# 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 not only the information is kept secret, but 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.**

## I. Introduction

Privacy and confidentiality are critical in communication systems [1]. The traditional security approaches (s.t., encryption [2], information-theoretic secrecy [3], and quantum key distribution [4, 5]) ensure that an eavesdropper is unable to recover any transmitted information. However, privacy and safety concerns may further require *covertness* [6, 7]. Covertness is a stronger requirement than traditional security: not only is the transmitted information kept secret, but also the transmission itself is concealed from detection by an adversary (a warden) [8, 9]. Despite the severity of limitations imposed by covertness, it is possible to communicate $O(\sqrt{n})$ bits information both reliably and covertly over $n$ classical channel uses [10–12]. 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 [13–15], as well as continuous-variable bosonic channels [16–18]. Covert sensing is also governed by an SRL [19].

Proving the achievability of the SRLs discovered so far involves the following principles. In the finite-dimensional case, both classical and quantum [11–15], a symbol (say, 0) in the input alphabet is designated as "innocent." Random coding is employed such that a non-innocent symbol is transmitted with probability $\sim 1/\sqrt{n}$ to ensure covertness. On the other hand, innocent symbol corresponding to zero transmitted power occurs naturally in the continuous-variable covert communication over classical additive white Gaussian noise (AWGN) [10–12] and classical-quantum bosonic [16–18] 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 [20–22]. Gagatsos et al. [17] 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. As in the unassisted setting, the transmission is limited to $O(1/\sqrt{n})$ mean photon number. However, in some communication settings, the coding scale is larger for continuous-variable channels [23]. So far, it has remained open whether such a performance boost can be achieved in covert communication over finite-dimensional quantum channels.

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 depolarizing channel is a fundamental model that has gained attention in both experimental [24] and theoretical [25] research. Depolarization may be regarded as the worst type of noise in a quantum system, and the insights on the depolarizing channel are often useful in the derivation of results for a general quantum channel [26, Sec. 11.9.1] [20]. 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 [27]. 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 [13, 14].

The paper is organized as follows. In Section II, the definitions and channel model are provided. The results are presented in Section III, which begins with a description of the solution principle, followed by the achievability proof, with technical details deferred to the appendices. Section IV presents a summary and discussion.

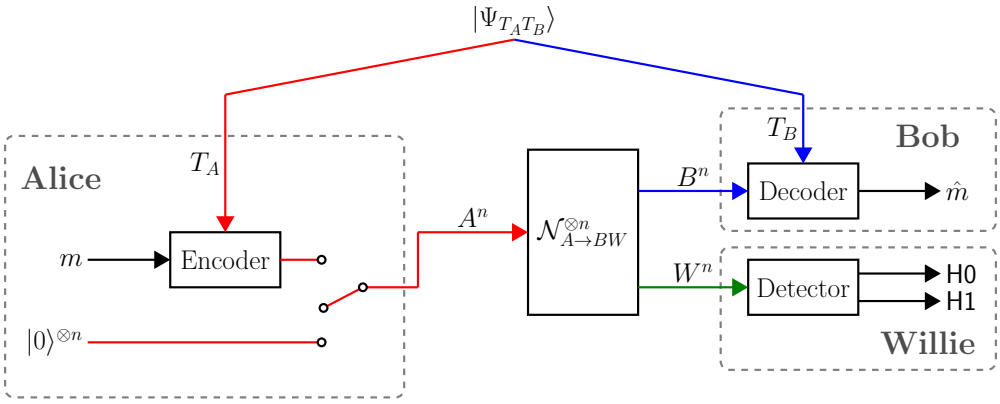


Fig. 1. Entanglement-assisted coding for covert communication over a quantum channel $\mathcal{N}_{A\to BW}$.

## II. Definitions and Channel Model

We use standard notation in quantum information processing, as, e.g., in [28, 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 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 [19]:

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

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.

We use the standard asymptotic notation $f(n)=O(g(n))$ for an asymptotic upper bound, i.e., there exist constants $m,n_0>0$ such that $0\leq f(n)\leq mg(n)$, for all $n\geq n_0$.

### A. 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 $\mathcal{N}_{A\to BW}^{\otimes n}(\rho_{A^n})$.

The depolarizing channel is a natural model for noise in quantum systems [20, 25]. The qubit depolarizing channel 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:

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

where $0<q<1$, with $\dim(\mathcal{H}_A)=\dim(\mathcal{H}_B)=2$. Here, we investigate covert communication over a depolarizing channel $\mathcal{V}_{A\to BE_1E_2}$ given by the Stinespring dilation: $\mathcal{V}_{A\to BE_1E_2}(\rho_A)=V\rho_A V^\dagger$, where $V:\mathcal{H}_A\to\mathcal{H}_B\otimes\mathcal{H}_{E_1}\otimes\mathcal{H}_{E_2}$ is the isometry [25]

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

We consider three cases:

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

Scenario 1 is 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. We note that the no-cloning theorem prohibits Willie from receiving a copy of Bob's output state.

*Remark* 1. In the boundary case of $q=0$, Bob receives the qubit state as is, while Willie obtains no information. If $q=1$, it is the other way around. Covert communication is trivial in the former case, and impossible in the latter.

### B. Entanglement-assisted Code

The definition of a code for covert communication over a quantum channel with entanglement assistance is given below. 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 $\mathcal{D}_{B^n T_B} = \{D_m\}_{m=1}^M$.

The communication setting is depicted in Figure 1. Suppose that Alice and Bob share the entangled state $\Psi_{T_A T_B}$, 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 $\rho^{(m)}_{A^n T_B} = (\mathcal{F}^{(m)}_{T_A^n \to A^n} \otimes \mathbb{1}_{T_B})(\Psi_{T_A T_B})$.

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 $\rho^{(m)}_{A^n T_B}$ occupying systems $A^n$ through $n$ uses of the covert communication channel $\mathcal{N}_{A \to BW}$. The joint output state is $\rho^{(m)}_{B^n W^n T_B} = \left(\mathcal{N}^{\otimes n}_{A \to BW} \otimes \mathrm{id}_{T_B}\right)\left(\rho^{(m)}_{A^n T_B}\right)$. Bob decodes the message from the reduced state $\rho^{(m)}_{B^n T_B}$ by applying the POVM $\mathcal{D}_{B^n T_B}$.

### C. Reliability and Covertness

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

$$P_e^{(n)}(\Psi, \mathcal{F}, \mathcal{D}) = \frac{1}{M} \sum_{m=1}^{M} \mathrm{Tr}\left[(\mathbb{1} - D_m)\rho^{(m)}_{B^n T_B}\right]. \quad (5)$$

Willie does not have access to Alice and Bob's entanglement resource and receives the reduced output state $\rho^{(m)}_{W^n} = \mathrm{Tr}_{B^n T_B}\left[\rho^{(m)}_{B^n W^n T_B}\right]$ 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 $P_{\text{FA}} = P(\text{choose } \mathsf{H1} | \mathsf{H0} \text{ is true})$ and $P_{\text{MD}} = P(\text{choose } \mathsf{H0} | \mathsf{H1} \text{ is true})$, respectively, and assuming equally likely hypotheses, Willie's average probability of error is $E^{(n)} = \frac{P_{\text{FA}} + P_{\text{MD}}}{2}$. 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 $\overline{\rho}_{W^n} = \frac{1}{M}\sum_{m=1}^{M} \rho^{(m)}_{W^n}$. A sufficient condition [13, 14] 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

$$P_e^{(n)}(\Psi, \mathcal{F}, \mathcal{D}) \leq \varepsilon\,, \text{ and } \; D(\overline{\rho}_{W^n} || \omega_0^{\otimes n}) \leq \delta\,. \quad (6)$$

### D. 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, $R = 0$, 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 [17]:

$$L = \frac{\log(M)}{\log(n)\sqrt{nD(\overline{\rho}_{W^n} || \omega_0^{\otimes n})}}. \quad (7)$$

*Definition* 1. A covert rate $L > 0$ is achievable with entanglement assistance if for every $\varepsilon, \delta > 0$, and sufficiently large $n$, there exists a $(2^{L \cdot \sqrt{\delta n}\log(n)}, n, \varepsilon, \delta)$ code. 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 $\alpha \in [0, 1]$:

$$\varphi_\alpha \equiv (1 - \alpha)\,|0\rangle\langle 0| + \alpha\,|1\rangle\langle 1|\,. \quad (8)$$

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 $\frac{n^{1/6}}{\log n} \cdot \gamma_n \to +\infty$. Choosing $\alpha = \alpha_n$ where

$$\alpha_n \equiv \frac{\gamma_n}{\sqrt{n}} \quad (9)$$

ensures covertness [13, 14]. 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 (6) is satisfied for large $n$.

## III. Results

We address the three scenarios presented in Section II-A. First, we consider the extreme cases of Scenario 1 and Scenario 2, where covertness is either impossible or trivial to achieve. We begin with Scenario 1, where Willie has access to the entire environment.

*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.* 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 $\mathrm{supp}(\omega_1) \not\subseteq \mathrm{supp}(\omega_0)$. We show this in detail in [29]. 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 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 information as without the covertness requirement, and send $O(n)$ bits.

*Proof.* If $W = E_2$, then Willie receives $\omega_0 = \omega_1 = (1 - \frac{q}{2})\,|0\rangle\langle 0| + \frac{q}{2}\,|1\rangle\langle 1|$ (see [29]). 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 $C_{\text{cov-EA}}(\mathcal{N})$ of a depolarizing channel. From

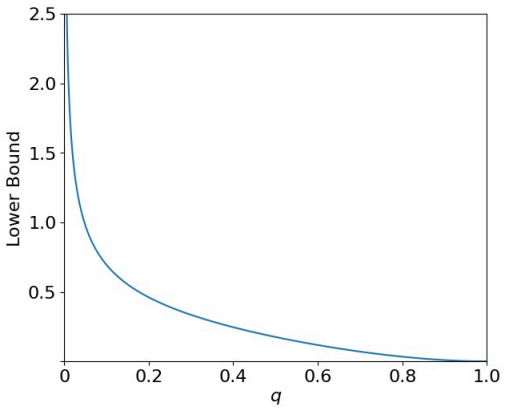


Fig. 2. Lower bound in Scenario 3 (see Section II-A).

this point on, we focus on Scenario 3, where Willie receives the first qubit of the environment (see Section II-A).

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

$$C_{\text{cov-EA}}(\mathcal{N}) \geq \frac{4\sqrt{2}}{3}\frac{(1-q)^2}{(2-q)\sqrt{\eta(\omega_1||\omega_0)}} \tag{10}$$

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 as 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 1). For $q = 0$, we have $C_{\text{cov-EA}}(\mathcal{N}) = +\infty$ in the $\sqrt{n}\log(n)$ scale, because the warden is degenerate and Alice can transmit a linear number of information bits. Whereas, for $q = 1$, the capacity is zero.

Following the definitions in Section II-D, a bound of the form $C_{\text{cov-EA}}(\mathcal{N}) \geq L_0$ implies that it is possible to transmit $L_0\sqrt{\delta n}\log(n)$ information bits reliably and covertly (see Definition 1). Recall that without entanglement assistance, covert communication requirements limit the message to $O(\sqrt{n})$ information bits [13, 14]. Thereby, we have established that entanglement assistance increases the message scale, from $O(\sqrt{n})$ to $O(\sqrt{n}\log(n))$ information bits. A similar result has been shown for continuous-variable bosonic channels [17]. 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* 2. In some communication settings, the coding scale is larger for continuous-variable channels. For example, in deterministic identification, the code size is super-exponential for Gaussian channels, whereas only exponential for finite-dimensional channels [23]. Nevertheless, we show here that in covert communication, the $\log(n)$ performance boost is not reserved to continuous variable systems.

### A. Proof Idea

We begin with the proof idea. Consider Scenario 3 as presented in Section II-A. First, we identify an entangled state that meets the above condition for covertness. As opposed to previous work, 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 gurantee 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 modify the approach in [17] to analyze the order of the number of covert information bits. The lemma below provides an achievability result for the transmission over a memoryless quantum channel, regardless of covertness. The derivation is based on 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 [17, 30].

We introduce additional notation for the moments of the quantum relative entropy. For every $\rho, \sigma \in \mathscr{S}(\mathcal{H})$, define

$$V(\rho||\sigma) = \text{Tr}[\rho|(\log(\rho) - \log(\sigma) - D(\rho||\sigma)|^2], \tag{11}$$
$$Q(\rho||\sigma) = \text{Tr}[\rho|(\log(\rho) - \log(\sigma) - D(\rho||\sigma)|^4]. \tag{12}$$

*Lemma* 4 (see [17, Lemma 1]). Consider a memoryless quantum channel $\mathcal{N}_{A\to B}$. For every $|\psi_{A_1A}\rangle$, arbitrary $\varepsilon > 0$, and sufficiently large $n$, there exists a coding scheme that employs pre-shared entanglement to transmit $\log(M)$ bits over $n$ uses of $\mathcal{N}_{A\to B}$ with decoding error probability $\varepsilon$ such that:

$$\log(M) \geq nD(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) + \sqrt{nV(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)}\Phi^{-1}(\varepsilon) - C_n \tag{13}$$

with

$$\psi_{A_1B} = (\text{id}_{A_1}\otimes\mathcal{N}_{A\to B})(\psi_{A_1A}) \tag{14}$$

and

$$C_n = \frac{\beta_{\text{B-E}}}{\sqrt{2\pi}}\frac{[Q(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)]^{\frac{3}{4}}}{V(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)} + \frac{V(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B)}{\sqrt{2\pi}} + \log(4\varepsilon n) \tag{15}$$

where $\beta_{\text{B-E}}$ is the *Berry-Esseen* constant and $\Phi^{-1}(x)$ is the inverse-Gaussian distribution function.

### B. Analysis

We present the main stages of the proof for Theorem 3, while the technical details are deferred to [29].

*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

$$\log(M) \geq 2\left(\frac{2}{3}-\nu\right)\frac{(1-q)^2}{2-q}\gamma_n\sqrt{n}\log(n) + O(\sqrt{n}\gamma_n). \tag{16}$$

*Proof.* To show achievability, we apply Lemma 4 with $|\psi_{A_1A}\rangle$ as in (1), with a parameter $\alpha = \alpha_n$ as in (9). Note that setting $\gamma_n = n^{\nu-\frac{1}{6}}$ as in the lemma statement yields

$$\alpha_n = \frac{\gamma_n}{\sqrt{n}} = n^{\nu-\frac{2}{3}}. \tag{17}$$

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 $\psi_A \equiv \mathrm{Tr}_{A_1}\left[|\psi_{A_1A}\rangle\langle\psi_{A_1A}|\right] = \varphi_{\alpha_n}$, with $\varphi_{\alpha_n}$ as in (8). That is, the reduced input state fits the achievability proof for the unassisted covert capacity in [13, 14], 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.

Having established both reliability and covertness, it remains to estimate the code size. Consider the joint state $\psi_{A_1B}$ of the output system $B$ and the reference system $A_1$, as in (14). In order to estimate each term on the right-hand side of (13), we first derive expressions for the operator logarithms, $\log(\psi_{A_1B})$ and $\log(\psi_{A_1} \otimes \psi_B)$, and then approximate the relative entropy and its moments.

The full technical details are given [29] (see appendices therein). We analyze the spectral decompositions and the Taylor expansions near $\alpha = 0$ [29, App. A]. Throughout the derivation, we maintain the exact value of the dominant terms and reduce the approximation error to its order class. We estimate the quantum relative entropy and its moments, and show that

$$\begin{aligned} D(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) &= -2\frac{(1-q)^2}{2-q}\alpha_n\log(\alpha_n) + O(\alpha_n)\,, \\ V(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) &= O(\alpha_n\log^2(\alpha_n))\,, \\ Q(\psi_{A_1B}||\psi_{A_1}\otimes\psi_B) &= O(\alpha_n\log^2(\alpha_n))\,, \end{aligned} \tag{18}$$

for $\alpha = \alpha_n$ as chosen above (see (17)) [29, App. B]. The proof is concluded by placing the approximations above into (13). The details are given in [29, App. C]. □

We are now ready for the proof outline of Theorem 3.

*Proof Outline for Theorem 3.* First, we observe that $\mathrm{supp}(\omega_1) \subseteq \mathrm{supp}(\omega_0)$ (see derivation in [29]), 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:

$$L_n = \frac{2\left(\frac{2}{3}-\nu\right)\frac{(1-q)^2}{2-q}\gamma_n + O\left(\frac{\gamma_n}{\log(n)}\right)}{\sqrt{D(\overline{\rho}_{W^n}||\omega_0^{\otimes n})}}\,. \tag{19}$$

As seen in the proof of Lemma 5, covertness is guaranteed by [13, 14]. Furthermore, the following property extends as well: there exists $\zeta > 0$ such that,

$$|D(\overline{\rho}_{W^n}||\omega_0^{\otimes n}) - nD(\omega_{\alpha_n}||\omega_0)| \leq e^{-\zeta\gamma_n^{\frac{3}{2}}n^{\frac{1}{4}}}\,, \tag{20}$$

where $\overline{\rho}_{W^n}$ is Willie's actual output state, the state $\omega_0 = \mathcal{N}_{A\to W}(|0\rangle\langle 0|)$ corresponds to the innocent input, and $\omega_{\alpha_n} \equiv \mathcal{N}_{A\to W}(\varphi_{\alpha_n})$, with $\varphi_{\alpha_n}$ as in (8). Based on a result that was recently developed for covert sensing [19, Lemma 5],

$$D(\omega_{\alpha_n}||\omega_0) = \frac{\alpha_n^2}{2}\eta(\omega_1||\omega_0) + O(\alpha_n^3) \tag{21}$$

for sufficiently small $\alpha_n$. Thus, by (20) and (21),

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

By applying this bound to the denominator in (19), we have:

$$L_n \geq \frac{2\left(\frac{2}{3}-\nu\right)\frac{(1-q)^2}{2-q}\gamma_n + O\left(\frac{\gamma_n}{\log(n)}\right)}{\sqrt{\frac{\gamma_n^2}{2}\eta(\omega_1||\omega_0) + e^{-\zeta\gamma_n^{\frac{3}{2}}n^{\frac{1}{4}}} + O\left(\frac{\gamma_n^3}{\sqrt{n}}\right)}}\,. \tag{22}$$

Hence, taking the limit of $n \to \infty$ completes the proof. □

## IV. Summary and Discussion

We study 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 detect any 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 $O(\sqrt{n})$ without entanglement assistance.

The square root law was derived for the non-trivial scenario, in which Bob cannot determine with certainty if the transmission is non-innocent. If Bob has this capability, then the scaling law becomes $O(\sqrt{n}\log n)$, even for a classical channel [13]. Therefore, it appears that entanglement assistance has a similar effect as granting Bob the capability of identifying a non-innocent transmission with certainty.

We provide the following interpretation, for both the Gaussian bosonic channel and the qubit depolarizing channel. 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 [31]. 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. Based on our derivation, a similar phenomenon is observed for the qubit depolarizing channel.


## Acknowledgment

This work was supported by the VATAT Program for Quantum Science and Technology through Grant n. 86636903 (Pereg, Zlotnick), and by the NSF grant CCF-2045530 (Bash). U. Pereg was also supported by the Chaya Chair n. 8776026. The authors thank Johannes Rosenberger (TUM) and the anonymous reviewers for useful remarks.

## 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] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, 2016.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] ——, "Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem," *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2637–2655, 2002.

[22] U. Pereg, C. Deppe, and H. Boche, "Quantum channel state masking," *IEEE Trans. Inf. Theory*, vol. 67, no. 4, pp. 2245–2268, 2021.

[23] 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.

[24] 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.

[25] D. Leung and J. Watrous, "On the complementary quantum capacity of the depolarizing channel," *Quantum*, vol. 1, 10 2015.

[26] M. M. Wilde, *Quantum information theory*, 2nd ed. Cambridge University Press, 2017.

[27] U. Pereg, C. Deppe, and H. Boche, "Communication with unreliable entanglement assistance," *IEEE Trans. Inf. Theory*, 2023.

[28] M. Tomamichel, *Quantum information processing with finite resources: mathematical foundations*. Springer, 2015, vol. 5.

[29] E. Zlotnick, B. Bash, and U. Pereg, "Entanglement-assisted covert communication via the qubit depolarizing channel," *arXiv preprint arXiv:2305.05477*, 2023. [Online]. Available: https://arxiv.org/pdf/2305.05477.pdf

[30] 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.

[31] A. S. Holevo, "Entanglement-assisted capacity of constrained channels," in *1st Int. Symp. Quantum Info.*, vol. 5128. SPIE, 2003, pp. 62–69.