Semantic Security with Unreliable Entanglement Assistance: Interception and Loss

Meir Lederman and Uzi Pereg

*Faculty of Electrical and Computer Engineering, Technion
†Helen Diller Quantum Center, Technion
Email: meirlederman@campus.technion.ac.il, uzipereg@technion.ac.il

***Abstract*—Semantic security 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. We derive achievable rates for both models, subject to a maximal error criterion and semantic security. As an example, we consider 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.**

I. Introduction

Information theoretic security has traditionally relied on weak and strong secrecy metrics. However, from a cryptographic standpoint, these were considered inadequate [1], due to the assumption of messages being randomly and uniformly distributed. Nonetheless, real-world messages often originate from structured data with low entropy, such as files or votes [2]. Semantic security has thus become the gold standard in the cryptography community [3–5]. Semantic security ensures that the eavesdropper gains no information, without making any assumptions on the message distribution. It can also be formulated as message indistinguishability, where Eve is unable to distinguish between any pair of messages [6].

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 [21] and Devetak [22] established a regularized capacity formula without entanglement assistance. Boche et al. [6] presented explicit constructions of semantic secuirty codes. Qi et al. [9] considered secure communication with entanglement assistance. The authors have recently considered communication with unreliable entanglement assistance and strong secrecy [23], assuming that the information is uniform.

Here, we consider two semantic 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.

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 assistance provides. In this manner, we adapt the transmission rate to the availability of entanglement assistance, while communication does not break down when the assisting resource is absent.

We establish an achievable rate region for communication with unreliable entanglement assistance and semantic security, for each setting. To demonstrate our results, we consider the amplitude damping channel. In the interception model, we encounter a phenomenon that is somewhat rare in network information theory [24]: Time sharing is impossible and the boundary of our achievable region is disconnected. Whereas, in the passive model, our achievable rate region outperforms time division.

In the analysis, we introduce a novel proof technique for the maximal error and security analysis. Our technique modifies the methods by Cai [25] for multiple access channels with correlated transmitters (see also [26]).

II. Coding Definitions

Before communication begins, the legitimate parties try to generate entanglement assistance. In the optimistic case, Alice and Bob have entanglement resources, G^n_A and G^n_B, respectively (see Figure 1(a)). However, G^n_B 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 [27], 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 $\Psi_{G^n_A,G^n_B}$,
- a collection of encoding maps $\{\mathcal{F}^{(m,m')}_{G^n_A\to A^n}\}$, and
- two POVMs, $\mathcal{D}_{B^nG^n_B}=\{D_{m,m'}\}$ and $\mathcal{D}^*_{B^n}=\{D^*_m\}$.

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

$$\rho^{m,m'}_{A^nG^n_B} = (\mathcal{F}^{(m,m')}_{G^n_A\to A^n}\otimes \mathrm{id})(\Psi_{G^n_AG^n_B}) \tag{1}$$

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

We have two maximum error criteria; in the presence of entanglement assistance:

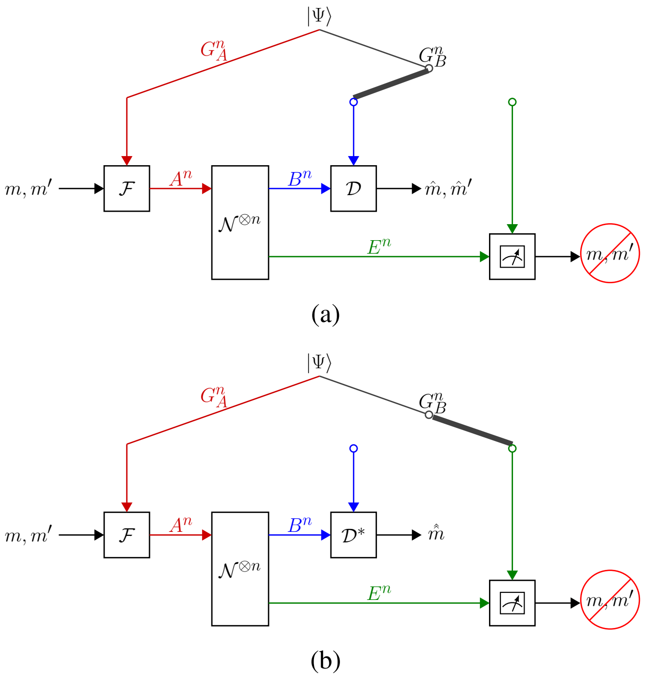
$$P_{e,\max}(\Psi,\mathcal{F},\mathcal{D}) = \max_{m,m'}\left[1-\mathrm{Tr}(D_{m,m'}\,\rho^{m,m'}_{B^nG^n_B})\right] ,$$

and without entanglement assistance:

$$P^*_{e,\max}(\Psi,\mathcal{F},\mathcal{D}^*) = \max_{m,m'}\left[1-\mathrm{Tr}(D^*_m\,\rho^{m,m'}_{B^n})\right] . \tag{2}$$

III. Semantic Security

We consider two security settings.



(a)

(b)

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

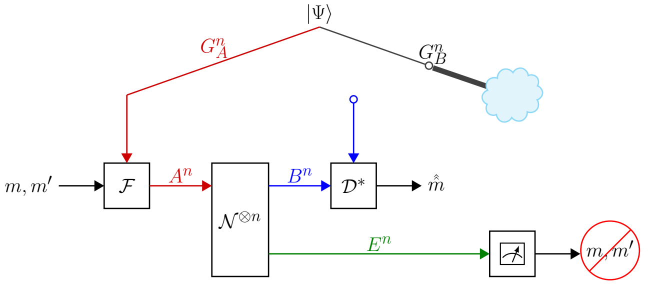


Fig. 2. Passive eavesdropper. The resource may get lost to the environment.

A. Security Under Interception

Suppose that Eve may steal the entanglement resource G^n_B. 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 $\theta_{E^nG^n_B}$, by

$$\Delta_{\mathrm{SI}}(\Psi,\mathcal{F},\theta_{E^nG^n_B}) = \max_{m,m'}\frac{1}{2}\left\|\rho^{m,m'}_{E^nG^n_B}-\theta_{E^nG^n_B}\right\|_1 . \tag{3}$$

Notice that we include the entangled resource G^n_B 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 semantic security under interception

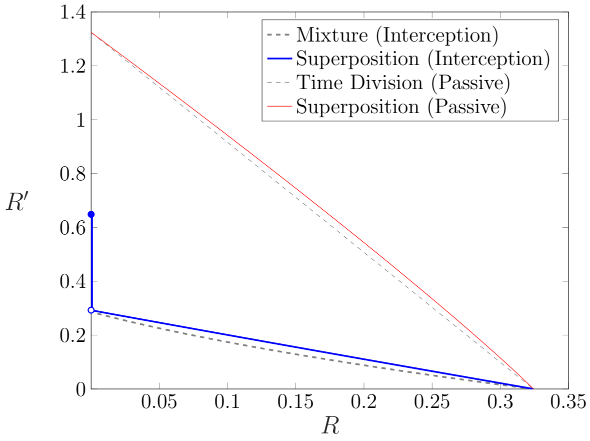


Fig. 3. Achievable rate regions for the amplitude damping channel with unreliable entanglement assistance and semantic security, for $\gamma = 0.3$

satisfies $\max\left(P_{e,\max}(\Psi,\mathcal{F},\mathcal{D}), P^*_{e,\max}(\Psi,\mathcal{F},\mathcal{D}^*)\right) \le \epsilon$, and there exists $\theta_{E^nG_B^n}$ such that $\Delta_{\text{SI}}(\Psi,\mathcal{F},\theta_{E^nG_B^n}) \le \delta$. 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 $\mathcal{C}_{\text{SI}}(\mathcal{N})$ with unreliable entanglement assistance and semantic security under interception is the closure of the set of all such pairs.

B. Passive Eavesdropper

The passive model assumes that Eve does not gain access to the resource G_B^n. See Figure 2. The security level is now

$$\Delta_{\text{PE}}(\Psi,\mathcal{F},\theta_{E^n}) = \max_{m,m'} \frac{1}{2}\left\|\rho_{E^n}^{m,m'} - \theta_{E^n}\right\|_1 \tag{4}$$

(cf. (3)). The capacity region $\mathcal{C}_{\text{PE}}(\mathcal{N})$ is defined accordingly.

Remark 1. As opposed to [23], we do not assume that the messages are uniformly distributed. Instead, (2)-(4) involve a maximum, in accordance with the semantic security approach.

IV. Main Results

A. Security Under 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 Section II). If entanglement assistance is available to Bob, he recovers both messages. Yet, if Eve has stolen the resource, then he recovers the first message alone.

Let $\mathcal{N}_{A\to BE}$ be a quantum wiretap channel. Define

$$\mathcal{R}_{\text{SI}}(\mathcal{N}) \equiv \bigcup_{p_X,\varphi_{G_1G_2},\mathcal{F}^{(x)}} \left\{ \begin{array}{rl} (R,R') : & R \le [I(X;B)_\omega - I(X;EG_2)_\omega]_+ \\ & R' \le [I(G_2;B|X)_\omega - I(G_2;E|X)_\omega]_+ \end{array} \right\} \tag{5}$$

where $[x]_+ \equiv \max(x,0)$, and

$$\omega_{XG_2A} \equiv \sum_{x\in\mathcal{X}} p_X(x)\,|x\rangle\langle x| \otimes (\text{id}\otimes\mathcal{F}^{(x)}_{G_1\to A})(\varphi_{G_2G_1})\,,$$
$$\omega_{XG_2BE} \equiv (\text{id}\otimes\text{id}\otimes\mathcal{N}_{A\to BE})(\omega_{XG_2A})\,, \tag{6}$$

Our main result on the interception model is given in the theorem below.

Theorem 1. The region $\mathcal{R}_{\text{SI}}(\mathcal{N})$ is achievable with unreliable entanglement assistance and semantic security under interception. That is, the capacity region is bounded by

$$\mathcal{C}_{\text{SI}}(\mathcal{N}) \supseteq \mathcal{R}_{\text{SI}}(\mathcal{N})\,. \tag{7}$$

The proof of Theorem 1 is given in section V. Our proof modifies the methods of Cai [25, 26], originally applied to multiple-access channels (without secrecy), using random message permutations.

B. Passive Eavesdropper

Here, the entanglement assistance can be lost to the environment, beyond Eve's reach. Define

$$\mathcal{R}_{\text{PE}}(\mathcal{N}) \equiv \bigcup_{p_X,\varphi_{G_1G_2},\mathcal{F}^{(x)}} \left\{ \begin{array}{rl} (R,R') : & R \le \ [I(X;B)_\omega - I(X;E)_\omega]_+ \\ & R' \le \ I(G_2;B|X)_\omega \end{array} \right\} \tag{8}$$

where ω_{XG_2BE} is as in (6). Our main result on the passive model is given below.

Theorem 2. The region $\mathcal{R}_{\text{PE}}(\mathcal{N})$ is achievable with unreliable entanglement assistance and a passive eavesdropper. That is, the capacity region is bounded by

$$\mathcal{C}_{\text{PE}}(\mathcal{N}) \supseteq \mathcal{R}_{\text{PE}}(\mathcal{N})\,. \tag{9}$$

As the assistance remains secure from the eavesdropper, Alice and Bob can use the entanglement resources in order to generate a secret key. Alice can then apply the one-time pad encoding to the excess message m'. The rest of the analysis follows similar steps as for Theorem 1. The details are omitted.

C. Example - Amplitude Damping Channel

Consider the amplitude damping channel $\mathcal{N}(\rho) = K_0\rho K_0^\dagger + K_1\rho K_1^\dagger$, with $K_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}\,|1\rangle\langle 1|$ and $K_1 = \sqrt{\gamma}\,|0\rangle\langle 1|$, with $\gamma\in[0,1]$. We numerically compute achievable regions for each setting, using the following ensemble. Define $|u_\beta\rangle = \sqrt{1-\beta}\,|0\rangle\otimes|0\rangle + \sqrt{\beta}\,|\Phi\rangle$, and set $|\phi_{G_1G_2}\rangle = \frac{1}{\|u_\beta\|}\,|u_\beta\rangle$, $p_X = \left(\frac{1}{2},\frac{1}{2}\right)$, 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.

The resulting achievable regions, for the interception and passive models, are indicated by the solid lines in Figure 3, 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 3, 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.

V. Proof of Theorem 1

We show achievability with semantic security under interception. The main technical novelty is in Section V-C. We begin with useful results from our previous work [23].

A. Random Code Analysis (Previous Work [23])

The code construction and previous results from [23] are summarized below. Fix a pure state $|\phi_{G_1G_2}\rangle$ and a collection of isometries $\{F^{(x)}_{G_1\to A}\}$. Denote $\left|\psi^x_{AG_2}\right\rangle = (F^{(x)}_{G_1\to A}\otimes \mathbb{1})\,|\phi_{G_1G_2}\rangle$ and $\omega^x_{BEG_2} = (\mathcal{N}_{A\to BE}\otimes \mathrm{id})(\psi^x_{AG_2})$. Suppose Alice and Bob would like to share $|\phi_{G_1G_2}\rangle^{\otimes n}$.

Classical Codebook Generation: Select a random codebook $\mathscr{C}_1 = \left\{x^n(m,k)\right\}_{m\in[1:2^{nR}],k\in[1:2^{nR_0}]}$, each codeword is i.i.d. $\sim p_X$. Denote the Heisenberg-Weyl operators of dimension D by $\{\Sigma^a_X\Sigma^b_Z\}$. Consider a Schmidt decomposition $\left|\psi^x_{AG_2}\right\rangle = \sum_{y\in\mathcal{Y}}\sqrt{p_{Y|X}(y|x)}\,\left|\xi_{y|x}\right\rangle\otimes\left|\xi'_{y|x}\right\rangle$. For every conditional type class $\mathcal{T}_n(t|x^n)$ in $\mathcal{Y}^n$, define $V_t(a_t,b_t,c_t) = (-1)^{c_t}\Sigma^{a_t}_X\Sigma^{b_t}_Z$, for $a_t,b_t \in \{0,...,|\mathcal{T}_n(t|x^n)|-1\}$, $c_t\in\{0,1\}$. Consider $U(\gamma) = \bigoplus_t V_t(a_t,b_t,c_t)$ with $\gamma = ((a_t,b_t,c_t)_t)$, and let Γ_{x^n} denote the set of all such vectors γ. Then, for every m and k, select $2^{n(R'+R'_0)}$ conditionally independent sequences, $\mathscr{C}_2 = \left\{\gamma(m',k'|x^n(m,k)\right\}_{m'\in[1:2^{nR'}],k'\in[1:2^{nR'_0}]}$, uniformly at random. The codebook $\mathscr{C} = (\mathscr{C}_1,\mathscr{C}_2)$ is publicly revealed.

Encoder: Select k and k' uniformly at random. To encode (m,m'), apply $\bigotimes_{i=1}^n F^{(x_i)}_{G_1\to A}$ and then $U(\gamma)$, with $x^n \equiv x^n(m,k)$ and $\gamma\equiv\gamma(m',k'|x^n(m,k))$. Transmit A^n.

Denote the output state by $\rho^{\gamma,x^n}_{B^nE^nG_2^n}$.

Decoder: Based on [15], Bob can decode the guaranteed and excess messages such that the expected message-average error probabilities satisfy

$$\mathbb{E}\left[\frac{1}{2^{n(R+R')}}\sum_{m,m'}P_e(\mathscr{C}|m,m')\right]\leq\epsilon_1\,, \tag{10}$$

$$\mathbb{E}\left[\frac{1}{2^{n(R+R')}}\sum_{m,m'}P^*_e(\mathscr{C}|m,m')\right]\leq\epsilon_1\,, \tag{11}$$

provided that $R+R_0 < I(X;B)_\omega - \epsilon_2$ and $R'+R'_0 < I(G_2;B|X)_\omega - \epsilon_3$.

We move to the security level. Denote

$$\Delta_{m'|m,k}(\mathscr{C}) = \frac{1}{2}\left\|\frac{1}{2^{nR'_0}}\sum_{k'=1}^{2^{nR'_0}}\rho^{\gamma(m',k'|x^n),x^n}_{E^nG_2^n} - \zeta^{x^n}_{E^nG_2^n}\right\|_1\,,$$

$$\Delta^*_m(\mathscr{C}) = \frac{1}{2}\left\|\frac{1}{2^{nR_0}}\sum_{k=1}^{2^{nR_0}}\omega^{x^n}_{E^nG_2^n} - \omega^{\otimes n}_{EG_2}\right\|_1\,, \tag{12}$$

with $x^n\equiv x^n(m,k)$, and $\zeta^{x^n}_{E^nG_2^n} = \frac{1}{|\Gamma_{x^n}|}\sum_{\gamma\in\Gamma_{x^n}}\rho^{\gamma,x^n}_{E^nG_2^n}$.

Based on the quantum covering lemma [28], we have the following indistinguishability bounds: [23]

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

$\forall m$, and

$$\Pr\left(\Delta_{m'|m,k}(\mathscr{C}) > e^{-\frac{\mu}{2}n}\right)\leq\exp\left\{-2^{n(R'_0-I(G_2;E|X)_\omega-\epsilon_5)}\right\} \tag{13}$$

$\forall(m,k,m')$, given $x^n\equiv x^n(m,k)$. The last two bounds tend to zero in a double exponential rate for $R_0 = I(X;EG_2)_\omega + 2\epsilon_4$. and $R'_0 = I(E;G_2|X)_\omega + 2\epsilon_5$.

B. 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,

$$\mathcal{A}_1 = \{\frac{1}{2^{n(R+R')}}\sum_{m,m'}P_e(\mathscr{C}|m,m') > \sqrt{\epsilon_1}\}\,, \tag{14}$$

$$\mathcal{A}_2 = \{\frac{1}{2^{n(R+R')}}\sum_{m,m'}P^*_e(\mathscr{C}|m,m') > \sqrt{\epsilon_1}\}\,, \tag{15}$$

$$\mathcal{B} = \{\exists(m,m') : \frac{1}{2}\left\|\rho^{m,m'}_{E^nG_B^n} - \omega^{\otimes n}_{EG_2}\right\|_1 > \delta\}\,. \tag{16}$$

By the union bound,

$$\Pr(\mathcal{A}_0\cup\mathcal{A}_1\cup\mathcal{B})\leq\Pr(\mathcal{A}_0)+\Pr(\mathcal{A}_1)+\Pr(\mathcal{B})\,. \tag{17}$$

By Markov's inequality, $\Pr(\mathcal{A}_j)\leq\sqrt{\epsilon_1}$ (see (10)-(11)). As for the last term, by the triangle inequality,

$$\begin{aligned}
&\frac{1}{2}\left\|\rho^{m,m'}_{E^nG_B^n} - \omega^{\otimes n}_{EG_2}\right\|_1\\
&= \frac{1}{2}\left\|\frac{1}{2^{n(R_0+R'_0)}}\sum_{k=1}^{2^{nR_0}}\sum_{k'=1}^{2^{nR'_0}}\rho^{\gamma(m',k'|x^n),x^n}_{E^nG_B^n} - \omega^{\otimes n}_{EG_2}\right\|_1\\
&\leq \frac{1}{2}\left\|\frac{1}{2^{nR_0}}\sum_{k=1}^{2^{nR_0}}\left(\frac{1}{2^{nR'_0}}\sum_{k'=1}^{2^{nR'_0}}\rho^{\gamma(m',k'|x^n),x^n}_{E^nG_B^n} - \zeta^{x^n}_{E^nG_2^n}\right)\right\|_1\\
&+\frac{1}{2}\left\|\frac{1}{2^{nR_0}}\sum_{k=1}^{2^{nR_0}}\zeta^{x^n}_{E^nG_2^n} - \omega^{\otimes n}_{EG_2}\right\|_1\\
&\leq \frac{1}{2^{nR_0}}\sum_{k=1}^{2^{nR_0}}\Delta_{m'|m,k}(\mathscr{C})\\
&+\frac{1}{2}\left\|\frac{1}{2^{nR_0}}\sum_{k=1}^{2^{nR_0}}\zeta^{x^n(m,k)}_{E^nG_2^n} - \omega^{\otimes n}_{EG_2}\right\|_1\,.
\end{aligned} \tag{18}$$

If we were to remove the encoding of γ, then Eve's output would have been $\omega^{x^n}_{E^nG_2^n}$, instead of $\zeta^{x}_{E^nG_2^n}$. Therefore, by trace monotonicity under quantum operations [29, Ex. 9.1.9], the last trace norm is bounded by $\Delta^*_m(\mathscr{C})$ (see (12)). Thus,

$$\begin{aligned}
&\Pr(\mathcal{B}) = \Pr\left(\frac{1}{2}\left\|\rho^{m,m'}_{E^nG_B^n} - \omega^{\otimes n}_{EG_2}\right\|_1 > \delta\right)\\
&\leq\Pr\left(\frac{1}{2^{nR_0}}\sum_{k=1}^{2^{nR_0}}\Delta_{m'|m,k}(\mathscr{C}) > \frac{\delta}{2}\right)+\Pr\left(\Delta^*_m(\mathscr{C}) > \frac{\delta}{2}\right)\\
&\leq\Pr\left(\exists k : \Delta_{m'|m,k}(\mathscr{C}) > \frac{\delta}{2}\right)+\exp\left\{-2^{n\epsilon_4}\right\}\\
&\leq\exp\left\{-2^{n\epsilon_6}\right\}
\end{aligned} \tag{19}$$

for some $\epsilon_6 > 0$ 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.

C. Semantic Security

We now complete the analysis for the maximum criteria. The proof modifies the methods of Cai [25, 26], originally applied to multiple-access channels.

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

$$e(m) \equiv \frac{1}{2^{nR'}} \sum_{m'=1}^{2^{nR'}} P_e(\mathscr{C}|m,m')\,. \tag{20}$$

Based on the analysis above, the average of $\{e(m)\}_{m=1}^{2^{nR}}$ is bounded by $\epsilon_1^{1/2}$. Therefore, at most a fraction of $\lambda = \epsilon_1{}^{1/4}$ of the messages m have $e(m) > \lambda$. Then, we can expurgate the worst $\lambda \cdot 2^{nR}$ messages, and the corresponding codewords. The guaranteed rate of the expurgated code is $R - \frac{1}{n}\log\big((1-\lambda)^{-1}\big)$, which tends to R as $n \to \infty$. Denote the expurgated message set by $\mathcal{M}$.

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 that $R' > 0$, 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 $\Pr\Big(\hat{L} \neq L\Big) = \frac{1}{n^2}\sum_{\ell=1}^{n^2} P_e(\mathscr{C}|1,\ell) \leq \sqrt{\epsilon_1}$. Now, consider the second block. Let $\Pi_1, \ldots, \Pi_{n^2}$ be an i.i.d. sequence of random permutations, each uniformly distributed on the permutation group on the excess message set $[1:2^{nR'}]$. Denote the associated random codebook by $\Pi(\mathscr{C})$. Then, for a given m',

$$\Pr(\Pi_{\ell'}(m') = \bar{m}') = \frac{(2^{nR'}-1)!}{(2^{nR'})!} = \frac{1}{2^{nR'}} \tag{21}$$

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

$$\begin{aligned} &\mathbb{E}\left[P_e^{(n)}(\Pi(\mathscr{C})|m,m')\right] \\ &= \sum_{\bar{m}'} \Pr(\Pi_{\ell'}(m') = \bar{m}') P_e^{(n)}(\mathscr{C}|m,\bar{m}') \\ &= \frac{1}{2^{nR'}} \sum_{\bar{m}'} P_e^{(n)}(\mathscr{C}|m,\bar{m}') = e(m) \leq \lambda\,. \end{aligned} \tag{22}$$

Now, by the Chernoff bound [25, Lemma 3.1],

$$\Pr\left(\frac{1}{n^2}\sum_{l'=1}^{n^2} P_e^{(n)}(\Pi(\mathscr{C})|m.m') > 4\lambda\right) < e^{-\lambda n^2} \tag{23}$$

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

$$P_e^{(n)}(\pi(\mathscr{C})|m,m') = \frac{1}{n^2}\sum_{\ell'=1}^{n^2} P_e^{(n)}(\pi_{\ell'}(\mathscr{C})|m,m') \leq 4\lambda \tag{24}$$

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

VI. Summary and Discussion

We consider semantic security with unreliable entanglement assistance, 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). The authors have recently considered the interception model with strong secrecy [23], assuming that the information is uniformly distributed.

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 (5)), 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 (8)), 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 (8)), 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 amplitude damping channel. In the interception model, where Eve can actively intercept the entanglement assistance, time division impossible and the boundary of our achievable region is disconnected. This occurs since interception can severely impact the achievable rates. 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 our previous work [23] has presented a regularized characterization for the special class of degraded channels, a single-letter capacity formula in special cases could lead to further insights.

Acknowledgments

M. Lederman and U. Pereg were supported by ISF Grants n. 939/23 and 2691/23, DIP n. 2032991, and Nevet Program of the Helen Diller Quantum Center at the Technion, n. 2033613. U. Pereg was also supported by the Israel VATAT Program for Quantum Science and Technology n. 86636903, and the Chaya Career Advancement Chair, n. 8776026.

References

[1] M. Bellare and S. Tessaro, "Polynomial-time, semantically-secure encryption achieving the secrecy capacity (2012)," *arXiv preprint arxiv:1201.3160*, 2012.

[2] 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.

[3] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Annual Cryptology Conference*. Springer, 2012, pp. 294–311.

[4] H. Boche, M. Cai, and M. Wiese, "Mosaics of combinatorial designs for semantic security on quantum wiretap channels," in *IEEE Int. Symp. Inf. Theory*. IEEE, 2022, pp. 856–861.

[5] M. Hayashi, "Upper bounds of eavesdropper's performances in finite-length code with the decoy method," *Physical Review A*, vol. 76, no. 1, p. 012329, 2007.

[6] H. Boche, M. Cai, C. Deppe, R. Ferrara, and M. Wiese, "Semantic security for quantum wiretap channels," *Journal of Mathematical Physics*, vol. 63, no. 9, 2022.

[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] M. Lederman and U. Pereg, "Secure communication with unreliable entanglement assistance," arXiv:2401.12861 **[quant-ph]**, 2024. [Online]. Available: https://arxiv.org/pdf/2401.12861.pdf

[24] 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.

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

[26] 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.

[27] 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.

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

[29] M. M. Wilde, *Quantum Information Theory*, 2nd ed. Cambridge Univ. Press, 2017.