_\omega - I(K; E^nG_B^n)_\omega + n(\varepsilon_n^* + \beta_n)
\end{aligned} \tag{91}$$

where the first inequality is due to (89), the second follows from the data processing inequality (see (85)), and the third from (88).

We move to the more challenging bound, on the excess rate. Here, we use the degraded property. Consider the scenario where Bob holds both B^n and G_B^n. As before, we use (88) and (90) to show that

$$\begin{aligned} nR' &= I(K';M'|K)_\pi \\ &\leq I(K';G_B^n B^n|K)_\omega - I(K';E^n G_B^n|K)_\omega + n(\varepsilon_n+\beta_n) \,. \end{aligned} \tag{92}$$

We can also write this as

$$\begin{aligned} n(R'-\varepsilon_n-\beta_n) \leq I(K'G_B^n;B^n|K)_\omega - I(K'G_B^n;E^n|K)_\omega - \\ [I(G_B^n;B^n|K)_\omega - I(G_B^n;E^n|K)_\omega] \,. \end{aligned} \tag{93}$$

Due to our assumption that the quantum wiretap channel is degraded, the expression within the square brackets above is nonnegative. Thus,

$$n(R'-\varepsilon_n-\beta_n) \leq I(K'G_B^n;B^n|K)_\omega - I(K'G_B^n;E^n|K)_\omega \,. \tag{94}$$

To complete the regularized converse proof, set $X=K$ and $G_2=(K',G_B^n)$ in (91) and (94), and take $n\to\infty$. □

IX. Summary

We study secure communication with unreliable entanglement assistance. Alice wishes to send a secret message to Bob, while exploiting pre-shared entanglement assistance. In our setting, the assistance is *unreliable* due to one of two reasons: Interception or loss. In the interception model, Eve may steal the entanglement assistance (see Figure 1(b)). Whereas, loss implies that Eve is passive and the assistance may get lost to the environment (see Figure 2). Our present work continues the line of research that started with [15] and [17] on unreliable entanglement assistance. However, the previous work [15, 17] did not include security concerns.

Here, we derive achievable rates for both the interception and loss models, subject to a maximal error criterion and semantic security. In the interception model, the guaranteed rate bound includes both Eve's system E and Bob's entangled resource G_B (see (24)), which reflects Eve's access to the entanglement assistance if she succeeds to intercept the resource. On the other hand, in the passive eavesdropper model, the guaranteed rate bound does not involve the entangled resource G_B (see (29)), as the assistance is beyond Eve's reach.

Moreover, the bound on the excess rate, in the passive model, does not include Eve's system at all (see (29)), i.e., secrecy does not entail a rate reduction. This is expected because given reliable entanglement assistance, Alice and Bob can secure a shared key, and apply the one-time pad encryption to the excess message.

As an example, we consider the erasure channel and the amplitude damping channel. For the erasure channel, time division is optimal. This is "good news" from a practical perspectives, as time division is much easier to implement.

We observe that in general, time division is impossible if Eve can actively intercept Bob's entanlged resource, since Alice's operations on her share of the entanglement could leak information on the guaranteed information. For the amplitude damping channel, the boundary of our achievable region is disconnected in agreement with this property. In the passive model, on the other hand, our encoding scheme outperforms time division.

Some questions still remain open, as we do not have a full understanding of the behavior of the capacity region, its convexity properties, and the type of entanglement that allows positive guaranteed rate under interception. Furthermore, while we have presented a regularized characterization, a single-letter capacity formula for the class of degraded channels could lead to further insights.

Acknowledgments

U. P. and M. L. were supported by Israel Science Foundation (ISF), n. 939/23 and 2691/23, German-Israeli Project Cooperation (DIP) n. 2032991, and Nevet Program of the Helen Diller Quantum Center at the Technion. U. P. was also supported by the Israel VATAT Junior Faculty Program for Quantum Science and Technology n. 86636903, and the Chaya Career Advancement Chair n. 8776026.

References

[1] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, 2008.

[2] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Advances Opt. Photon.*, vol. 12, no. 4, pp. 1012–1236, 2020.

[3] R. F. Schaefer, H. Boche, and H. V. Poor, "Secure communication under channel uncertainty and adversarial attacks," *Proc. IEEE*, vol. 103, no. 10, pp. 1796–1813, 2015.

[4] M. Cai and A. Winter, "Quantum wiretap channel coding assisted by noisy correlation," `arXiv:2402.13194`, 2024.

[5] H. Boche, M. Cai, M. Wiese, C. Deppe, and R. Ferrara, "Semantic security for quantum wiretap channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2020)*, 2020, pp. 1990–1995.

[6] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type ii," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3863–3879, July 2016.

[7] J. Yin, Y. H. Li, S. K. Liao, M. Yang, Y. Cao, L. Zhang, J. G. Ren, W. Q. Cai, W. Y. Liu, and S. L. Li, "Entanglement-based secure quantum cryptography over

1,120 kilometres," *Nature*, vol. 582, no. 7813, pp. 501–505, 2020.

[8] E. Zlotnick, B. Bash, and U. Pereg, "Entanglement-assisted covert communication via qubit depolarizing channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT'2023)*, 2023, pp. 198–203.

[9] H. Qi, K. Sharma, and M. M. Wilde, "Entanglement-assisted private communication over quantum broadcast channels," *J. Phys. A: Math. Theo.*, vol. 51, no. 37, p. 374001, 2018.

[10] J. Nötzel and S. DiAdamo, "Entanglement-enhanced communication networks," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE'2020)*, 2020, pp. 242–248.

[11] E. T. Campbell and S. C. Benjamin, "Measurement-based entanglement under conditions of extreme photon loss," *Physical Rev. Lett.*, vol. 101, no. 13, p. 130502, 2008.

[12] J. Yin, Y. Cao, Y. H. Li, J. G. Ren, S. K. Liao, L. Zhang, W. Q. Cai, W. Y. Liu, B. Li, and H. Dai, "Satellite-to-ground entanglement-based quantum key distribution," *Physical Rev. Lett.*, vol. 119, no. 20, p. 200501, 2017.

[13] A. Czerwinski and K. Czerwinska, "Statistical analysis of the photon loss in fiber-optic communication," *Photon.*, vol. 9, no. 8, p. 568, 2022.

[14] G. Fettweis and H. Boche, "On 6G and trustworthiness," *Commun. ACM*, vol. 65, no. 4, pp. 48–49, 2022.

[15] U. Pereg, C. Deppe, and H. Boche, "Communication with unreliable entanglement assistance," *IEEE Trans. Inf. Theory*, vol. 69, no. 7, pp. 4579–4599, 2023.

[16] W. Huleihel and Y. Steinberg, "Channels with cooperation links that may be absent," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 5886–5906, 2017.

[17] U. Pereg, "Communication over entanglement-breaking channels with unreliable entanglement assistance," *Physical Rev. A*, vol. 108, p. 042616, 2023.

[18] F. Dupuis, J. Florjanczyk, P. Hayden, and D. Leung, "The locking-decoding frontier for generic dynamics," *Proc. Roy. Soc. A: Math., Physical, Eng. Sci.*, vol. 469, no. 2159, p. 20130289, 2013.

[19] O. Fawzi, P. Hayden, and P. Sen, "From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking," *J. ACM (JACM)*, vol. 60, no. 6, pp. 1–61, 2013.

[20] H. Boche, M. Cai, C. Deppe, and J. Nötzel, "Classical-quantum arbitrarily varying wiretap channel: Secret message transmission under jamming attacks," *J. Math. Phys.*, vol. 58, no. 10, 2017.

[21] N. Cai, A. Winter, and R. W. Yeung, "Quantum privacy and quantum wiretap channels," *Prob. Inform. Transm.*, vol. 40, pp. 318–336, 2004.

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

[23] H. Boche and J. Nötzel, "Positivity, discontinuity, finite resources, and nonzero error for arbitrarily varying quantum channels," *J. Math. Phys.*, vol. 55, no. 12, p. 122201, 2014.

[24] S. Barz, G. Cronenberg, A. Zeilinger, and P. Walther, "Heralded generation of entangled photon pairs," *Nature Photon.*, vol. 4, no. 8, pp. 553–556, 2010.

[25] J. G. Proakis, *Digital Communications*, 4th ed. McGraw-Hill, 2001.

[26] Q. Zhuang, E. Y. Zhu, and P. W. Shor, "Additive classical capacity of quantum channels assisted by noisy entanglement," *Phys. Rev. Lett.*, vol. 118, no. 20, p. 200503, 2017.

[27] A. S. Holevo, "The capacity of the quantum channel with general signal states," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 269–273, Jan 1998.

[28] B. Schumacher and M. D. Westmoreland, "Sending classical information via noisy quantum channels," *Phys. Rev. A*, vol. 56, no. 1, p. 131, July 1997.

[29] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, "Entanglement-assisted classical capacity of noisy quantum channels," *Phys. Rev. Lett.*, vol. 83, no. 15, p. 3081, Oct 1999.

[30] D. Elkouss and S. Strelchuk, "Superadditivity of private information for any number of uses of the channel," *Phys. Rev. Lett.*, vol. 115, no. 4, p. 040501, 2015.

[31] K. Li, A. Winter, X. Zou, and G. Guo, "Private capacity of quantum channels is not additive," *Physical Rev. Lett.*, vol. 103, no. 12, p. 120501, 2009.

[32] S. Zou, Y. Liang, L. Lai, H. V. Poor, and S. Shamai, "Broadcast networks with layered decoding and layered secrecy: Theory and applications," *Proc. IEEE*, vol. 103, no. 10, pp. 1841–1856, 2015.

[33] U. Pereg, R. Ferrara, and M. R. Bloch, "Key assistance, key agreement, and layered secrecy for bosonic broadcast channels," in *Proc. IEEE Inf. Theory Workshop (ITW'2021)*, 2021, pp. 1–6.

[34] R. Ahlswede and A. Winter, "Strong converse for identification via quantum channels," *IEEE Trans. Inf. Theory*, vol. 48, no. 3, pp. 569–579, 2002.

[35] N. Cai, "The maximum error probability criterion, random encoder, and feedback, in multiple input channels," *Entropy*, vol. 16, no. 3, pp. 1211–1242, 2014.

[36] U. Pereg, C. Deppe, and H. Boche, "The multiple-access channel with entangled transmitters," `arXiv:2303.10456 [quant-ph]`. Submitted to IEEE Trans. Inf. Theory, 2023.

[37] U. Pereg, "Communication over quantum channels with parameter estimation," *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 359–383, 2022.

[38] A. Winter, "Coding theorem and strong converse for quantum channels," *IEEE Trans. Inf. Theory*, vol. 45, no. 7, pp. 2481–2485, Nov 1999.

[39] V. Giovannetti and R. Fazio, "Information-capacity description of spin-chain correlations," *Physical Rev. A*, vol. 71, no. 3, p. 032314, 2005.

[40] M. Tahmasbi and M. R. Bloch, "Toward undetectable quantum key distribution over bosonic channels," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 585–598, 2020.

[41] M. Hayashi, *Quantum information*. Springer, 2006.