# Entanglement-Assisted Covert Communication via Qubit Depolarizing Channels

Elyakim Zlotnick*, Boulat Bash†, and Uzi Pereg*

*Electrical and Computer Engineering and Hellen-Diller Quantum Center, Technion – Israel Institute of Technology
†Electrical and Computer Engineering, University of Arizona

**Abstract**

We consider entanglement-assisted communication over the qubit depolarizing channel under the security requirement of covert communication, where the transmission itself must be concealed from detection by an adversary. Previous work showed that $O(\sqrt{n})$ information bits can be reliably and covertly transmitted in $n$ channel uses without entanglement assistance. However, Gagatsos et al. (2020) showed that entanglement assistance can increase this scaling to $O(\sqrt{n}\log n)$ for continuous-variable bosonic channels. Here, we present a finite-dimensional parallel, and show that $O(\sqrt{n}\log n)$ covert bits can be transmitted reliably over $n$ uses of a qubit depolarizing channel. The coding scheme employs "weakly" entangled states such that the squared amplitude scales as $O\left(1/\sqrt{n}\right)$.

**Index Terms**

Quantum communication, covert communication, entanglement assistance, square-root law violation.

## I. Introduction

Privacy and confidentiality are critical in communication systems [1]. The traditional security approaches (e.g., encryption [2], information-theoretic secrecy [3], and quantum key distribution [4–6]) ensure that an eavesdropper is unable to recover any transmitted information. However, privacy and safety concerns may further require *covertness* [7, 8]. Covertness is a stringent requirement whereby the transmission itself is concealed from detection by an adversary (a warden) [9, 10]. Despite the severity of limitations imposed by covertness, it is possible to communicate $O(\sqrt{n})$ bits of information both reliably and covertly over $n$ classical channel uses [11–13]. This property is referred to as the "square root law" (SRL). The SRL has also been observed in covert communication over finite-dimensional classical-quantum channels [14–16], as well as continuous-variable bosonic channels [17–20]. Covert sensing is also governed by an SRL [21, 22]. Other covert models are studied in [23–28].

Proving the achievability of the SRLs discovered so far involves the following principles. In the finite-dimensional case, both classical and quantum [12–16], a symbol (say, 0) in the input alphabet is designated as "innocent." The codebook is generated such that a non-innocent symbol is transmitted with probability $\sim 1/\sqrt{n}$ to ensure covertness. On the other hand, the innocent symbol corresponding to zero transmitted power occurs naturally in the continuous-variable covert communication over classical additive white Gaussian noise (AWGN) [11–13] and classical-quantum bosonic [17–20] channels. Maintaining average transmitted power $O(1/\sqrt{n})$ correspondingly measured in Watts and in the emitted photon number ensures covertness.

Pre-shared entanglement resources are known to increase performance and throughput [29–33]. Gagatsos et al. [19] showed that entanglement assistance allows transmission of $O(\sqrt{n}\log n)$ reliable and covert bits over $n$ uses of continuous-variable bosonic channel, surpassing the SRL scaling (see also [34]). As in the unassisted setting, the transmission is limited to $O(1/\sqrt{n})$ mean photon number. However, so far it has remained open whether such a performance boost can be achieved in communication over finite-dimensional quantum channels.

The depolarizing channel is a fundamental model that has gained significant attention in both experimental [35, 36] and theoretical [37, 38] research. Depolarization may be regarded as the worst type of noise in a quantum system and can also be interpreted as the result of a random unitary error with a probability law that follows the Haar measure, or, alternatively, a random Pauli error. Furthermore, the insights on the depolarizing channel are often useful in the derivation of results for a general quantum channel [29], [39, Sec. 11.9.1].

Here, we show that entanglement assistance enables reliable and covert transmission of $O(\sqrt{n}\log n)$ bits in $n$ uses of a finite-dimensional qubit depolarizing channel. The entanglement-assisted covert communication scheme is illustrated in Figure 1. Our analysis is fundamentally different from the previous works. In particular, we do *not* encode a random bit sequence with $\sim 1/\sqrt{n}$ frequency (or probability) of non-innocent symbols. Instead, we employ "weakly" entangled states of the form

$$|\psi_{A_1A}\rangle = \sqrt{1-\alpha}\,|00\rangle + \sqrt{\alpha}\,|11\rangle\,, \tag{1}$$

such that the squared amplitude of this quantum superposition of states describing innocent and non-innocent symbols is $\alpha = O\left(1/\sqrt{n}\right)$. The labels $A_1$ and $A$ correspond to a reference system and to the channel input system, respectively. The former can be interpreted as Bob's share of the entanglement resource. The idea is inspired by a recent work on non-covert communication showing that controlling $\alpha \in [0,1]$ using states in (1) can outperform time division [40]. To show covertness, we observe that tracing out the resource system $A_1$ from $|\psi_{A_1A}\rangle$ results in a state identical to the one in unassisted scenario from [14, 15].

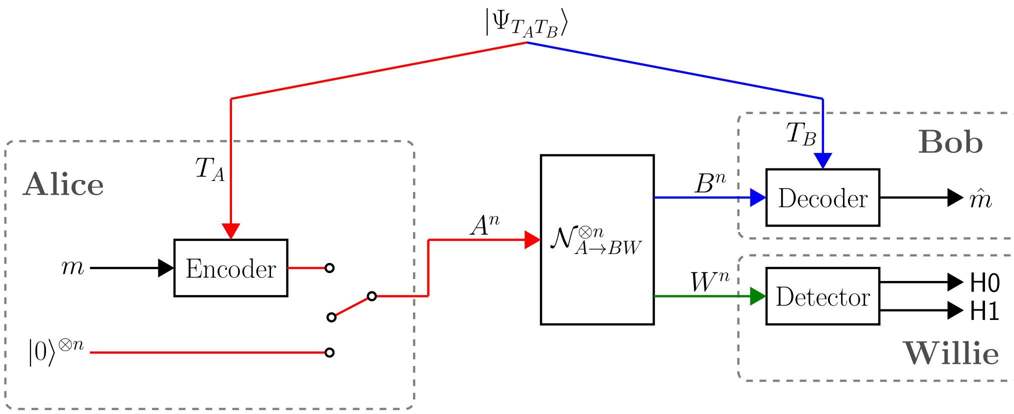


Fig. 1. Entanglement-assisted coding for covert communication over a quantum channel $\mathcal{N}_{A\to BW}$. Alice and Bob access entangled resources in systems $T_A$ and $T_B$, respectively. Message $m$ is encoded by applying the map $\mathcal{F}^{(m)}_{T_A\to A^n}$ to the entangled system $T_A$. Alice decides whether to transmit to Bob (Case 1) or not (Case 0). A switch connects the channel to the encoder in Case 1 or to a zero sequence $|0\rangle^{\otimes n}$ in Case 0. Alice transmits the systems $A^n$ over the quantum channel. Bob receives the channel output systems $B^n$, and performs a joint decoding measurement on the systems $B^n$ and $T_B$, using a POVM $\mathcal{D}_{B^nT_B}$. Willie receives the output systems $W^n$, and performs a binary measurement to test whether transmission has taken place.

The paper is organized as follows. In Section II, the definitions and channel model are provided, including notation, an overview of the system and coding, and a presentation of the covert communication problem. The results are described in Section III, with the main achievability proof in Section IV and technical details deferred to the appendices. Section V presents interpretation through energy-constrained communication, and Section V concludes with a summary and discussion.

## II. Definitions and Channel Model

### A. Notation

We use standard notation in quantum information processing, as, e.g., in [41, Ch. 2.2.1]. The Hilbert space for system $A$ is denoted by $\mathcal{H}_A$. The space of linear operators (resp. density operators) $\mathcal{H}\to\mathcal{H}$ is denoted by $\mathcal{L}(\mathcal{H})$ (resp. $\mathscr{S}(\mathcal{H})$). A positive operator-valued measure (POVM) $\{D_m\}_{m=1}^M$ is a set of positive semidefinite linear operators in $\mathcal{L}(\mathcal{H})$ such that $\sum_{m=1}^M D_m = \mathbb{1}$, where $\mathbb{1}$ is the identity operator on $\mathcal{H}$.

Given a pair of quantum states $\rho,\sigma\in\mathscr{S}(\mathcal{H})$, the quantum relative entropy is defined as $D(\rho||\sigma)=\mathrm{Tr}[\rho(\log(\rho)-\log(\sigma)]$, if $\mathrm{supp}(\rho)\subseteq\mathrm{supp}(\sigma)$; and $D(\rho||\sigma)=+\infty$, otherwise. In addition, for a spectral decomposition $\sigma=\sum_i\lambda_i P_i$, let [22]:

$$\eta(\rho||\sigma)=\sum_{i\neq j}\frac{\log(\lambda_i)-\log(\lambda_j)}{\lambda_i-\lambda_j}\mathrm{Tr}[(\rho-\sigma)P_i(\rho-\sigma)P_j]+\sum_i\frac{1}{\lambda_i}\mathrm{Tr}[(\rho-\sigma)P_i(\rho-\sigma)P_i]\,. \tag{2}$$

Given a bipartite state $\rho_{AB}$, the quantum mutual information is defined as $I(A;B)_\rho=H(\rho_A)+H(\rho_B)-H(\rho_{AB})$, where $H(\rho)\equiv-\mathrm{Tr}[\rho\log\rho]$ denotes the von Neumann entropy for a density operator $\rho$. Furthermore, the conditional quantum entropy is defined by $H(A|B)_\rho=H(\rho_{AB})-H(\rho_B)$.

A quantum channel is defined as a completely-positive trace-preserving (CPTP) linear map $\mathcal{N}_{A\to B}:\mathcal{L}(\mathcal{H}_A)\to\mathcal{L}(\mathcal{H}_B)$. Every quantum channel has a Stinespring representation, $\mathcal{N}_{A\to B}(\rho)=\mathrm{Tr}_E(V\rho V^\dagger)$, for $\rho\in\mathcal{L}(\mathcal{H}_A)$, where the operator $V:\mathcal{H}_A\to\mathcal{H}_B\otimes\mathcal{H}_E$ is an isometry.

For a given function $g(n)$, we denote by $O\big(g(n)\big)$ the set of functions $f(n)$ for which there exist positive constants $c$ and $n_0$ such that $|f(n)|\leq cg(n)$ for all $n\geq n_0$, we write $f(n)=O\big(g(n)\big)$ to indicate that a function $f(n)$ belongs to the set $O\big(g(n)\big)$ [42]. Equivalently,

$$f(n)=O\big(g(n)\big)\ \text{if}\ \limsup_{n\to\infty}\left|\frac{f(n)}{g(n)}\right|<\infty\,. \tag{3}$$

Similarly, for continuous-variable functions, $F$ and $G$ on $\in[0,\infty)$, we write

$$F(x)=\mathcal{O}\big(G(x)\big)\ \text{if}\ \limsup_{x\to 0}\left|\frac{F(x)}{G(x)}\right|<\infty\,. \tag{4}$$

Additionally, for a given function $g(n)$, we denote by $\omega\big(g(n)\big)$ the set of functions $f(n)$ where for all positive constants $c$ there exists $n_0$ such that $0 \le cg(n) \le f(n)$ for all $n \ge n_0$. We write $f(n) = \omega\big(g(n)\big)$ to indicate that a function $f(n)$ belongs to the set $\omega\big(g(n)\big)$. Equivalently,

$$f(n) = \omega\big(g(n)\big) \text{ if } \lim_{n\to\infty} \frac{f(n)}{g(n)} = \infty\,. \tag{5}$$

Similarly, for a given function $g(n)$, we denote by $o\big(g(n)\big)$ the set of functions $f(n)$ where for all positive constants $c$ there exists $n_0$ such that $0 \le f(n) \le cg(n)$ for all $n \ge n_0$. We write $f(n) = o\big(g(n)\big)$ to indicate that a function $f(n)$ belongs to the set $o\big(g(n)\big)$. Equivalently,

$$f(n) = o\big(g(n)\big) \text{ if } \lim_{n\to\infty} \frac{f(n)}{g(n)} = 0\,. \tag{6}$$

### *B. Channel Model*

Consider a covert communication quantum channel $\mathcal{N}_{A\to BW}$, which maps a quantum input state $\rho_A$ to a joint output state $\rho_{BW}$. The systems $A$, $B$, and $W$ are associated with the transmitter, the legitimate receiver, and an adversarial warden, referred to as Alice, Bob, and Willie. The marginal channels $\mathcal{N}_{A\to B}$ and $\mathcal{N}_{A\to W}$, from Alice to Bob, and from Alice to Willie, respectively, satisfy $\mathcal{N}_{A\to B}(\rho_A) = \mathrm{Tr}_W\left(\mathcal{N}_{A\to BW}(\rho_A)\right)$ and $\mathcal{N}_{A\to W}(\rho_A) = \mathrm{Tr}_B\left(\mathcal{N}_{A\to BW}(\rho_A)\right)$ for $\rho_A \in \mathscr{S}(\mathcal{H}_A)$. Our channel is memoryless: for $\rho_{A^n}$ occupying input systems $A^n = (A_1, \ldots, A_n)$, the joint output state is $\mathcal{N}^{\otimes n}_{A\to BW}(\rho_{A^n})$.

The depolarizing channel is a natural model for noise in quantum systems [29, 37, 38]. The qubit depolarizing channel with parameter $q$ transmits the input qubit perfectly with probability $1-q$, and outputs a completely mixed state with probability $q$. Consider a qubit depolarizing channel from Alice to Bob expressed as:

$$\begin{aligned}\mathcal{N}_{A\to B}(\rho_A) &= (1-q)\rho_A + q\frac{\mathbb{1}}{2}\\ &= \left(1-\frac{3q}{4}\right)\rho_A + \frac{q}{4}\left(X\rho_A X + Y\rho_A Y + Z\rho_A Z\right),\end{aligned} \tag{7}$$

where $0 < q < 1$, with dimensions $\dim(\mathcal{H}_A) = \dim(\mathcal{H}_B) = 2$, $X$, $Y$, and $Z$ are the Pauli operators, and (7) follows from the Pauli twirl identity [39, Ch. 4.7.4]. Here, we investigate covert communication over a depolarizing channel $\mathcal{V}_{A\to BE_1E_2}$ given by the Stinespring dilation:

$$\mathcal{V}_{A\to BE_1E_2}(\rho_A) = V\rho_A V^\dagger, \tag{8}$$

where $V : \mathcal{H}_A \to \mathcal{H}_B \otimes \mathcal{H}_{E_1} \otimes \mathcal{H}_{E_2}$ is an isometry defined by

$$V \equiv \sqrt{1-\frac{3q}{4}}\mathbb{1}\otimes|00\rangle + \sqrt{\frac{q}{4}}X\otimes|01\rangle + \sqrt{\frac{q}{4}}Y\otimes|11\rangle + \sqrt{\frac{q}{4}}Z\otimes|10\rangle\ . \tag{9}$$

*Remark* 1. The canonical Stinespring dilation for the qubit depolarizing channel is defined by $\widetilde{\mathcal{V}}_{A\to BE}(\rho) = \widetilde{V}\rho\widetilde{V}^\dagger$, where $\widetilde{V} \equiv \sqrt{1-\frac{3q}{4}}\mathbb{1}\otimes|0\rangle + \sqrt{\frac{q}{4}}X\otimes|1\rangle + \sqrt{\frac{q}{4}}Y\otimes|2\rangle + \sqrt{\frac{q}{4}}Z\otimes|3\rangle$ (see [38, Eq. (13)]). For $E \equiv (E_1, E_2)$, our definition in (9) is equivalent to this canonical description. Note, however, that any other Stinespring representation is equivalent to (9) up to an isometry on the environment $E$ [43, Sec. III-B].

We consider three cases:

- Scenario 1: Willie receives $(E_1, E_2)$
- Scenario 2: Willie receives $E_2$
- Scenario 3: Willie receives $E_1$

*Remark* 2. In any depolarizing channel model, Scenario 1 represents the worst-case scenario where Willie is given access to Bob's entire environment, $E = (E_1, E_2)$. This is the maximum amount of information that Willie can acquire in the quantum setting. It is important to note that the no-cloning theorem applies in the quantum setting and prohibits Willie from receiving a copy of Bob's output state, whereas in the classical setting, Willie could have a copy of Bob's output. Hence, the quantum channel from Alice to Willie is *not* a depolarizing channel.

*Remark* 3. In the boundary case of $q = 0$, Bob receives the qubit state as is, while Willie obtains no information, in agreement with the no-cloning theorem. Essentially, there is no warden in this case, hence we may transmit $O(n)$ bits, and achieve a positive Shannon rate in bits per channel use. Conversely, if $q = 1$, Willie receives the qubit state, and Bob gets only noise, rendering any communication impossible.

*Remark* 4. Scenarios 2 and 3 can be practically motivated by Willie's instruments not having access to the entirety of Alice and Bob's environment. While the model specification of Willie's observation may seem artificial, it allows us to demonstrate interesting properties of covert communication with entanglement assistance. We argue that covert communication is impossible in Scenario 1, while in Scenario 2, Alice can transmit $O(n)$ covert bits to Bob. Yet, Scenario 3 is the most interesting case, where entanglement assistance increases the scale of information bits from $O(\sqrt{n})$ to $O(\sqrt{n}\log n)$. We observe that the performance does not only depend on the dimension, as Willie receives a single qubit in both Scenarios 2 and 3, yet the behavior is completely different. Further details are given in the Results section (see Section III).

### C. Entanglement-assisted Code

The definition of a code for covert communication over a quantum channel with entanglement assistance is given below.

*Definition* 1. An $(M,n)$ entanglement-assisted code $(\Psi,\mathcal{F},\mathcal{D})$ consists of: a message set $[1:M]$, where $M$ is an integer, a pure entangled state $\Psi_{T_A T_B}$, a collection of encoding maps $\mathcal{F}^{(m)}_{T_A\to A^n}:\mathscr{S}(\mathcal{H}_{T_A})\to\mathscr{S}(\mathcal{H}_A^{\otimes n})$ for $m\in[1:M]$, and a decoding POVM $\mathcal{D}_{B^nT_B}=\{D_m\}_{m=1}^M$.

The communication setting is depicted in Figure 1. Suppose that Alice and Bob share the entangled state $\Psi_{T_AT_B}$, in systems $T_A$ and $T_B$, respectively. Alice wishes to send one of $M$ equally-likely messages. To encode a message $m$, she applies the encoding map $\mathcal{F}^{(m)}_{T_A\to A^n}$ to her share $T_A$ of the entanglement resource. This results in a quantum state $\rho^{(m)}_{A^nT_B}=(\mathcal{F}^{(m)}_{T_A^n\to A^n}\otimes\mathbb{1}_{T_B})(\Psi_{T_AT_B})$.

Alice decides whether to transmit to Bob (Case 1), or not (Case 0). The innocent state is $|0\rangle$; any other state is non-innocent. She does not transmit in Case 0: the channel input is $|0\rangle^{\otimes n}$. In Case 1, she transmits part of $\rho^{(m)}_{A^nT_B}$ occupying systems $A^n$ through $n$ uses of the covert communication channel $\mathcal{N}_{A\to BW}$. The joint output state is $\rho^{(m)}_{B^nW^nT_B}=\left(\mathcal{N}^{\otimes n}_{A\to BW}\otimes\mathrm{id}_{T_B}\right)\left(\rho^{(m)}_{A^nT_B}\right)$. Bob decodes the message from the reduced output state $\rho^{(m)}_{B^nT_B}=\mathrm{Tr}_{W^n}\left[\rho^{(m)}_{B^nW^nT_B}\right]$ by applying the POVM $\mathcal{D}_{B^nT_B}$.

*Remark* 5. We assume without loss of generality that the innocent state is represented by $|0\rangle$. However, it is important to note that this choice is arbitrary. Since the depolarizing channel is symmetric with respect to the input state, our findings can easily be extended to any product state $|\psi_{\text{idle}}\rangle^{\otimes n}$ that corresponds to an idle transmission system.

*Remark* 6. In our achievability analysis, we identify the entanglement resource $\Psi_{T_AT_B}$ with the product state $\psi^{\otimes n}_{A_1A}$, as in (1). That is, we use entanglement resources such that Alice and Bob's entangled systems, $T_A$ and $T_B$, consist of $n$ copies of $A$ and $A_1$, respectively.

### D. Reliability and Covertness

We characterize reliability by the average probability of decoding error for entanglement-assisted code $(\Psi,\mathcal{F},\mathcal{D})$ defined in Section II-C:

$$P_e^{(n)}(\Psi,\mathcal{F},\mathcal{D})=\frac{1}{M}\sum_{m=1}^{M}\mathrm{Tr}\left[(\mathbb{1}-D_m)\rho^{(m)}_{B^nT_B}\right] \tag{10}$$

where $\rho^{(m)}_{B^nT_B}$ is the reduced state of the joint output state.

Willie does not have access to Alice and Bob's entanglement resource and receives the reduced output state $\rho^{(m)}_{W^n}=\mathrm{Tr}_{B^nT_B}\left[\rho^{(m)}_{B^nW^nT_B}\right]$ occupying the system $W^n$. Willie has to determine whether Alice transmitted to Bob. To this end, he performs a binary measurement $\{\Delta_{\mathsf{H0}},\Delta_{\mathsf{H1}}\}$, where the outcome $\mathsf{H1}$ represents the hypothesis that Alice sent information, while $\mathsf{H0}$ indicates the contrary hypothesis.

He fails by either accusing Alice of transmitting when she is not (false alarm), or missing Alice's transmission (missed detection). Denoting the probabilities of these errors by $P_{\mathsf{FA}}=P(\text{choose }\mathsf{H1}|\mathsf{H0}\text{ is true})$ and $P_{\mathsf{MD}}=P(\text{choose }\mathsf{H0}|\mathsf{H1}\text{ is true})$, respectively, and assuming equally likely hypotheses, Willie's average probability of error is $E^{(n)}=\frac{P_{\mathsf{FA}}+P_{\mathsf{MD}}}{2}$. A random choice yields an ineffective detector with $E^{(n)}=\frac{1}{2}$. The goal of covert communication is to design a sequence of codes such that Willie's detector is forced to be arbitrarily close to ineffective. Denote the average state that Willie receives by

$$\overline{\rho}_{W^n}=\frac{1}{M}\sum_{m=1}^{M}\rho^{(m)}_{W^n} \tag{11}$$

where $\rho^{(m)}_{W^n}$ is the reduced state of the joint output $\rho^{(m)}_{B^nW^nT_B}$. A sufficient condition [14, 15] to render *any* detector ineffective for Willie is $D(\overline{\rho}_{W^n}||\omega_0^{\otimes n})\approx 0$, where $\omega_0\equiv\mathcal{N}_{A\to W}(|0\rangle\langle 0|)$ is the output corresponding to innocent input. Formally, an $(M,n,\varepsilon,\delta)$-code for entanglement-assisted covert communication satisfies

$$P_e^{(n)}(\Psi,\mathcal{F},\mathcal{D})\le\varepsilon \tag{12}$$

and

$$D(\overline{\rho}_{W^n}||\omega_0^{\otimes n})\le\delta\,. \tag{13}$$

### E. Capacity

In traditional communication problems, the coding rate is defined as $R = \frac{\log(M)}{n}$, i.e., the number of bits per channel use. In covert communication, however, the best achievable rate is zero, since the number of information bits is sublinear in $n$. Here we prove that entanglement assistance allows reliable transmission of $\log(M) = O(\sqrt{n}\log n)$ covert bits. Hence, the covert coding rate is characterized as in [19]:

$$L = \frac{\log(M)}{\sqrt{\delta n}\log n}. \tag{14}$$

where $\delta$ is the covertness level in (13).

*Definition* 2. A covert rate $L > 0$ is achievable with entanglement assistance if for every $\varepsilon, \delta > 0$, and sufficiently large $n$, there exists a $(2^{L\sqrt{\delta n}\log n}, n, \varepsilon, \delta)$ code.

*Remark* 7. Achievable rates correspond to error and covertness levels that tend to zero in the limit of $n \to \infty$. That is, one may rewrite Definition 2 as follows [14]. A rate $L$ is asymptotically achievable if there exists a sequence of codes such that

$$\frac{\log(M)}{\log n\sqrt{nD(\overline{\rho}_{W^n}||\omega_0^{\otimes n})}} \geq L - \zeta_n \quad \forall n \geq n_0 \tag{15}$$

for some $n_0 > 0$ and sequence $\zeta_n$ that tends to zero as $n \to \infty$, while the error probability satisfies

$$\lim_{n\to\infty} P_e^{(n)}(\Psi, \mathcal{F}, \mathcal{D}) = 0\,, \tag{16}$$

and the covertness,

$$\lim_{n\to\infty} D(\overline{\rho}_{W^n}||\omega_0^{\otimes n}) = 0\,. \tag{17}$$

*Definition* 3. The entanglement-assisted covert capacity is defined as the supremum of achievable covert rates. We denote this capacity by $C_{\text{cov-EA}}(\mathcal{N})$, where the subscript stands for covert communication with entanglement assistance.

Consider the following state, with $\alpha \in [0, 1]$:

$$\varphi_\alpha \equiv (1-\alpha)\,|0\rangle\langle 0| + \alpha\,|1\rangle\langle 1|\ . \tag{18}$$

Let $\gamma_n = o(1) \cap \omega\left(\frac{\log n}{n^{1/6}}\right)$, that is, as $n \to \infty$,$\gamma_n \to 0$ and $\frac{n^{1/6}\gamma_n}{\log n} \to +\infty$. Choosing $\alpha = \alpha_n$ where

$$\alpha_n \equiv \frac{\gamma_n}{\sqrt{n}} \tag{19}$$

ensures covertness [14, 15]. That is, if the average state of the input system $A^n$ is given by $\rho_{A^n} = (\varphi_{\alpha_n})^{\otimes n}$, then the covertness requirement (13) is satisfied for large $n$.

## III. Results

We address the three scenarios presented in Section II-B. We begin with the case where Willie receives the entire environment, i.e., both $E_1$ and $E_2$. This can be viewed as the worst-case scenario (see Remark 2).

*Theorem* 1. Covert communication is impossible in Scenario 1. Hence, if $W = (E_1, E_2)$, then $C_{\text{cov-EA}}(\mathcal{N}) = 0$.

*Proof of Theorem 1.* Let $\omega_0$ and $\omega_1$ denote Willie's output states corresponding to the inputs $|0\rangle$ and $|1\rangle$, respectively. That is $\omega_x \equiv \mathcal{N}_{A\to W}(|x\rangle\langle x|)$ for $x \in \{0, 1\}$.

In this scenario, we have $\text{supp}(\omega_1) \not\subseteq \text{supp}(\omega_0)$. We show this in detail in Appendix I-A . Therefore, Willie can perform a measurement to detect a non-zero transmission with certainty. □

Essentially, in Scenario 1, Willie's entanglement with the transmitted qubit is strong enough for him to detect any encoding operation.

Next, we consider another extreme setting.

*Theorem* 2. Covert communication is trivial in Scenario 2. That is, if $W = E_2$, then Alice can communicate unconstrained by the covertness requirement, and transmits $O(n)$ bits.

*Proof of Theorem 2.* If $W = E_2$, then Willie receives $\omega_0 = \omega_1 = \left(1 - \frac{q}{2}\right)|0\rangle\langle 0| + \frac{q}{2}\,|1\rangle\langle 1|$ (see Appendix I-B). In this scenario, even without entanglement assistance, Alice can transmit classical codewords as in the standard non-covert model, while Willie cannot discern between zero and non-zero inputs. □

We proceed to our main result on the entanglement-assisted covert capacity $C_{\text{cov-EA}}$ of the depolarizing channel. From this point on, we focus on Scenario 3, where Willie receives the first qubit of the environment (see Section II-B).

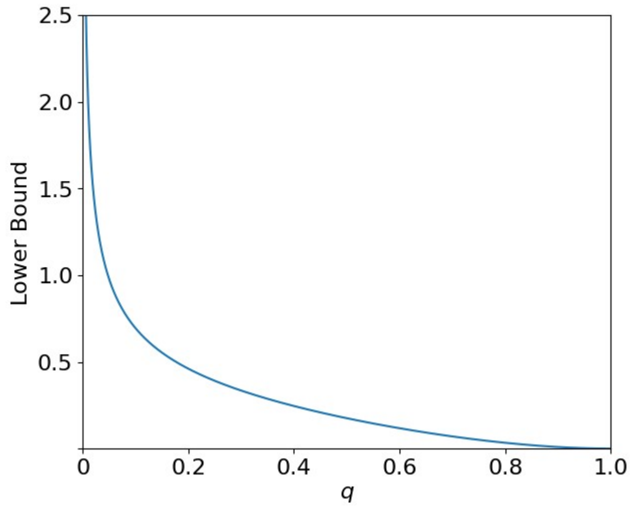


Fig. 2. The lower bound on the entanglement-assisted covert capacity of Scenario 3 in Theorem 3, as a function of the noise parameter $q$.

*Theorem* 3. Consider a qubit depolarizing channel $\mathcal{N}_{A\to BW}$ as specified in Section II-B above, where $W = E_1$. The entanglement-assisted covert capacity is bounded as

$$C_{\text{cov-EA}}(\mathcal{N}) \geq \frac{4\sqrt{2}}{3}\frac{(1-q)^2}{(2-q)\sqrt{\eta(\omega_1||\omega_0)}} \tag{20}$$

where $\omega_0 \equiv \mathcal{N}_{A\to W}(|0\rangle\langle 0|)$ and $\omega_1 \equiv \mathcal{N}_{A\to W}(|1\rangle\langle 1|)$.

Note that $\eta(\omega_1||\omega_0)$ is defined in (2). Our lower bound is depicted in Figure 2. As can be seen in the figure, our lower bound has the expected behavior for the covert capacity in the boundary points (see Remark 3). For $q = 0$, we have $C_{\text{cov-EA}}(\mathcal{N}) = +\infty$ in the $\sqrt{n}\log n$ scale, because the warden only receives noise and Alice can transmit a linear number of information bits (effectively, there is no warden). Whereas, for $q = 1$, the covert and non-covert capacities are zero.

Following the definitions in Section II-E, a bound of the form $C_{\text{cov-EA}} \geq L_0$ implies that it is possible to transmit $L_0\sqrt{\delta n}\log n$ information bits reliably and covertly (see Definitions 2 and 3). Recall that without entanglement assistance, covert communication requirements limit the message to $O(\sqrt{n})$ information bits [14, 15]. Thereby, we have established that entanglement assistance increases the message scale in covert communication, from $O(\sqrt{n})$ to $O(\sqrt{n}\log n)$ information bits. A similar result has been shown for continuous-variable bosonic channels by Gagatsos et al. [19]. To the best of our knowledge, our result in Theorem 3, on the depolarizing channel, is the first demonstration of such a property for a finite-dimensional channel.

*Remark* 8. In some communication settings, the coding scale is larger for continuous-variable channels. For example, in deterministic identification, the code size is super-exponential and scales as $2^{n\log nR}$ for Gaussian channels [44] and Poisson channels [45]. On the other hand, deterministic identification is limited to an exponential scale for finite-dimensional channels [46]. Nevertheless, we show here that in covert communication over a qubit depolarizing channel, entanglement assistance can increase the number of information bits from $O(\sqrt{n})$ to $O(\sqrt{n}\log n)$, as in the bosonic case. In other words, the $\log n$ performance boost is not reserved to continuous variable systems.

## IV. Proof of Theorem 3

### A. Proof Idea

Consider Scenario 3 presented in Section II-B. First, we identify an entangled state that meets the above condition for covertness. As opposed to previous works [12–14], we do *not* encode a random bit sequence with $\sim {}^1/\sqrt{n}$ frequency (or probability) of 1's. Instead, we encode "weakly" entangled states as in (1), such that the squared amplitude of this quantum superposition of states describing innocent and non-innocent symbols is $\alpha = O\left({}^1/\sqrt{n}\right)$. In order to guarantee covertness, the probability amplitude must be such that the state of the transmission is very close to that of a sequence of innocent states $|0\rangle^{\otimes n}$. Furthermore, we adapt the approach in [19] to analyze the order of the number of covert information bits.

### B. Position-Based Coding

The lemma below provides an achievability result for the transmission over a memoryless quantum channel, regardless of covertness. For every $\rho, \sigma \in \mathscr{S}(\mathcal{H})$, define the second and fourth moments of the quantum relative entropy,

$$V(\rho||\sigma) = \text{Tr}[\rho|(\log(\rho) - \log(\sigma) - D(\rho||\sigma)|^2]\,, \tag{21}$$

$$Q(\rho||\sigma) = \mathrm{Tr}[\rho|(\log(\rho) - \log(\sigma) - D(\rho||\sigma)|^4] \tag{22}$$

respectively.

*Lemma* 4 (Position-based coding, see [19, Lemma 1] [47, 48]). Consider a memoryless quantum channel $\mathcal{N}_{A\to B}$. For every pure entangled state $|\psi_{A_1A}\rangle \in \mathcal{H}_{A_1} \otimes \mathcal{H}_A$, arbitrarily small $\varepsilon > 0$, and sufficiently large $n$, there exists a coding scheme that employs pre-shared entanglement resources to transmit $\log(M)$ bits over $n$ uses of $\mathcal{N}_{A\to B}$ with decoding error probability $\varepsilon$ such that:

$$\log(M) \geq nD(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B) + \sqrt{nV(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)}\Phi^{-1}(\varepsilon) - C_n \tag{23}$$

with

$$\psi_{A_1B} = (\mathrm{id}_{A_1} \otimes \mathcal{N}_{A\to B})(\psi_{A_1A}) \tag{24}$$

and

$$C_n = \frac{\beta_{\text{B-E}}}{\sqrt{2\pi}} \frac{[Q(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)]^{\frac{3}{4}}}{V(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)} + \frac{V(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)}{\sqrt{2\pi}} + \log(4\varepsilon n) \tag{25}$$

where $D(\cdot||\cdot)$ is the quantum relative entropy, $V(\cdot||\cdot)$, $Q(\cdot||\cdot)$ are the second and fourth moments in (21)-(22), $\beta_{\text{B-E}}$ is the *Berry-Esseen* constant satisfying $0.40973 \leq \beta_{\text{B-E}} \leq 0.4784$, and

$$\Phi^{-1}(\varepsilon) = \sup\{\varepsilon \in [0,1] | \Phi(\varepsilon) \leq \varepsilon\}\,, \qquad \Phi(\varepsilon) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\varepsilon} e^{\frac{x^2}{2}}\, dx\,. \tag{26}$$

The derivation of Lemma 4 builds upon a *position-based* coding scheme, where each message is associated with $n$ entangled pairs and Bob uses sequential decoding on the output and the entanglement resources for each message consecutively [19, 48] (see proof of Lemma 1 in [19]).

### C. Analysis

In this section, we give the proof for Theorem 3. We present the main stages of the proof, while the technical details are deferred to the appendix. We begin with the following lemma.

*Lemma* 5. Let $\gamma_n = n^{\nu - \frac{1}{6}}$, where $0 < \nu < \frac{1}{6}$ is arbitrary and does not depend on $n$. Then, there exists an entanglement-assisted covert coding scheme for qubit depolarizing channel with blocklength $n$, size $M$, and average error probability $\varepsilon$ that satisfies

$$\log(M) \geq 2\left(\frac{2}{3} - \nu\right) \frac{(1-q)^2}{2-q} \gamma_n \sqrt{n} \log n + O(\sqrt{n}\gamma_n)\,. \tag{27}$$

*Proof.* To prove the lemma, we need to show that, for arbitrarily small $\varepsilon, \delta > 0$ and large $n$, there exists an $(M, n, \varepsilon, \delta)$ code for the depolarizing channel with entanglement assistance, with a code size $M$ as in (27). To this end, we apply Lemma 4 with $|\psi_{A_1A}\rangle$ as in (1), with a parameter $\alpha = \alpha_n$ as in (19). Note that setting $\gamma_n = n^{\nu - \frac{1}{6}}$ as in the lemma statement yields

$$\alpha_n = \frac{\gamma_n}{\sqrt{n}} = n^{\nu - \frac{2}{3}}. \tag{28}$$

Intuitively, as the value of $\alpha_n$ is small, the input state that Alice sends through the channel is close to the innocent state, i.e., $\psi_A \approx |0\rangle\langle 0|$. Given the joint state $\psi_{A_1A} \equiv |\psi_{A_1A}\rangle\langle\psi_{A_1A}|$, the channel input $A$ is in the reduced state $\psi_A \equiv \mathrm{Tr}_{A_1}[|\psi_{A_1A}\rangle\langle\psi_{A_1A}|] = \varphi_{\alpha_n}$, with $\varphi_{\alpha_n}$ as in (18). That is, the reduced input state fits the achievability proof for the covert capacity without entanglement assistance in [14, 15], i.e., without entanglement assistance. Based on the analysis therein, this input state meets the covertness requirement. As the covertness requirement does not involve the entanglement resources, it follows that covertness holds here as well, i.e., $D(\overline{\rho}_{W^n}||\omega_0^{\otimes n})$ tends to zero as $n \to \infty$.

Having established both reliability and covertness, it remains to estimate the code size. To this end, consider the joint state $\psi_{A_1B}$ of the output system $B$ and the reference system $A_1$, as in (24). In order to estimate each term on the right-hand side of (23), we first derive expressions for the operator logarithms, $\log(\psi_{A_1B})$ and $\log(\psi_{A_1} \otimes \psi_B)$, and then we approximate the relative entropy $D(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)$, and its second and fourth moments $V(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)$ and $Q(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)$.

The full technical details are given in the appendices. In Appendix II, we analyze the spectral decompositions, and then use the Taylor expansions near $\alpha = 0$. Throughout the derivation, we maintain the exact value of the dominant terms and reduce the approximation error to its order class, following the asymptotic notation in Section II-A. In Appendix III, we estimate the quantum relative entropy and its moments, and show that

$$D(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B) = -2\frac{(1-q)^2}{2-q} \alpha_n \log(\alpha_n) + O(\alpha_n)\,,$$

$$V(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) = O\big(\alpha_n \log^2(\alpha_n)\big)\,,$$
$$Q(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) = O\big(\alpha_n \log^2(\alpha_n)\big)\,, \tag{29}$$

for $\alpha = \alpha_n$ as chosen above (see (28)).

The proof is concluded by placing the approximations above into (23) , as detailed in Appendix IV. □

We are now ready for the proof of Theorem 3.

*Proof of Theorem 3.* First, we observe that in this scenario, $\text{supp}(\omega_1) \subseteq \text{supp}(\omega_0)$ and, in addition, $\omega_0 \neq \omega_1$ (see derivation in Appendix I-C), therefore, covert communication is possible, and not trivial. Then, even if Willie's output state is $\omega_1$, there is still ambiguity whether the input is innocent or not.

By Lemma 5, we have established achievability for the following covert rate:

$$L_n = \frac{2\left(\frac{2}{3}-\nu\right)\frac{(1-q)^2}{2-q}\gamma_n + O\left(\frac{\gamma_n}{\log n}\right)}{\sqrt{D(\overline{\rho}_{W^n}||\omega_0^{\otimes n})}}\,. \tag{30}$$

We have seen that covertness holds as the reduced input state is the same as the average input in previous code constructions [14, 15]. Furthermore, the following property extends as well: there exists $\zeta > 0$ such that,

$$|D(\overline{\rho}_{W^n}||\omega_0^{\otimes n}) - nD(\omega_{\alpha_n}||\omega_0)| \le e^{-\zeta\gamma_n^{\frac{3}{2}}n^{\frac{1}{4}}}\,, \tag{31}$$

where $\overline{\rho}_{W^n}$ is the actual state of Willie's system as defined in (11), the state $\omega_0 = \mathcal{N}_{A\to W}(|0\rangle\langle 0|)$ is the Willie's output corresponding to the innocent input, and $\omega_{\alpha_n} \equiv \mathcal{N}_{A\to W}(\varphi_{\alpha_n})$, with $\varphi_{\alpha_n}$ as in (18) (see achievability proof in [14], [15, Theorem 1]). This holds since the derivation depends on the reduced input state alone, as Willie does not have access to the entanglement resource.

Based on a result that was recently developed for covert sensing using entangled states [22, Lemma 5],

$$D(\omega_{\alpha_n}||\omega_0) = \frac{\alpha_n^2}{2}\eta(\omega_1||\omega_0) + O(\alpha_n^3) \tag{32}$$

for sufficiently small $\alpha_n$. Thus, by (31) and (32),

$$D(\overline{\rho}_{W^n}||\omega_0^{\otimes n}) \le \frac{\gamma_n^2}{2}\eta(\omega_1||\omega_0) + e^{-\zeta\gamma_n^{\frac{3}{2}}n^{\frac{1}{4}}} + O\left(\frac{\gamma_n^3}{\sqrt{n}}\right)\,. \tag{33}$$

By applying this bound to the denominator in (30), we have:

$$L_n \ge \frac{2\left(\frac{2}{3}-\nu\right)\frac{(1-q)^2}{2-q}\gamma_n + O\left(\frac{\gamma_n}{\log n}\right)}{\sqrt{\frac{\gamma_n^2}{2}\eta(\omega_1||\omega_0) + e^{-\zeta\gamma_n^{\frac{3}{2}}n^{\frac{1}{4}}} + O\left(\frac{\gamma_n^3}{\sqrt{n}}\right)}}\,. \tag{34}$$

Hence, in the limit of $n\to\infty$, we achieve

$$L \ge \frac{2\left(\frac{2}{3}-\nu\right)\frac{(1-q)^2}{2-q}}{\sqrt{\frac{1}{2}\eta(\omega_1||\omega_0)}} \tag{35}$$

for arbitrarily small $\nu > 0$, which completes the proof. □

## V. Energy Constraint Interpretation

We provide an interpretation for the logarithmic advantage. In the bosonic case, the ratio between the entanglement-assisted capacity and the unassisted capacity, follows a logarithmic trend of $\log(1/E)$, where $E$ is the limit on the transmission mean photon number [49, 50]. Yet, to ensure covertness, the mean photon number must be restricted to $E_n = O(\frac{1}{\sqrt{n}})$. Consequently, an $O(\log n)$ factor arises [51]. Based on our derivation, a similar phenomenon is observed for the qubit depolarizing channel.

Indeed, consider communication over a finite-dimensional channel under an energy constraint, $E$, without the covertness constraint [49, Sec. 2]. Then, the capacities with and without entanglement assistance, are given by [49]

$$C_0(\mathcal{N},E) = \max_{\{p_x(x),\phi_A^{(x)}\}:\text{Tr}(\mathsf{F}\rho_A)\le E} I(X;B)_\rho \tag{36}$$

$$C_{\text{EA}}(\mathcal{N},E) = \max_{\psi_{A_1A}:\text{Tr}(\mathsf{F}\psi_A)\le E} I(A_1;B)_\omega \tag{37}$$

with the observable (Hamiltonian) $\mathsf{F} = |1\rangle\langle 1|$, where

$$\rho_{XA} = \sum_{x\in\mathcal{X}} p_X(x)\,|x\rangle\langle x| \otimes \phi_A^{(x)}\,, \tag{38}$$

$$\rho_{XB} = (\mathrm{id}_X \otimes \mathcal{N}_{A\to B})(\rho_{XA})\,, \tag{39}$$

and

$$\omega_{A_1 B} = (\mathrm{id}_X \otimes \mathcal{N}_{A\to B})(\psi_{A_1 A}) \tag{40}$$

The maximization in (36) is over all the input ensembles $\{p_x(x), \phi_A^{(x)}\}$ such that the reduced average state $\rho_A \equiv \mathrm{Tr}_X(\rho_{XA})$ satisfies the energy constraint $\mathrm{Tr}(\mathsf{F}\rho_A) \leq E$. Similarly, the maximization in (37) is over all the entangled input states $|\psi_{A_1 A}\rangle$ with a reduced state $\psi_A$ such that $\mathrm{Tr}(\mathsf{F}\psi_A) \leq E$.

Now, consider the qubit depolarizing channel with an energy constraint $E$, where $0 < E \leq \frac{1}{2}$. Without assistance, the ensemble that achieves the maximum is $\{(1-E, E), |0\rangle, |1\rangle\}$. The capacity without entanglement assistance is thus given by

$$C_0(\mathcal{N}, E) = h_2\left(E * \frac{q}{2}\right) - h_2\left(\frac{q}{2}\right)\,, \tag{41}$$

where '$*$' denotes the binary convolution operation: $\alpha * \beta = (1-\alpha)\beta + \alpha(1-\beta)$.

As for the entanglement-assisted capacity, the maximum is attained for

$$|\Psi_{A_1 A}\rangle \equiv \sqrt{1-E}\,|00\rangle + \sqrt{E}\,|11\rangle\ . \tag{42}$$

Therefore,

$$C_{\mathrm{EA}}(\mathcal{N}, E) = h_2(E) + h_2\left(E * \frac{q}{2}\right) - H(\psi_{A_1 B})\,. \tag{43}$$

where

$$\psi_{A_1 B} = (\mathrm{id} \otimes \mathcal{N}_{A\to B})(|\Psi_{A_1 A}\rangle\langle\Psi_{A_1 A}|)\,. \tag{44}$$

For completeness, we prove those capacity characterizations above in Appendix V.

Now, based on the derivations in Subsection IV-C, for $E \to 0$, we have

$$\begin{aligned}\frac{C_{\mathrm{EA}}(\mathcal{N}, E)}{C_0(\mathcal{N}, E)} &= \frac{h_2(E) + h_2\left(E * \frac{q}{2}\right) - H(\psi_{A_1 B})}{h_2\left(E * \frac{q}{2}\right) - h_2\left(\frac{q}{2}\right)} \\ &\sim \frac{-E\log(E)}{E} \\ &= -\log(E)\,,\end{aligned} \tag{45}$$

by taking $\alpha = E$. To satisfy the covert constraint, we effectively impose an energy constraint $E_n \sim \frac{1}{\sqrt{n}}$, which results in the following ratio between the entanglement-assisted and unassisted covert capacities,

$$\frac{C_{\text{EA-cov}}(\mathcal{N})}{C_{0\text{-cov}}(\mathcal{N})} \sim \log n\,. \tag{46}$$

## VI. Summary and Discussion

We have studied covert communication through the qubit depolarizing channel, where Alice and Bob share entanglement resources and wish to communicate, while an adversarial warden, Willie, is trying to detect their communication. We addressed three scenarios. In the first scenario, Willie can determine with certainty whether Alice has transmitted a non-innocent state, making covert communication impossible. In the second, Willie cannot distinguish between the $|0\rangle$ and $|1\rangle$ inputs, making covert communication effortless. The outcomes of our study mainly pertain to the third scenario, wherein covert communication is both feasible and non-trivial. Our results show that it is possible to transmit $O(\sqrt{n}\log n)$ bits reliably and covertly. This result surpasses the maximum scaling of $O(\sqrt{n})$ reliable and covert bits in both the classical and quantum cases without entanglement assistance.

The square root law for the unassisted cases (both classical and quantum) was derived for the non-trivial scenario, in which Bob cannot determine with certainty if Alice sends a non-innocent symbol. However, if Bob has this capability, i.e., $\mathrm{supp}(\mathcal{N}_{A\to B}(|1\rangle\langle 1|)) \nsubseteq \mathrm{supp}(\mathcal{N}_{A\to B}(|0\rangle\langle 0|))$, then the scaling law becomes $O(\sqrt{n}\log n)$, even for a classical channel [12, 14, 15]. Therefore, it appears that entanglement assistance has a similar effect as granting Bob the capability of identifying a non-innocent transmission with certainty. We also discussed the energy constraint interpretation in Section V, where we have seen that the entanglement-assisted and unassisted capacities under an energy constraint scale as $C_{\mathrm{EA}}(\mathcal{N}, E) \sim -E\log(E)$ and $C_0(\mathcal{N}, E) \sim E$, respectively, without covertness. Hence, the ratio between those capacities follows $\log(1/E)$. The covertness constraint effectively imposes an energy constraint of $E_n \sim \frac{1}{\sqrt{n}}$. Hence, the ratio between the covert entanglement-assisted and unassisted capacity scales as $\log n$. While the energy constraint interpretation provides another view on this behavior, a full understanding of the effect of entanglement resources on the performance remains elusive.

A promising future research direction is to consider a more general model, where the covert communication channel is formed by a concatenation of the depolarizing channel $\mathcal{V}_{A\to BE}$ with a general channel $\mathcal{P}_{E\to W}$ to Willie, namely, $\mathcal{N}_{A\to BW} =$

$(\mathrm{id}_B \otimes \mathcal{P}_{E\to W}) \circ \mathcal{V}_{A\to BE}$. Those scenarios are out of scope for the current paper, but it would be interesting to consider in future work. The amount of entanglement utilized also requires further study. Recently, Wang et al. [34] improved the previous result by Gagatsos et al. [19] and showed achievability using $\sim \sqrt{n}$ two-mode squeezed vacuum states, i.e., entanglement of dimension $\sim 2^{\sqrt{n}}$, which is negligible when compared to the code size. Here, relying on position-based coding, we use $n$ qubit pairs per message. It would be worthwhile to explore methods to reduce the entanglement dimension within the finite dimensional setting as well.

Our results can be viewed as a step forward towards understanding covert communication via general quantum channels in the presence of pre-shared entanglement resources. Following the past literature, the preliminary results on entanglement-assisted communication via the depolarizing and erasure channels [29] have led to a complete characterization for a general quantum channel [30]. We can only hope to see the same progress in the study of covert communication. The quantum erasure channel is another fundamental model in quantum information theory [52], where for an input state $\rho$, Bob receives the original state with probability $1-q$, or an erasure state $|e\rangle\langle e|$, which is orthogonal to the qubit space, with probability $q$. For this channel, Bob can determine that Alice sent $|1\rangle$ with certainty, as $\mathrm{supp}(\mathcal{N}_{A\to B}(|1\rangle\langle 1|)) \not\subseteq \mathrm{supp}(\mathcal{N}_{A\to B}(|0\rangle\langle 0|))$. Thereby, the scaling law becomes $O(\sqrt{n}\log n)$ information bits, even without entanglement resources. At this point, it remains unclear whether this scaling can be achieved with entanglement assistance for every quantum channel that satisfies $\mathrm{supp}(\mathcal{N}_{A\to W}(|1\rangle\langle 1|)) \subseteq \mathrm{supp}(\mathcal{N}_{A\to W}(|0\rangle\langle 0|))$.


## ACKNOWLEDGMENT

This work was supported by the VATAT Program for Quantum Science and Technology through Grant n. 86636903 (Pereg, Zlotnick), and by the US National Science Foundation (NSF) grant CCF-2045530 (Bash). U. Pereg was also supported by the Chaya Chair n. 8776026, and the Helen Diller Quantum Center at the Technion. The authors would like to thank Johannes Rosenberger (Technical University of Munich) for useful discussions. Furthermore, the authors thank the anonymous reviewer for pointing out the interpretation and relation to the asymptotic behavior of the ratio between the entanglement-assisted and unassisted capacities.


## APPENDIX ORGANIZATION

The appendices are organized as follows. In Appendix I we provide the technical analysis of the channel from Alice to Willie. Appendix II presents mathematical tools and derivations for decomposing the operators $\psi_{A_1B}$ and $\psi_{A_1} \otimes \psi_B$, and their logarithms. In Appendix III, we provide the detailed approximation of $D(\psi_{A_1B}||\psi_{A_1} \otimes \psi_B)$ and its moments. Appendix IV presents the approximation of the code size.

## APPENDIX I
## WILLIE'S CHANNELS

### A. Willie Receives $(E_1, E_2)$

For the given scenario where Willie receives the entire environment, it is possible to demonstrate that,

$$\omega_0 = \begin{pmatrix} 1-\frac{3q}{4} & 0 & 0 & \sqrt{\frac{q}{4}(1-\frac{3q}{4})} \\ 0 & \frac{q}{4} & -i\frac{q}{4} & 0 \\ 0 & i\frac{q}{4} & \frac{q}{4} & 0 \\ \sqrt{\frac{q}{4}(1-\frac{3q}{4})} & 0 & 0 & \frac{q}{4} \end{pmatrix}, \tag{47}$$

and

$$\omega_1 = \begin{pmatrix} 1-\frac{3q}{4} & 0 & 0 & -\sqrt{\frac{q}{4}(1-\frac{3q}{4})} \\ 0 & \frac{q}{4} & i\frac{q}{4} & 0 \\ 0 & -i\frac{q}{4} & \frac{q}{4} & 0 \\ -\sqrt{\frac{q}{4}(1-\frac{3q}{4})} & 0 & 0 & \frac{q}{4} \end{pmatrix}. \tag{48}$$

The null spaces of $\omega_0$ and $\omega_1$ contain vectors,

$$|e_0\rangle \equiv \begin{pmatrix} 0 \\ i \\ 1 \\ 0 \end{pmatrix}, \tag{49}$$

and

$$|e_1\rangle \equiv \begin{pmatrix} 0 \\ -i \\ 1 \\ 0 \end{pmatrix}, \tag{50}$$

respectively. Since $\langle e_0|e_1\rangle = 0$, it follows that $\mathrm{supp}(\omega_1) \not\subseteq \mathrm{supp}(\omega_0)$.

### B. Willie Receives $E_2$

Suppose Alice transmits the general state $\rho = (1-a)\,|0\rangle\langle 0| + a\,|1\rangle\langle 1| + b\,|0\rangle\langle 1| + b^*\,|1\rangle\langle 0|$. Then, Willie receives the state,

$$\mathcal{N}_{A\to W}(\rho) = \left(1-\frac{q}{2}\right)|0\rangle\langle 0| + \frac{q}{2}\,|1\rangle\langle 1| + 2\,\mathrm{Re}\{b\}\Bigg(\left(\sqrt{\left(1-\frac{3q}{4}\right)\frac{q}{4}} + i\frac{q}{4}\right)|0\rangle\langle 1| + \left(\sqrt{\left(1-\frac{3q}{4}\right)\frac{q}{4}} - i\frac{q}{4}\right)|1\rangle\langle 0|\Bigg)\,. \tag{51}$$

Substituting $\rho = |0\rangle\langle 0|$ and $\rho = |1\rangle\langle 1|$ into (51), respectively, yields:

$$\begin{aligned}\omega_0 &= \mathcal{N}_{A\to W}(|0\rangle\langle 0|)\\ &= \left(1-\frac{q}{2}\right)|0\rangle\langle 0| + \frac{q}{2}\,|1\rangle\langle 1|\ ,\end{aligned} \tag{52}$$

and

$$\begin{aligned}\omega_1 &= \mathcal{N}_{A\to W}(|1\rangle\langle 1|)\\ &= \left(1-\frac{q}{2}\right)|0\rangle\langle 0| + \frac{q}{2}\,|1\rangle\langle 1|\ .\end{aligned} \tag{53}$$

### C. Willie Receives $E_1$

Suppose Alice transmits the general state $\rho = (1-a)\,|0\rangle\langle 0| + a\,|1\rangle\langle 1| + b\,|0\rangle\langle 1| + b^*\,|1\rangle\langle 0|$. Then, Willie receives the state,

$$\mathcal{N}_{A\to W} = \left(1-\frac{q}{2}\right)|0\rangle\langle 0| + \frac{q}{2}\,|1\rangle\langle 1| + (1-2a)\Bigg(\left(\sqrt{\left(1-\frac{3q}{4}\right)\frac{q}{4}} - i\frac{q}{4}\right)|0\rangle\langle 1| + \left(\sqrt{\left(1-\frac{3q}{4}\right)\frac{q}{4}} + i\frac{q}{4}\right)|1\rangle\langle 0|\Bigg) \tag{54}$$

Substituting $\rho = |0\rangle\langle 0|$ and $\rho = |1\rangle\langle 1|$ into (54), respectively, yields:

$$\begin{aligned}\omega_0 &= \mathcal{N}_{A\to W}(|0\rangle\langle 0|)\\ &= \left(1-\frac{q}{2}\right)|0\rangle\langle 0| + \frac{q}{2}\,|1\rangle\langle 1| + \left(\sqrt{1-\frac{3q}{4}}\sqrt{\frac{q}{4}} + i\frac{q}{4}\right)|1\rangle\langle 0| + \left(\sqrt{1-\frac{3q}{4}}\sqrt{\frac{q}{4}} - i\frac{q}{4}\right)|0\rangle\langle 1|\ ,\end{aligned} \tag{55}$$

and

$$\begin{aligned}\omega_1 &= \mathcal{N}_{A\to W}(|1\rangle\langle 1|)\\ &= \left(1-\frac{q}{2}\right)|0\rangle\langle 0| + \frac{q}{2}\,|1\rangle\langle 1| - \left(\sqrt{1-\frac{3q}{4}}\sqrt{\frac{q}{4}} + i\frac{q}{4}\right)|1\rangle\langle 0| - \left(\sqrt{1-\frac{3q}{4}}\sqrt{\frac{q}{4}} - i\frac{q}{4}\right)|0\rangle\langle 1|\ .\end{aligned} \tag{56}$$

The determinant of both $\omega_0$ and $\omega_1$ is,

$$|\omega_0| = |\omega_1| = \frac{3q}{8}(2-q)\,. \tag{57}$$

Since the determinant is not equal to zero (for $0 < q < 1$), it follows that $\omega_0$ and $\omega_1$ span the entire qubit space, thus, in particular $\mathrm{supp}(\omega_1) \subseteq \mathrm{supp}(\omega_0)$.

## Appendix II
## Matrix Logarithms Estimation

### A. Approximation Tools

We provide the approximation tools that are used throughout the derivation, using the "big $\mathcal{O}$-notation" in Section II-A.

- Useful Taylor expansions (at $x = 0$):

$$\sqrt{a+bx+cx^2} = \sqrt{a} + \frac{b}{2\sqrt{a}}x + \mathcal{O}(x^2)\,, \tag{58}$$

$$\log\big(a+bx+cx^2\big) = \frac{\ln(a)}{\ln(2)} + \frac{b}{a\ln(2)}x - \frac{b^2-2ac}{a^2\ln(4)}x^2 + \mathcal{O}(x^3)\,, \tag{59}$$

$$\sqrt{x(1-x)} = \sqrt{x} + \mathcal{O}(x^{\frac{3}{2}})\,, \tag{60}$$

$$\frac{x}{\sqrt{x(1-x)}} = \sqrt{x} + \mathcal{O}(x^{\frac{3}{2}})\,, \tag{61}$$

$$\frac{1}{\sqrt{x(1-x)}} = \frac{1}{\sqrt{x}} + \mathcal{O}(\sqrt{x})\,, \tag{62}$$

$$\frac{1}{\sqrt{cx+1}} = 1 + \mathcal{O}(x)\,, \tag{63}$$
$$\frac{1}{\sqrt{\frac{c}{x}+1}} = \frac{1}{\sqrt{c}}\sqrt{x} + \mathcal{O}(x^{\frac{3}{2}})\,. \tag{64}$$

- The spectral decomposition of a Hermitian operator,

$$P = a\,|00\rangle\langle 00| + b\,|01\rangle\langle 01| + c\,|10\rangle\langle 10| + d\,|11\rangle\langle 11| + s(|00\rangle\langle 11| + |11\rangle\langle 00|) \tag{65}$$

consists of the eigenvalues

$$\begin{aligned} \lambda_1 &= \frac{1}{2}\left(a+d+\sqrt{(a+d)^2 - 4(ad-s^2)}\right), \\ \lambda_4 &= \frac{1}{2}\left(a+d-\sqrt{(a+d)^2 - 4(ad-s^2)}\right), \\ \lambda_2 &= b, \\ \lambda_3 &= c\,. \end{aligned} \tag{66}$$

and the associated eigenvectors,

$$\begin{aligned} |\lambda_1\rangle &= C_1\left(\widetilde{\lambda}_1\,|00\rangle + |11\rangle\right), \\ |\lambda_4\rangle &= C_4\left(\widetilde{\lambda}_4\,|00\rangle + |11\rangle\right), \\ |\lambda_2\rangle &= |01\rangle\,, \\ |\lambda_3\rangle &= |10\rangle\;. \end{aligned} \tag{67}$$

where

$$\widetilde{\lambda}_1 \equiv -\frac{a-\lambda_1}{s}\,, \tag{68}$$
$$\widetilde{\lambda}_4 \equiv -\frac{a-\lambda_4}{s}\,, \tag{69}$$
$$C_1 \equiv \frac{1}{\sqrt{\widetilde{\lambda}_1^2+1}}\,, \tag{70}$$
$$C_4 \equiv \frac{1}{\sqrt{\widetilde{\lambda}_4^2+1}}\,. \tag{71}$$

### *B. Output density operators*

The joint state $\psi_{A_1B}$ of the reference system and Bob's output is obtained by applying the depolarizing channel:

$$\begin{aligned} \psi_{A_1B} &= (\mathbb{1}_{A_1}\otimes\mathcal{N}_{A\to B})(\psi_{A_1A}) \\ &= \left(1-\frac{3}{4}q\right)\psi_{A_1A} + \frac{q}{4}[(\mathbb{1}_{A_1}\otimes X)\psi_{A_1A}(\mathbb{1}_{A_1}\otimes X) + (\mathbb{1}_{A_1}\otimes Y)\psi_{A_1A}(\mathbb{1}_{A_1}\otimes Y) \\ &\quad + (\mathbb{1}_{A_1}\otimes Z)\psi_{A_1A}(\mathbb{1}_{A_1}\otimes Z)]\,. \end{aligned} \tag{72}$$

Algebraic manipulations yield

$$\begin{aligned} \psi_{A_1B} = &\left(1-\frac{q}{2}\right)(1-\alpha)\,|00\rangle\langle 00| + \left(1-\frac{q}{2}\right)\alpha\,|11\rangle\langle 11| + \frac{q}{2}(1-\alpha)\,|01\rangle\langle 01| + \frac{q}{2}\alpha\,|10\rangle\langle 10| \\ &+ (1-q)\sqrt{\alpha}\sqrt{1-\alpha}(|00\rangle\langle 11| + |11\rangle\langle 00|)\,. \end{aligned} \tag{73}$$

The reduced matrices $\psi_{A_1}$ and $\psi_B$ are, thus,

$$\psi_B = \left[\left(1-\frac{q}{2}\right)*\alpha\right]|0\rangle\langle 0| + \left[\frac{q}{2}*\alpha\right]|1\rangle\langle 1|\;, \tag{74}$$
$$\psi_{A_1} = (1-\alpha)\,|0\rangle\langle 0| + \alpha\,|1\rangle\langle 1|\,, \tag{75}$$

where $\alpha * \beta = (1-\alpha)\beta + \alpha(1-\beta)$. Then,

$$\begin{aligned} \psi_{A_1}\otimes\psi_B = &(1-\alpha)\left[\left(1-\frac{q}{2}\right)*\alpha\right]|00\rangle\langle 00| + (1-\alpha)\left[\frac{q}{2}*\alpha\right]|01\rangle\langle 01| \\ &+ \alpha\left[\left(1-\frac{q}{2}\right)*\alpha\right]|10\rangle\langle 10| + \alpha\left[\frac{q}{2}*\alpha\right]|11\rangle\langle 11|\;. \end{aligned} \tag{76}$$

The logarithm of $\psi_{A_1} \otimes \psi_B$ can be computed directly as it is diagonal in the standard basis. This is not the case for $\psi_{A_1B}$. Using (66), the spectral decomposition consists of the following eigenvalues:

$$\begin{aligned}
\lambda_1 &= \frac{1}{2}\left(1 - \frac{q}{2} + \sqrt{\left[1-\frac{q}{2}\right]^2 - 4q\left[1-\frac{3q}{4}\right]\alpha + 4q\left[1-\frac{3q}{4}\right]\alpha^2}\right), \\
\lambda_4 &= \frac{1}{2}\left(1 - \frac{q}{2} - \sqrt{\left[1-\frac{q}{2}\right]^2 - 4q\left[1-\frac{3q}{4}\right]\alpha + 4q\left[1-\frac{3q}{4}\right]\alpha^2}\right), \\
\lambda_2 &= \frac{q}{2}(1-\alpha), \\
\lambda_3 &= \frac{q}{2}\alpha\,. \qquad (77)
\end{aligned}$$

Using the Taylor approximation in (58), we approximate $\lambda_1$ and $\lambda_4$ by

$$\begin{aligned}
\lambda_1 &= \frac{1}{2}\left(1 - \frac{q}{2} + \left(1-\frac{q}{2}\right) - \frac{4q\left(1-\frac{3}{4}q\right)}{2\left(1-\frac{q}{2}\right)}\alpha + \mathcal{O}(\alpha^2)\right), \\
\lambda_4 &= \frac{1}{2}\left(1 - \frac{q}{2} - \left(1-\frac{q}{2}\right) - \frac{4q\left(1-\frac{3}{4}q\right)}{2\left(1-\frac{q}{2}\right)}\alpha + \mathcal{O}(\alpha^2)\right). \qquad (78)
\end{aligned}$$

That is,

$$\lambda_1 = 1 - \frac{q}{2} - \frac{q\left(1-\frac{3}{4}q\right)}{\left(1-\frac{q}{2}\right)}\alpha + \mathcal{O}(\alpha^2)\,, \qquad (79)$$

$$\lambda_4 = \frac{q\left(1-\frac{3}{4}q\right)}{\left(1-\frac{q}{2}\right)}\alpha + \mathcal{O}(\alpha^2)\,. \qquad (80)$$

The eigenvectors of $\psi_{A_1B}$ are given in (67), with $\widetilde{\lambda}_1$ and $\widetilde{\lambda}_4$ satisfying

$$\widetilde{\lambda}_1 = \frac{q-2}{2(q-1)\sqrt{\alpha}} + \mathcal{O}(\sqrt{\alpha})\,, \qquad (81)$$

$$\widetilde{\lambda}_4 = -\frac{2(q-1)}{(q-2)}\sqrt{\alpha} + \mathcal{O}(\sqrt{\alpha}^{\frac{3}{2}})\,, \qquad (82)$$

by (62). and

$$C_1^2 = 4\frac{(q-1)^2}{(q-2)^2}\alpha + \mathcal{O}(\alpha^2)\,, \qquad (83)$$

$$C_4^2 = 1 + \mathcal{O}(\alpha)\,, \qquad (84)$$

by (64).

By applying (59), we approximate the logarithm of the eigenvalues as follows. For the joint state $\psi_{A_1B}$,

$$\log(\lambda_1) = \log\left(1-\frac{q}{2}\right) + \mathcal{O}(\alpha)\,, \qquad (85)$$

$$\log(\lambda_2) = \log\left(\frac{q}{2}\right) + \mathcal{O}(\alpha)\,, \qquad (86)$$

$$\log(\lambda_3) = \log\left(\frac{q}{2}\right) + \log(\alpha) + \mathcal{O}(\alpha^2)\,, \qquad (87)$$

$$\log(\lambda_4) = \log(C(q)) + \log(\alpha) + \mathcal{O}(\alpha^2)\,. \qquad (88)$$

As for the product state $\psi_{A_1} \otimes \psi_B$, we have

$$\log\Big((1-\alpha)\left[\left(1-\frac{q}{2}\right)*\alpha\right]\Big) = \log\left(1-\frac{q}{2}\right) + \mathcal{O}(\alpha)\,, \qquad (89)$$

$$\log\Big((1-\alpha)\left[\left(\frac{q}{2}\right)*\alpha\right]\Big) = \log\left(\frac{q}{2}\right) + \mathcal{O}(\alpha)\,, \qquad (90)$$

$$\log\Big((\alpha)\left[\left(1-\frac{q}{2}\right)*\alpha\right]\Big) = \log\left(1-\frac{q}{2}\right) + \log(\alpha) + \mathcal{O}(\alpha)\,, \qquad (91)$$

$$\log\Big((\alpha)\left[\left(\frac{q}{2}\right)*\alpha\right]\Big) = \log\left(\frac{q}{2}\right) + \log(\alpha). \qquad (92)$$

Hence, the operator-logarithm for $\psi_{A_1B}$ satisfies

$$\log(\psi_{A_1B}) = \log(\lambda_1)\,|\lambda_1\rangle\langle\lambda_1| + \log(\lambda_2)\,|\lambda_2\rangle\langle\lambda_2| + \log(\lambda_3)\,|\lambda_3\rangle\langle\lambda_3| + \log(\lambda_3 4)\,|\lambda_4\rangle\langle\lambda_4|$$

$$
\begin{aligned}
&= \left[\left(1-\frac{q}{2}\right)+\frac{4(q-1)^2}{(q-2)^2}\alpha\log(\alpha)\ +\mathcal{O}(\sqrt{\alpha})\right]|00\rangle\langle 00| \\
&\quad+\left[\log\left(\frac{q}{2}\right)+\mathcal{O}(\alpha)\right]|01\rangle\langle 01| \\
&\quad+\left(\log\left(\frac{q}{2}\right)+\log(\alpha)+\mathcal{O}(\alpha^2)\right)|10\rangle\langle 10| \\
&\quad+\left[\log(C(q))+\log(\alpha)+\mathcal{O}(\alpha\log(\alpha))\right]|11\rangle\langle 11| \\
&\quad+\left[-\frac{2(q-1)}{(q-2)}\sqrt{\alpha}\log(\alpha)+\mathcal{O}(\sqrt{\alpha})\right]|00\rangle\langle 11| \\
&\quad+\left[-\frac{2(q-1)}{(q-2)}\sqrt{\alpha}\log(\alpha)+\mathcal{O}(\sqrt{\alpha})\right]|11\rangle\langle 00|\ ,
\end{aligned} \tag{93}
$$

and for $\psi_{A_1}\otimes\psi_B$,

$$
\begin{aligned}
\log(\psi_{A_1}\otimes\psi_B) &= \left[\log\left(1-\frac{q}{2}\right)+\mathcal{O}(\alpha)\right]|00\rangle\langle 00| \\
&\quad+\left[\log\left(\frac{q}{2}\right)+\mathcal{O}(\alpha)\right]|01\rangle\langle 01| \\
&\quad+\left[\log\left(1-\frac{q}{2}\right)+\log(\alpha)+\mathcal{O}(\alpha)\right]|10\rangle\langle 10| \\
&\quad+\left[\log\left(\frac{q}{2}\right)+\log(\alpha)+\mathcal{O}(\alpha)\right]|11\rangle\langle 11|\ .
\end{aligned} \tag{94}
$$

## Appendix III
## Relative Entropy and Moments

In this section, we develop the approximations for the relative entropy $D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)$, and its second and fourth moments, $V(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)$ and $Q(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)$.

### *A. Relative Entropy*

Consider the relative entropy, $D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)$. By subtracting (94) from (93),

$$
\begin{aligned}
\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B) &= \left[\frac{4(q-1)^2}{(q-2)^2}\alpha\log(\alpha)+\mathcal{O}(\sqrt{\alpha})\right]|00\rangle\langle 00| \\
&\quad+\left[\mathcal{O}(\alpha)\right]|01\rangle\langle 01| \\
&\quad+\left[\log\left(\frac{q}{2}\right)-\log\left(1-\frac{q}{2}\right)+\mathcal{O}(\alpha)\right]|10\rangle\langle 10| \\
&\quad+\left[\log(C(q))-\log\left(\frac{q}{2}\right)+\mathcal{O}(\alpha\log(\alpha))\right]|11\rangle\langle 11| \\
&\quad+\left[-\frac{2(q-1)}{(q-2)}\sqrt{\alpha}\log(\alpha)+\mathcal{O}(\sqrt{\alpha})\right]|00\rangle\langle 11| \\
&\quad+\left[-\frac{2(q-1)}{(q-2)}\sqrt{\alpha}\log(\alpha)+\mathcal{O}(\sqrt{\alpha})\right]|11\rangle\langle 00|\ .
\end{aligned} \tag{95}
$$

Multiplying by $\psi_{A_1B}$, we have

$$
\begin{aligned}
\psi_{A_1B}[\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)] &= \left[\left(1-\frac{q}{2}\right)\frac{4(q-1)^2}{(q-2)^2}\alpha\log(\alpha)-2(1-q)\frac{2(q-1)}{(q-2)}\alpha\log(\alpha)+\mathcal{O}(\sqrt{\alpha})\right]|00\rangle\langle 00| \\
&\quad+\mathcal{O}(\alpha)\left(|01\rangle\langle 01|+|10\rangle\langle 10|+|11\rangle\langle 11|\right) \\
&\quad+\left[\mathcal{O}(\sqrt{\alpha}\log(\alpha))\right]|00\rangle\langle 11| \\
&\quad+\left[\mathcal{O}(\sqrt{\alpha}\log(\alpha))\right]|11\rangle\langle 00|\ .
\end{aligned} \tag{96}
$$

Applying the trace, we approximate the relative entropy:

$$
\begin{aligned}
D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) &= \mathrm{Tr}\left[\psi_{A_1B}\log(\psi_{A_1B})-\psi_{A_1B}\log(\psi_{A_1}\otimes\psi_B)\right] \\
&= \left[\left(1-\frac{q}{2}\right)\frac{4(q-1)^2}{(q-2)^2}-(1-q)\frac{2(q-1)}{(q-2)}\right]\alpha\log(\alpha)+\mathcal{O}(\alpha) \\
&= -2\frac{(1-q)^2}{2-q}\alpha\log(\alpha)+\mathcal{O}(\alpha)\,.
\end{aligned} \tag{97}
$$

### B. Second Moment

Next, we consider the second moment of the relative entropy. By squaring (95), we have:

$$\begin{aligned}|\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)|^2 = &\left[\frac{4(q-1)^2}{(q-2)^2}\alpha\log^2(\alpha)+\mathcal{O}(\alpha\log(\alpha))\right]|00\rangle\langle 00|\\ &+\left[\mathcal{O}(\alpha^2)\right]|01\rangle\langle 01|\\ &+\left[\left(\log\left(\frac{q}{2}\right)-\log\left(1-\frac{q}{2}\right)\right)^2+\mathcal{O}(\alpha)\right]|10\rangle\langle 10|\\ &+\left[\left(\log(C(q))-\log\left(\frac{q}{2}\right)\right)^2+\frac{4(q-1)^2}{(q-2)^2}\alpha\log^2(\alpha)+\mathcal{O}(\alpha\log(\alpha))\right]|11\rangle\langle 11|\\ &+\left[\mathcal{O}(\sqrt{\alpha}\log(\alpha))\right](|00\rangle\langle 11|+|11\rangle\langle 00|)\,. \end{aligned}\tag{98}$$

As we multiply by $\psi_{A_1B}$,

$$\begin{aligned}\psi_{A_1B}|\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)|^2 = &\left[\left(1-\frac{q}{2}\right)\frac{4(q-1)^2}{(q-2)^2}\alpha\log^2(\alpha)+\mathcal{O}(\alpha\log(\alpha))\right]|00\rangle\langle 00|\\ &+\left[\mathcal{O}(\alpha^2)\right]|01\rangle\langle 01|+\left[\mathcal{O}(\alpha)\right]|10\rangle\langle 10|\\ &+\left[\mathcal{O}(\alpha\log(\alpha))\right]|11\rangle\langle 11|\\ &+\left[\mathcal{O}(\sqrt{\alpha}\log(\alpha)\right](|00\rangle\langle 11|+|11\rangle\langle 00|)\,. \end{aligned}\tag{99}$$

Using (97) and applying the trace to the above, we obtain an approximation of the second moment:

$$\begin{aligned}V(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) &= \mathrm{Tr}\left[\psi_{A_1B}\left|\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)\right.\ -D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)\right|^2\Big]\\ &= \mathrm{Tr}\left[\psi_{A_1B}\left|\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)\right|^2\right]-2D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)\\ &\qquad\times\mathrm{Tr}\left[\psi_{A_1B}\left|\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)\right|\right]+D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)^2\\ &= \mathrm{Tr}\left[\psi_{A_1B}\left|\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)\right|^2\right]-D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)^2\\ &= \left(1-\frac{q}{2}\right)\frac{4(q-1)^2}{(q-2)^2}\alpha\log^2(\alpha)+\mathcal{O}(\alpha\log(\alpha))+\mathcal{O}(\alpha^2\log^2(\alpha))\\ &= \frac{2(q-1)^2}{q-2}\alpha\log^2(\alpha)+\mathcal{O}(\alpha\log(\alpha))\,. \end{aligned}\tag{100}$$

### C. Fourth Moment

Consider

$$Q(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)=\mathrm{Tr}\Big[\psi_{A_1B}\Big|\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)-D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)\Big|^4\Big]\,.\tag{101}$$

We use the binomial identity: $(X-c)^4=X^4-4cX^3+6c^2X^2-4c^3X+c^4$, for a Hermitian operator $X\in\mathcal{L}(\mathcal{H})$ and a real number $c$. Substituting $X=\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)$, and $c=D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)$, we obtain

$$\begin{aligned}Q(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) = &\ \mathrm{Tr}\left[\psi_{A_1B}\left(\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)\right)^4\right]\\ &-4D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)\times\mathrm{Tr}\left[\psi_{A_1B}\Big(\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B)\Big)^3\right]+\mathcal{O}(\alpha^3\log^4(\alpha))\,. \end{aligned}\tag{102}$$

Using (95) and (98),

$$\begin{aligned}(\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B))^4 = &\left[\mathcal{O}(\alpha\log^2(\alpha))\right]|00\rangle\langle 00|\\ &+\left[\mathcal{O}(\alpha^4)\right]|01\rangle\langle 01|\\ &+\left[\mathcal{O}(1)\right]|10\rangle\langle 10|\\ &+\left[\mathcal{O}(1)\right]|11\rangle\langle 11|\\ &+\left[\mathcal{O}(\sqrt{\alpha}\log(\alpha)\right]|00\rangle\langle 11|\\ &+\left[\mathcal{O}(\sqrt{\alpha}\log(\alpha)\right]|11\rangle\langle 00|\,, \end{aligned}\tag{103}$$

and

$$\begin{aligned}(\log(\psi_{A_1B})-\log(\psi_{A_1}\otimes\psi_B))^3 = &\left[\mathcal{O}(\alpha\log^2(\alpha))\right]|00\rangle\langle 00|\\ &+\left[\mathcal{O}(\alpha^3)\right]|01\rangle\langle 01| \end{aligned}$$

$$
\begin{aligned}
&+[\mathcal{O}(1)]\,|10\rangle\langle 10| + [\mathcal{O}(1)]\,|11\rangle\langle 11| \\
&+ \left[\mathcal{O}(\sqrt{\alpha}\log(\alpha)\right]\,|00\rangle\langle 11| \\
&+ \left[\mathcal{O}(\sqrt{\alpha}\log(\alpha)\right]\,|11\rangle\langle 00|\ .
\end{aligned} \tag{104}
$$

Multiplying by $\psi_{A_1B}$, we have

$$
\begin{aligned}
\psi_{A_1B}\left|(\log(\psi_{A_1B}) - \log(\psi_{A_1}\otimes\psi_B))^4\right| &= \left[\mathcal{O}(\alpha\log^2(\alpha))\right]\,|00\rangle\langle 00| \\
&+ \left[\mathcal{O}(\alpha^4)\right]\,|01\rangle\langle 01| \\
&+ [\mathcal{O}(\alpha)]\,(|10\rangle\langle 10| + |11\rangle\langle 11|) \\
&+ \left[\mathcal{O}(\sqrt{\alpha}\log(\alpha)\right]\,|00\rangle\langle 11| \\
&+ \left[\mathcal{O}(\sqrt{\alpha}\log(\alpha)\right]\,|11\rangle\langle 00|\ ,
\end{aligned} \tag{105}
$$

and

$$
\begin{aligned}
\psi_{A_1B}\left|(\log(\psi_{A_1B}) - \log(\psi_{A_1}\otimes\psi_B))^3\right| &= \left[\mathcal{O}(\alpha\log^2(\alpha))\right]\,|00\rangle\langle 00| \\
&+ \left[\mathcal{O}(\alpha^3)\right]\,|01\rangle\langle 01| \\
&+ [\mathcal{O}(\alpha)]\,(|10\rangle\langle 10| + |11\rangle\langle 11|) \\
&+ \left[\mathcal{O}(\sqrt{\alpha}\log(\alpha)\right]\,|00\rangle\langle 11| + |11\rangle\langle 00| \\
&+ \left[\mathcal{O}(\sqrt{\alpha}\log(\alpha)\right]\,|11\rangle\langle 00|\ .
\end{aligned} \tag{106}
$$

Finally, by tracing out, we obtain the order of the fourth moment:

$$
Q(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) = \mathcal{O}(\alpha\log^2(\alpha))\,. \tag{107}
$$

## Appendix IV
## Code size

We observe that when choosing $\alpha = \alpha_n = \frac{\gamma_n}{\sqrt{n}}$ with $\gamma_n = n^{\nu-\frac{1}{6}}$, we obtain the following approximation for the first term on the right-hand side of (23),

$$
\begin{aligned}
nD(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) &= -2\frac{(1-q)^2}{2-q}\sqrt{n}\gamma_n\log\left(\frac{\gamma_n}{\sqrt{n}}\right) + O(\sqrt{n}\gamma_n) \\
&= -2\frac{(1-q)^2}{2-q}n^{\nu+\frac{1}{3}}\log\left(n^{\nu-\frac{2}{3}}\right) + O(n^{\nu+\frac{1}{3}}) \\
&= 2\left(\frac{2}{3}-\nu\right)\frac{(1-q)^2}{2-q}n^{\nu+\frac{1}{3}}\log n + O(n^{\nu+\frac{1}{3}})\,.
\end{aligned} \tag{108}
$$

In a similar manner, we approximate the second term by

$$
\begin{aligned}
\sqrt{nV(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)} &= O\left(\sqrt{\sqrt{n}\gamma_n\log^2(n^{\nu-\frac{2}{3}})}\right) \\
&= O\left(\sqrt{n^{\nu+\frac{1}{3}}}\log n\right) \\
&= O\left(n^{\frac{\nu}{2}+\frac{1}{6}}\log n\right)\ .
\end{aligned} \tag{109}
$$

Finally, the last term (23) is $C_n$, as defined in (25). To show that this term vanishes, we write

$$
\begin{aligned}
\frac{[Q(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)]^{\frac{3}{4}}}{V(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)} &= O\left(\frac{\left(n^{\frac{\nu}{2}+\frac{1}{6}}\log n\right)^{\frac{3}{4}}}{n^{\frac{\nu}{2}+\frac{1}{6}}\log n}\right) \\
&= O\left(n^{-\frac{\nu}{8}-\frac{1}{6}}\log^{-\frac{1}{4}}(n)\right)
\end{aligned} \tag{110}
$$

which tends to zero as $n\to\infty$. Hence,

$$
\log(M) \geq 2\left(\frac{2}{3}-\nu\right)\frac{(1-q)^2}{2-q}n^{\nu+\frac{1}{3}}\log n + O(n^{\nu+\frac{1}{3}}) \tag{111}
$$

for every $0<\nu<\frac{1}{6}$.

# APPENDIX V
# ENERGY-CONSTRAINED CAPACITIES

We provide the proof for the energy-constrained capacity formula of the qubit depolarizing channel. Note that this model does not involve a covertness requirement.

## A. Unassisted Capacity

We begin with communication without assistance.

*Theorem* 6. Consider a qubit depolarizing channel $\mathcal{N}_{A\to B}$ as specified in Section II-B, and let $E \in [0,1]$. The energy-constrained capacity without entanglement assistance is given by

$$C_0(\mathcal{N},E) = \begin{cases} h_2\left(E * \frac{q}{2}\right) - h_2\left(\frac{q}{2}\right) & 0 < E < \frac{1}{2} \\ 1 - h_2\left(\frac{q}{2}\right) & \frac{1}{2} \leq E \leq 1, \end{cases} \tag{112}$$

where '$*$' denotes the binary convolution operation: $\alpha * \beta = (1-\alpha)\beta + \alpha(1-\beta)$.

*Proof.* Consider the general capacity characterization in (36). For $0 < E < \frac{1}{2}$, the direct part follows by choosing the ensemble $\{(1-E, E), |0\rangle, |1\rangle\}$, which results in the average input state

$$\widetilde{\rho}_A \equiv (1-E)\,|0\rangle\!\langle 0| + E\,|1\rangle\!\langle 1| \ . \tag{113}$$

Otherwise, if $E \geq \frac{1}{2}$, set the input ensemble to be uniform, i.e., $\left\{\left(\frac{1}{2},\frac{1}{2}\right), |0\rangle, |1\rangle\right\}$

We move to the converse part. For $E \geq \frac{1}{2}$, the converse part immediately follows from the capacity result without constraints. Hence, suppose that $0 < E < \frac{1}{2}$. For every input ensemble, the Holevo information functional, $I(X;B)_\rho$, is bounded as follows:

$$\begin{aligned} I(X;B)_\rho &= H(B)_\rho - H(B|X)_\rho \\ &\leq H(B)_\rho - H^{\min}(\mathcal{N}) \end{aligned} \tag{114}$$

where $H^{\min}(\mathcal{N})$ is the minimum output entropy, $H^{\min}(\mathcal{N}) \equiv \min_{\rho_A} H(\mathcal{N}(\rho_A))$. For the qubit depolarizing channel,

$$H^{\min}(\mathcal{N}) = h_2\left(\frac{q}{2}\right) \tag{115}$$

by [39, Sec. 20.4.4].

It remains to bound $H(B)_\rho$. Consider a general input state

$$\rho_A \equiv \begin{pmatrix} 1-a & b \\ b^* & a \end{pmatrix} \tag{116}$$

that satisfies the maximization constraint, $\mathrm{Tr}(\mathsf{F}\rho_A) \leq E$ (see (36)). The corresponding output state is

$$\rho_B \equiv \begin{pmatrix} (1-q)(1-a) + \frac{q}{2} & (1-q)b \\ (1-q)b^* & (1-q)a + \frac{q}{2} \end{pmatrix} . \tag{117}$$

The eigenvalues of $\rho_B$ are thus

$$\pi_\pm = \frac{1}{2}\left(1 \pm \sqrt{1 - 4\left(((1-q)(1-a) + \frac{q}{2})((1-q)a + \frac{q}{2})\right) + 4|b|^2}\right) . \tag{118}$$

Hence, the output entropy is

$$H(\rho_B) = -\pi_+ \log(\pi_+) - \pi_- \log(\pi_-) \,. \tag{119}$$

Notice that the eigenvalues $\pi_\pm$ do not depend on the phase of the off-diagonal entry, $b$, hence the entropies of $\rho_A$ and $Z\rho_A Z$ are the same. It thus follows that

$$H(\rho_B) = H(Z\rho_B Z) \tag{120}$$

with

$$Z\rho_B Z \equiv \begin{pmatrix} (1-q)(1-a) + \frac{q}{2} & -(1-q)b \\ -(1-q)b^* & (1-q)a + \frac{q}{2} \end{pmatrix} . \tag{121}$$

Since the entropy is concave, we have

$$\begin{aligned} H(\rho_B) &= \frac{1}{2}H(\rho_B) + \frac{1}{2}H(Z\rho_B Z) \\ &\leq H\left(\frac{1}{2}\rho_B + \frac{1}{2}Z\rho_B Z\right) \end{aligned}$$

$$= H\left(\left[(1-q)(1-a)+\frac{q}{2}\right]|0\rangle\langle 0| + \left[(1-q)a+\frac{q}{2}\right]|1\rangle\langle 1|\right)$$
$$= H\Big(\mathcal{N}_{A\to B}\left((1-a)\,|0\rangle\langle 0| + a\,|1\rangle\langle 1|\right)\Big). \tag{122}$$

Therefore, the maximal output entropy can be achieved with $b = 0$. i.e., for an input state of the form

$$\rho_A \equiv \begin{pmatrix} 1-a & 0 \\ 0 & a \end{pmatrix}. \tag{123}$$

Since the energy constraint requires $a \leq E$,

$$H(B)_\rho \leq \max_{0\leq a\leq E} H\Big(\mathcal{N}_{A\to B}\left((1-a)\,|0\rangle\langle 0| + a\,|1\rangle\langle 1|\right)\Big) \tag{124}$$
$$= \max_{0\leq a\leq E} h_2\Big(a * \frac{q}{2}\Big) \tag{125}$$
$$= h_2\Big(E * \frac{q}{2}\Big) \tag{126}$$

This completes the proof of Theorem 6. □

### B. Entanglement-Assisted Capacity

We move to the energy-constrained capacity of the qubit depolarizing channel, when Alice and Bob are provided with pre-shared entanglement.

*Theorem* 7. The energy-constrained entanglement-assisted capacity is given by

$$C_{\mathrm{EA}}(\mathcal{N}, E) = \begin{cases} h_2(E) + h_2\left(E * \frac{q}{2}\right) - H(\Psi_{A_1 B}) & 0 < E < \frac{1}{2} \\ 2 - H\left(1 - \frac{3q}{4}, \frac{q}{4}, \frac{q}{4}, \frac{q}{4}\right) & \frac{1}{2} \leq E \leq 1, \end{cases} \tag{127}$$

where $\Psi_{A_1 B} \equiv (\mathrm{id} \otimes \mathcal{N})(|\Psi_{A_1 A}\rangle\langle\Psi_{A_1 A}|)$.

*Proof.* Recall that the entanglement-assisted capacity of a general channel $\mathcal{N}_{A\to B}$ is given by 37. For the qubit depolarizing channel, we can restrict our attention to input states of the form $|\psi_{A_1 A}\rangle = \sqrt{1-a}\,|00\rangle + \sqrt{a}\,|11\rangle$, since the depolarizing channel is unitarily covariant (see [39, Section 24.8]). For $E < \frac{1}{2}$, the maximum is attained by the entangled state

$$|\Psi_{A_1 A}\rangle = \sqrt{1-E}\,|00\rangle + \sqrt{E}\,|11\rangle, \tag{128}$$

which is associated with an energy value $\mathrm{Tr}(\mathsf{F}\psi_A) = E$. Whereas, for $E \geq \frac{1}{2}$ the capacity is attained with $a = \frac{1}{2}$. This completes the proof of Theorem 7. □

## References


[1] M. Wang, T. Zhu, T. Zhang, J. Zhang, S. Yu, and W. Zhou, "Security and privacy in 6G networks: New areas and new challenges," *Digital Commun. Netw.*, vol. 6, no. 3, pp. 281–291, 2020.

[2] J. Talbot, D. Welsh, and D. J. A. Welsh, *Complexity and cryptography: An Introduction*. Cambridge University Press, 2006, vol. 13.

[3] M. Bloch and J. Barros, *Physical-layer Security: From Information Theory to Security engineering*. Cambridge University Press, 2011.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in *Proc. IEEE Int. Conf. Comp.*, 1984.

[5] R. Renner, "Security of quantum key distribution," *Int. J. Quantum Inf.*, vol. 6, no. 01, pp. 1–127, 2008.

[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, no. 3, p. 1301, 2009.

[7] M. Bloch, O. Günlü, A. Yener, F. Oggier, H. V. Poor, L. Sankar, and R. F. Schaefer, "An overview of information-theoretic security and privacy: Metrics, limits and applications," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 5–22, 2021.

[8] 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.

[9] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, "Hiding information in noise: Fundamental limits of covert wireless communication," *IEEE Commun. Mag.*, vol. 53, no. 12, pp. 26–31, 2015.

[10] M. Tahmasbi, A. Savard, and M. R. Bloch, "Covert capacity of non-coherent rayleigh-fading channels," *IEEE Trans. Inf. Theory*, vol. 66, no. 4, pp. 1979–2005, 2020.

[11] B. A. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1921–1930, 2013.

[12] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, 2016.
[13] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Trans. Inf. Theory*, vol. 62, no. 6, pp. 3493–3503, 2016.
[14] A. Sheikholeslami, B. A. Bash, D. Towsley, D. Goeckel, and S. Guha, "Covert communication over classical-quantum channels," in *Proc. IEEE Int. Symp. Inform. Theory (ISIT)*, Barcelona, Spain, Jul. 2016.
[15] M. S. Bullock, A. Sheikholeslami, M. Tahmasbi, R. C. Macdonald, S. Guha, and B. A. Bash, "Covert communication over classical-quantum channels," arXiv:1601.06826 [quant-ph], 2023.
[16] M. Tahmasbi and M. R. Bloch, "Framework for covert and secret key expansion over classical-quantum channels," *Phys. Rev. A*, vol. 99, no. 5, p. 052329, 2019.
[17] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, "Quantum-secure covert communication on bosonic channels," *Nat. commun.*, vol. 6, no. 1, pp. 1–9, 2015.
[18] M. S. Bullock, C. N. Gagatsos, S. Guha, and B. A. Bash, "Fundamental limits of quantum-secure covert communication over bosonic channels," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 3, pp. 471–482, 2020.
[19] C. N. Gagatsos, M. S. Bullock, and B. A. Bash, "Covert capacity of bosonic channels," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 2, pp. 555–567, 8 2020.
[20] S.-Y. Wang, T. Erdoğan, and M. Bloch, "Towards a characterization of the covert capacity of bosonic channels under trace distance," in *IEEE Int. Symp. Inf. Theory (ISIT)*, 2022, pp. 318–323.
[21] B. A. Bash, C. N. Gagatsos, A. Datta, and S. Guha, "Fundamental limits of quantum-secure covert optical sensing," in *IEEE Int. Symp. Inf. Theory (ISIT)*. IEEE, 2017, pp. 3210–3214.
[22] M. Tahmasbi and M. R. Bloch, "On covert quantum sensing and the benefits of entanglement," *IEEE J. Sel. Areas Inf. Theory*, vol. 2, no. 1, pp. 352–365, 2021.
[23] D. Deng, X. Li, S. Dang, M. C. Gursoy, and A. Nallanathan, "Covert communications in intelligent reflecting surface-assisted two-way relaying networks," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 11, pp. 12 380–12 385, 2022.
[24] H. ZivariFard, M. R. Bloch, and A. Nosratinia, "Covert communication in the presence of an uninformed, informed, and coordinated jammer," in *2022 IEEE International Symposium on Information Theory (ISIT)*, 2022, pp. 306–311.
[25] B. Yang, T. Taleb, G. Chen, and S. Shen, "Covert communication for cellular and x2u-enabled uav networks with active and passive wardens," *IEEE Network*, vol. 36, no. 1, pp. 166–173, 2022.
[26] B. Amihood and A. Cohen, "Covertly controlling a linear system," in *2022 IEEE Information Theory Workshop (ITW)*, 2022, pp. 321–326.
[27] M. Hayashi and A. Vazquez-Castro, "Covert communication with gaussian noise: from random access channel to point-to-point channel," *arXiv preprint arXiv:2310.15519*, 2023.
[28] A. Bounhar, M. Sarkiss, and M. Wigger, "Mixing a covert and a non-covert user," *arXiv preprint arXiv:2305.06268*, 2023.
[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, 1999.
[30] ——, "Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem," *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2637–2655, 2002.
[31] S. Hao, H. Shi, W. Li, J. H. Shapiro, Q. Zhuang, and Z. Zhang, "Entanglement-assisted communication surpassing the ultimate classical capacity," *Phys. Rev. Lett.*, vol. 126, no. 25, p. 250501, 2021.
[32] A. Chiuri, S. Giacomini, C. Macchiavello, and P. Mataloni, "Experimental achievement of the entanglement-assisted capacity for the depolarizing channel," *Phys. Rev. A*, vol. 87, no. 2, p. 022333, 2013.
[33] U. Pereg, C. Deppe, and H. Boche, "Quantum channel state masking," *IEEE Trans. Inf. Theory*, vol. 67, no. 4, pp. 2245–2268, 2021.
[34] S.-Y. Wang, S.-J. Su, and M. Bloch, "Resource-efficient entanglement-assisted covert communications over bosonic channels," *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2024.
[35] A. Chiuri, S. Giacomini, C. Macchiavello, and P. Mataloni, "Experimental achievement of the entanglement-assisted capacity for the depolarizing channel," *Phys. Rev. A*, vol. 87, no. 2, p. 022333, 2013.
[36] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell *et al.*, "Quantum supremacy using a programmable superconducting processor," *Nature*, vol. 574, no. 7779, pp. 505–510, 2019.
[37] C. King, "The capacity of the quantum depolarizing channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 221–229, 2003.
[38] D. Leung and J. Watrous, "On the complementary quantum capacity of the depolarizing channel," *Quantum*, vol. 1, 10 2015.
[39] M. M. Wilde, *Quantum information theory*, 2nd ed. Cambridge University Press, 2017.
[40] U. Pereg, C. Deppe, and H. Boche, "Communication with unreliable entanglement assistance," *Preprint available on arXiv:2112.09227. Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, pp. 2231–2236, 2022.
[41] M. Tomamichel, *Quantum information processing with finite resources: mathematical foundations*. Springer, 2015, vol. 5.

[42] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*. MIT press, 2022.
[43] D. Kretschmann, D. Schlingemann, and R. F. Werner, "The information-disturbance tradeoff and the continuity of stinespring's representation," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1708–1717, 2008.
[44] M. J. Salariseddigh, U. Pereg, H. Boche, and C. Deppe, "Deterministic identification over fading channels," in *IEEE Inf. Theory Workshop (ITW)*, 2021, pp. 1–5.
[45] M. J. Salariseddigh, U. Pereg, H. Boche, C. Deppe, V. Jamali, and R. Schober, "Deterministic identification for molecular communications over the poisson channel," *arXiv:2203.02784*, 2022.
[46] R. Ahlswede and G. Dueck, "Identification via channels," *IEEE Trans. Inf. Theory*, vol. 35, pp. 15–29, 1989.
[47] S. Khabbazi Oskouei, S. Mancini, and M. M. Wilde, "Union bound for quantum information processing," *Proc. Royal Soc. A*, vol. 475, no. 2221, p. 20180612, 2019.
[48] M. M. Wilde, "Position-based coding and convex splitting for private communication over quantum channels," *Quantum Inf. Proc.*, vol. 16, no. 10, p. 264, 2017.
[49] A. S. Holevo, "Entanglement-assisted capacity of constrained channels," in *1st Int. Symp. Quantum Info.*, vol. 5128. SPIE, 2003, pp. 62–69.
[50] S. Guha, Q. Zhuang, and B. A. Bash, "Infinite-fold enhancement in communications capacity using pre-shared entanglement," in *IEEE Int. Symp. Inf. Theory (ISIT)*, 2020, pp. 1835–1839.
[51] H. Shi, Z. Zhang, and Q. Zhuang, "Practical route to entanglement-assisted communication over noisy bosonic channels," *Phys. Rev. App.*, vol. 13, no. 3, mar 2020.
[52] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, "Capacities of quantum erasure channels," *Phys. Rev. Lett.*, vol. 78, no. 16, p. 3217, 1997.