Covert Entanglement Generation and Secrecy

Ohad Kimelfeld[*§], Boulat A. Bash[†] and Uzi Pereg[‡§]

[*] Physics Department, Technion Israel Institute of Technology, Haifa, Israel
[†] Electrical and Computer Engineering Department, University of Arizona, Tucson, AZ, USA
[‡] Electrical and Computer Engineering Department, Technion, Haifa, Israel
[§] Helen Diller Quantum Center, Technion, Haifa, Israel

***Abstract*—We determine the covert capacity for entanglement generation over a noisy quantum channel. While secrecy guarantees that the transmitted information remains inaccessible to an adversary, covert communication ensures that the transmission itself remains undetectable. The entanglement dimension follows a square root law (SRL) in the covert setting, i.e., $O(\sqrt{n})$ Einstein-Podolsky-Rosen (EPR) pairs can be distributed covertly and reliably over n channel uses. We begin with covert communication of classical information under a secrecy constraint. We then leverage this result to construct a coding scheme for covert entanglement generation. Single-letter expressions are derived for both the covert secrecy and the covert entanglement-generation capacities.**

I. Introduction

Privacy is a fundamental aspect of communication systems [1–11]. Traditional security approaches deny eavesdropper access to the transmitted information [12]. Covert communication prevents the detection of transmitted signals by masking them in noise. Although this strengthens security, its cost is the *square root law* (SRL): only $O(\sqrt{n})$ reliable and covert bits can be transmitted in n channel uses [13–24]. While secrecy and covertness seem orthogonal, their combination is considered for classical channels in [17, Sec. VII-C]. Tutorial on covert communication [25] and a recent survey [26] are available.

Recently, there has been a growing interest in how pre-shared entanglement resources can boost communication performance in general [27–35], and covert communication in particular [36–38]. In several channel models, entanglement assistance enables transmission on the order of $O(\sqrt{n}\log n)$ information bits [39–41]. This highlights the significance of covert entanglement generation. Entanglement generation is closely related to quantum subspace transmission [42–44], i.e., sending quantum information. Anderson et al. [45, 46] have recently developed lower bounds on the quantum covert rate using twirl modulation and depolarizing channel codes. Here, we give a more refined characterization and determine the capacity for covert entanglement generation in terms of the channel itself. Moreover, while Anderson et al. [46] use a pre-shared classical secret key of size $\sim \sqrt{n}\log n$ bits, our scheme does not require a pre-shared secret key.

Furthermore, entanglement generation is intimately related to secrecy [47, 48]. Due to the no-cloning theorem, quantum information transmission inherently ensures secrecy [49]. If the adversary could obtain the quantum information that Alice is sending to Bob, then Bob could not recover it without contradicting the no-cloning theorem. Devetak [44] introduced a coherent version of classical secrecy codes, which leverage their privacy properties to define subspaces where Alice can securely encode quantum information. The decoupling approach [50, 51] uses similar idea. In this sense, secrecy is both necessary and sufficient to establish entanglement generation.

Consider a covert entanglement generation setting, as in Figure 1. Alice first decides whether to transmit, or not. When inactive, the channel input is $|0\rangle^{\otimes n}$. Otherwise, she prepares a maximally entangled state Φ_{RM} locally, and encodes her "quantum message" M. She then transmits the encoded system A^n using n channel uses. At the channel output, Bob and Willie receive B^n and W^n, respectively. Bob performs a decoding operation which recovers a state that is close to $\Phi_{R\widehat{M}}$. Meanwhile, Willie performs a hypothesis test to detect whether Alice has transmitted information or not.

Our approach is fundamentally different from that in Anderson et al. [45, 46]. First, we consider both covert and secret communication of classical information via a classical-quantum (c-q) channel, and determine the covert secrecy capacity. This generalizes Bloch's result [17, Sec. VII-C] to c-q channels. One might argue that, with covertness, secrecy is redundant, as Willie would not attempt to decode a message he does not detect. However, covertness is typically defined in a statistical sense: while the probability of detection is small, it is not necessarily zero. Thus, in rare cases when Willie detects anomalous activity, secrecy ensures that he still cannot extract meaningful information. Covert secrecy is thus a problem of independent interest, not merely an auxiliary result for the main derivation. Then, we use Devetak's approach [44, Sec. IV] of constructing an entanglement-generation code from a secrecy code. This uses secrecy to establish entanglement generation. As a result, we achieve the same covert entanglement-generation rate as the secret classical information rate. Unlike Anderson et al. [46], our scheme does not require a pre-shared secret key.

We prove that approximately $C_{\text{EG}}\sqrt{n}$ EPR pairs can be generated covertly. The optimal rate C_{EG}, i.e., the covert capacity for entanglement generation, is given by

$$C_{\text{EG}} = \frac{\left[D\left(\sigma_1||\sigma_0\right) - D\left(\omega_1||\omega_0\right)\right]_+}{\sqrt{\frac{1}{2}\chi^2\left(\omega_1||\omega_0\right)}}, \tag{1}$$

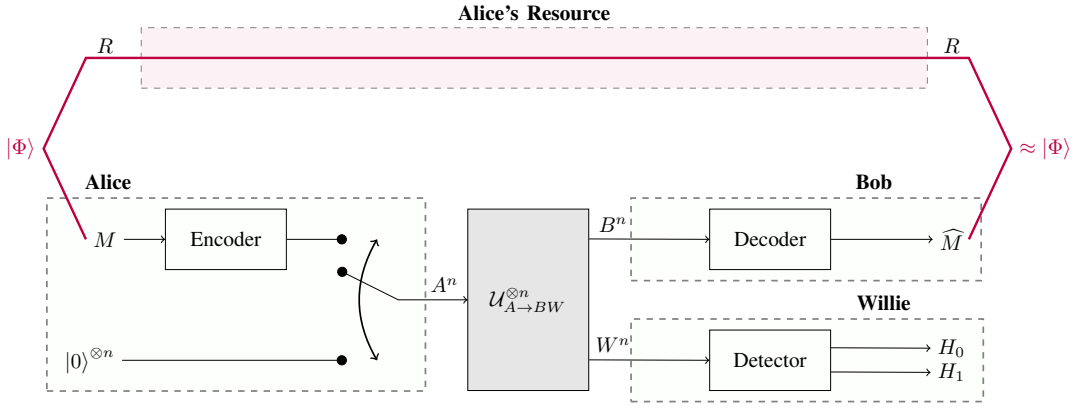

Fig. 1. Covert entanglement generation. Alice prepares $|\Phi\rangle_{RM}$, locally. If inactive, the channel input is $|0\rangle^{\otimes n}$. Otherwise, she encodes and transmits A^n via the quantum channel. Bob receives B^n, and produces $\widehat{M}$. In order to detect the transmission, Willie performs a measurement on W^n to estimate whether Alice is quiet (null hypothesis H_0) or transmitting (alternate hypothesis H_1).

where $[t]_+ \equiv \max(0,t)$ for every $t \in \mathbb{R}$; σ_0 and ω_0 are Bob and Willie's respective outputs for the "innocent" input $|0\rangle$, whereas σ_1 and ω_1 are the outputs associated with inputs that are orthogonal to $|0\rangle$; $D(\rho||\sigma)$ is the quantum relative entropy and $\chi^2(\rho||\sigma)$ is the quantum chi-square divergence defined in (2) below (see [52, Eq. (4)], [53, Sec. 1.1.4]). Remarkably, we establish a single-letter formula for this fully quantum model. Separately in [54], we extend our result to continuous-variable bosonic channels.

The paper is organized as follows. In Section II, we address covert communication of classical information under a secrecy constraint. In Section III, we present the model definitions and capacity result for covert entanglement generation. The proof outline for covert and secret communication is given in Section IV. Section V concludes with a summary and discussion. See detailed analysis in [55].

Basic Definitions: We use the following notation conventions: $\mathcal{X}, \mathcal{Y}, \mathcal{Z}, \ldots$ are finite sets, $\mathbf{x}, \mathbf{y}, \mathbf{z}, \ldots$ represent random variables, and $x, y, z, \ldots$ their values. We use $x^j = (x_1, x_2, \ldots, x_j)$ for a sequence of letters from $\mathcal{X}$, and $[i:j] \equiv \{i, i+1, \ldots, j\}$ where $j > i$. $[t]_+ \equiv \max(0,t)$ for $t \in \mathbb{R}$. We use standard asymptotic notation [56, Ch. 3.1] $O(g(n))$, $o(g(n))$, $\Omega(g(n))$, $\omega(g(n))$ for functions $g : \mathbb{N} \to \mathbb{R}$. The quantum state of system A is described by a density operator ρ on a finite-dimensional Hilbert space $\mathcal{H}_A$. We denote the dimension by either d_A or $\dim(\mathcal{H}_A)$. Let $|\Phi\rangle_{A_1A_2} \equiv \frac{1}{\sqrt{d_A}} \sum_{i=0}^{d_A-1} |i\rangle_{A_1} \otimes |i\rangle_{A_2}$.

The quantum relative entropy and fidelity between ρ and σ are denoted as $D(\rho||\sigma)$ and $F(\rho,\sigma)$, respectively. The quantum chi-square divergence can be defined by $\chi^2(\rho||\sigma) = \frac{\partial^2}{\partial \alpha^2} D(\alpha\rho + (1-\alpha)\sigma||\sigma)\Big|_{\alpha=0}$ (see [57, Sec. 2.6]). Explicitly, given a spectral decomposition of a full-rank operator, $\sigma = \sum_i \lambda_i \Pi_i$, we have [52, Eq. (4)]

$$\chi^2(\rho||\sigma) = \sum_{i\neq j} \frac{\log(\lambda_i) - \log(\lambda_j)}{\lambda_i - \lambda_j} \mathrm{Tr}\left[(\rho-\sigma)\Pi_i(\rho-\sigma)\Pi_j\right] + \sum_i \frac{1}{\lambda_i} \mathrm{Tr}\left[(\rho-\sigma)\Pi_i(\rho-\sigma)\Pi_i\right] \tag{2}$$

with natural exponents and logarithms. A quantum channel $\mathcal{N}_{A\to B}$ is a linear CPTP map. See details in [55, Sec. II].

II. Classical Information With Secrecy

First, we consider covert transmission of *classical* information with *secrecy* over a quantum channel.

A. Coding Definitions

Consider a c-q channel $\mathcal{P}_{X\to BW}$. The reduced states of Bob and Willie are $\sigma_x \equiv \mathrm{Tr}_W(\mathcal{P}_{X\to BW}(x))$ and $\omega_x \equiv \mathrm{Tr}_B(\mathcal{P}_{X\to BW}(x))$, respectively. Alice wishes to send a classical message to Bob with covertness and secrecy guarantees.

Definition 1. A classical secrecy code $(\mathcal{M}, \mathcal{L}, f, \Lambda)$ for $\mathcal{P}_{X\to BW}$ consists of: a secret message set $\mathcal{M}$, a public message set $\mathcal{L}$, an encoding function $f : \mathcal{M}\times\mathcal{L} \to \mathcal{X}^n$, and a collection of decoding measurements $\{\Lambda_{B^n}^{(m,\ell)}, (m,\ell) \in \mathcal{M}\times\mathcal{L}\}$.

Per Figure 2, Alice desires to send a secret message $m \in \mathcal{M}$ and a public message $\ell \in \mathcal{L}$ to Bob. In covert communication, Alice makes a decision on whether to communicate or not. Assume $\mathcal{X} \equiv \{0,1\}$. If Alice decides to be inactive, the channel input is $x^n = (0,0,\ldots,0)$. Otherwise, she transmits a codeword $x^n = f(m,\ell)$. The joint output state is thus $\rho_{B^nW^n}^{(m,\ell)} = \mathcal{P}_{X\to BW}^{\otimes n}(f(m,\ell))$. Bob receives B^n, performs a decoding measurement $\{\Lambda_{B^n}^{(m,\ell)}\}$ and obtains an estimate $(\hat{m},\hat{\ell})$. The average error probability is given by

$$\overline{P}_e^{(n)} = \frac{1}{|\mathcal{M}||\mathcal{L}|} \sum_{\substack{(m,\ell)\in \\ \mathcal{M}\times\mathcal{L}}} \left(1 - \mathrm{Tr}\left(\Lambda_{B^n}^{(m,\ell)} \rho_{B^n}^{(m,\ell)}\right)\right). \tag{3}$$

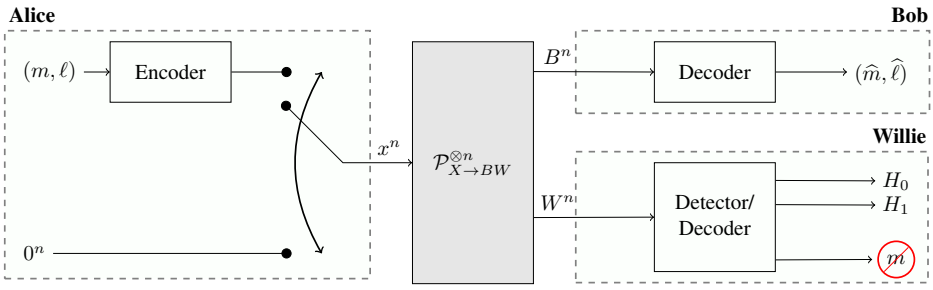

Fig. 2. Covert secrecy for a c-q channel. The goal is to send classical information both secretly and covertly.

Meanwhile, Willie receives W^n in the following average state:

$$\overline{\rho}_{W^n} = \frac{1}{|\mathcal{M}|} \sum_{m\in\mathcal{M}} \rho_{W^n}^{(m)}, \tag{4}$$

where $\rho_{W^n}^{(m)} = \frac{1}{|\mathcal{L}|}\sum_{\ell\in\mathcal{L}} \rho_{W^n}^{(m,\ell)}$.

1) Detection by Warden: Willie performs a hypothesis test to determine whether there is transmission. If he identifies transmission, he may also try to recover the message. Let $e_W(n)$ denote the average probability of erroneous detection, assuming equally likely hypotheses. Alice wants to encode while making Willie's detector asymptotically ineffective, with $e_W(n) \to \frac{1}{2}$. By the quantum Pinsker inequality, $e_W(n) \geq \frac{1}{2}\left(1 - \sqrt{\frac{1}{2} D\left(\overline{\rho}_{W^n} || \omega_0^{\otimes n}\right)}\right)$, where ω_0 is Willie's output corresponding to the innocent input $x = 0$ (see [49, Sec. 9.1.4 and Th. 11.9.1]). Thus, a code is covert if $D\left(\overline{\rho}_{W^n} || \omega_0^{\otimes n}\right) \to 0$ as $n \to \infty$. The covert encoding scheme is based on a sparse coding, with only a fraction of α_n non-zero transmissions [24, 58], taking $\alpha_n = \frac{\gamma_n}{\sqrt{n}}$, where $\gamma_n \to 0$. Hence, $\omega_{\alpha_n} = (1-\alpha_n)\omega_0 + \alpha_n\omega_1$ is called the "quantum-secure covert state" [24, Sec. II-E]. Covertness follows from $D\left(\omega_{\alpha_n}^{\otimes n} || \omega_0^{\otimes n}\right) = nD\left(\omega_{\alpha_n} || \omega_0\right) \approx \frac{1}{2}\gamma_n^2 \chi^2\left(\omega_1 || \omega_0\right)$.

2) Covert Secrecy Capacity: The code should satisfy three requirements: reliability, covertness, and secrecy. An $(|\mathcal{M}|, |\mathcal{L}|, n, \varepsilon, \delta_{\text{cov}}, \delta_{\text{sec}})$ secrecy code satisfies

(i) *Decoding Reliability:* $\overline{P}_e^{(n)} \leq \varepsilon$

(ii) *Covertness Criterion:* $D\left(\overline{\rho}_{W^n} || \omega_0^{\otimes n}\right) \leq \delta_{\text{cov}}$

(iii) *Secrecy:* $\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}} \left\| \rho_{W^n}^{(m)} - \breve{\rho}_{W^n} \right\|_1 \leq \delta_{\text{sec}}$ for some $\breve{\rho}_{W^n}$, which does not depend on the secret message m.

Typically, the secrecy rate is defined as $R_{\text{S}} \equiv \frac{\log|\mathcal{M}|}{n}$ (bits per channel use). However, in the covert setting, the best achievable transmission rate is zero, since $\log|\mathcal{M}| = O(\sqrt{n})$. Instead, the covert secrecy rate is characterized as

$$L_{\text{S}} \equiv \frac{\log|\mathcal{M}|}{\sqrt{n\delta_{\text{cov}}}}, \tag{5}$$

hence, $|\mathcal{M}| = e^{\sqrt{n\delta_{\text{cov}}} L_{\text{S}}}$. Similarly, we define the public message as

$$L_{\text{public}} \equiv \frac{\log|\mathcal{L}|}{\sqrt{n\delta_{\text{cov}}}}, \tag{6}$$

and thus $|\mathcal{L}| = e^{\sqrt{n\delta_{\text{cov}}} L_{\text{public}}}$ (see [16], [17], [24]).

Definition 2 (Achievable covert secrecy rate). A covert secrecy rate $L_{\text{S}} > 0$ is achievable if, for every $\varepsilon, \delta_{\text{cov}}, \delta_{\text{sec}} > 0$, sufficiently large n, and some public message rate L_{public}, there exists a $(e^{\sqrt{n\delta_{\text{cov}}} L_{\text{S}}}, e^{\sqrt{n\delta_{\text{cov}}} L_{\text{public}}}, n, \varepsilon, \delta_{\text{cov}}, \delta_{\text{sec}})$ code for covert and secret classical communication.

Definition 3 (Covert secrecy capacity). The covert secrecy capacity $C_{\text{S}}(\mathcal{P})$ of a classical-quantum covert communication channel $\mathcal{P}_{X\to BW}$ is the supremum of all achievable rates.

3) Assumptions: For simplicity, we assume a binary input, i.e., $\mathcal{X} = \{0, 1\}$. We are interested in covert communication under the following assumptions: $\omega_1 \neq \omega_0$,

$$\text{supp}(\omega_1) \subseteq \text{supp}(\omega_0), \text{ and } \text{supp}(\sigma_1) \subseteq \text{supp}(\sigma_0). \tag{7}$$

This guarantees that the test is not trivial and that neither Bob nor Willie can detect a non-zero transmission with certainty.

Remark 1. When Willie's support condition $\text{supp}(\omega_1) \subseteq \text{supp}(\omega_0)$ is violated, Willie can identify any non-innocent transmission with certainty, as $D(\omega_1 \| \omega_0) \to \infty$. Covert communication is then fundamentally impossible, and the covert capacity is trivially zero.

Remark 2. While Bob's objective is to recover information (either classical or quantum), if $\text{supp}(\sigma_1) \nsubseteq \text{supp}(\sigma_0)$, then Bob has an unfair advantage over Willie in the sense that he can identify a non-innocent input with certainty. This improves the information scale to $\sim \sqrt{n}\log n$, surpassing the standard square root law.

B. Capacity Theorem

Recall $\sigma_x = \text{Tr}_W\left(\mathcal{P}_{X\to BW}(x)\right)$ and $\omega_x = \text{Tr}_B\left(\mathcal{P}_{X\to BW}(x)\right)$, for $x \in \{0, 1\}$.

Theorem 1. Let $\mathcal{P}_{X\to BW}$ be a c-q covert communication channel. Consider covert communication of classical information with secrecy via this channel. If $\mathcal{P}_{X\to BW}$ satisfies (7), then the covert secrecy capacity is given by

$$C_{\text{S}}(\mathcal{P}) = \frac{\left[D\left(\sigma_1 || \sigma_0\right) - D\left(\omega_1 || \omega_0\right)\right]_+}{\sqrt{\frac{1}{2}\chi^2\left(\omega_1 || \omega_0\right)}}. \tag{8}$$

The proof outline for Theorem 1 is given in Section IV. Further details are given in [55, Sec. S.3]. We combine several

methods from previous works on secret and covert communication. We build upon covert communication results without secrecy [24], along with the secrecy coding approach proposed by Bloch [17] for classical channels. We employ binning and use Hayashi's quantum channel resolvability lemma to guarantee secrecy [59].

III. Covert Entanglement Generation

We now turn to our main problem of interest. Consider a quantum channel $\mathcal{N}_{A\to B}$ with a Stinespring dilation $\mathcal{U}_{A\to BW}$. Hence, W is interpreted as the receiver's environment. Suppose that an adversarial warden, Willie, holds W. The complementary channel from Alice to Willie is defined by $\mathcal{N}^c_{A\to W} \equiv \mathrm{Tr}_B \circ \mathcal{U}_{A\to BW}$. Alice would like to generate entanglement with Bob covertly, i.e. without Willie knowing whether Alice transmitted or not. Assume that $|0\rangle$ is the "innocent" input, corresponding to the case where Alice is inactive, i.e., she is not using the channel in order to generate shared entanglement with Bob. Let $\{|0\rangle, |1\rangle\}$ be an orthonormal basis, and denote Bob and Willie's outputs by $\sigma_x \equiv \mathcal{N}_{A\to B}(|x\rangle\langle x|)$, $\omega_x \equiv \mathcal{N}^c_{A\to W}(|x\rangle\langle x|)$, respectively, for $x \in \{0,1\}$.

A. Coding Definitions

Definition 4. A (T, n) entanglement-generation code consists of a Hilbert space $\mathcal{H}_M$ of dimension T, and a collection of encoding and decoding maps, $\mathcal{F}_{M\to A^n}$ and $\mathcal{D}_{B^n\to\widehat{M}}$, respectively.

The setting is depicted in Figure 1. The goal is to generate entanglement between Alice and Bob, without being detected by Willie. Alice prepares $|\Phi\rangle_{RM}$ locally, on $\mathcal{H}_M^{\otimes 2}$, where R is a resource that she keeps, and M is the resource that she would like to distribute to Bob. If Alice decides to be inactive, the input is $|0\rangle^{\otimes n}$. Otherwise, if she does perform the task, she applies $\mathcal{F}_{M\to A^n}$ on her "quantum message" M, which results in a quantum state τ_{RA^n}. She then transmits the encoded system A^n via $\mathcal{U}^{\otimes n}_{A\to BW}$. The joint output state is thus $\tau_{RB^nW^n} = (\mathrm{id}_R \otimes \mathcal{U}^{\otimes n}_{A\to BW})(\tau_{RA^n})$. Bob decodes B^n by

$$\tau_{R\widehat{M}} = \left(\mathrm{id}_R \otimes \mathcal{D}_{B^n\to\widehat{M}}\right)(\tau_{RB^n}) \,. \tag{9}$$

Meanwhile, Willie receives W^n in the reduced state $\tau_{W^n} = \mathrm{Tr}_{RB^n}(\tau_{RB^nW^n})$ and performs his hypothesis test.

A $(T, n, \varepsilon, \delta)$-code for covert entanglement generation satisfies the following conditions:

(i) *Decoding Reliability:* $F\left(\tau_{R\widehat{M}}, \Phi_{RM}\right) \geq 1-\varepsilon$.
(ii) *Covertness Criterion:* $D\left(\tau_{W^n}||\omega_0^{\otimes n}\right) \leq \delta$.

Remark 3. As all Stinespring dilations are isometrically equivalent, the result does not depend on the choice of dilation.

Remark 4. Entanglement generation is intimately related to secrecy. Devetak [44] introduced a coherent version of classical secrecy codes, which leverage their privacy properties to define subspaces where Alice can securely encode quantum information, ensuring its inaccessibility.

In traditional tasks, the entanglement rate is defined as $R_{\mathrm{EG}} \equiv \frac{\log[\dim(\mathcal{H}_M)]}{n}$, i.e., the number of qubit pairs per channel use. However, in the covert setting, the best achievable entanglement rate is zero, as $\log[\dim(\mathcal{H}_M)] = O(\sqrt{n})$. Instead, we define the covert entanglement-generation rate as

$$L_{\mathrm{EG}} \equiv \frac{\log T}{\sqrt{n\delta}}\,, \quad \text{where } T = \dim(\mathcal{H}_M)\,, \tag{10}$$

hence, $T = e^{\sqrt{n\delta}L_{\mathrm{EG}}}$.

Definition 5 (Achievable covert entanglement-generation rate). A covert entanglement-generation rate $L_{\mathrm{EG}} > 0$ is achievable if for every $\varepsilon, \delta > 0$ and sufficiently large n, there exists a $(e^{\sqrt{n\delta}L_{\mathrm{EG}}}, n, \varepsilon, \delta)$ code for covert entanglement generation.

Definition 6 (Covert entanglement-generation capacity). The covert entanglement-generation capacity $C_{\mathrm{EG}}(\mathcal{N})$ of a quantum channel $\mathcal{N}_{A\to B}$ is the supremum of all achievable rates.

B. Capacity Theorem

For simplicity, we assume $d_A = 2$. Recall $\sigma_x = \mathcal{N}_{A\to B}(|x\rangle\langle x|)$ and $\omega_x = \mathcal{N}^c_{A\to W}(|x\rangle\langle x|)$, for $x \in \{0,1\}$.

Theorem 2. Consider covert entanglement generation via a quantum channel $\mathcal{U}_{A\to BW}$ that satisfies (7). Then, the covert entanglement-generation capacity is given by

$$C_{\mathrm{EG}}(\mathcal{N}) = \frac{[D(\sigma_1||\sigma_0) - D(\omega_1||\omega_0)]_+}{\sqrt{\frac{1}{2}\chi^2(\omega_1||\omega_0)}}\,. \tag{11}$$

The proof of Theorem 2 is given in [55, Sec. V].

Remark 5. Recall that $\{|x\rangle\}_{x=0,1}$ is an orthonormal basis for the input Hilbert space $\mathcal{H}_A$. We may define a c-q channel, $\mathcal{P}_{X\to BW}(x) \equiv \mathcal{U}_{A\to BW}(|x\rangle\langle x|_A)$ for $x \in \{0,1\}$. To show achievability, we construct an entanglement generation code for the quantum channel $\mathcal{N}_{A\to B}$ from classical secrecy codes for $\mathcal{P}_{X\to BW}$, following the approach in [44]. The covert entanglement-generation capacity is identical to the classical covert secrecy capacity.

Remark 6. In a recent work on covert quantum communication [46], a lower bound is established using Pauli twirl modulation with the aid of $O(\sqrt{n}\log n)$ key bits, based on a method that employs a sparse signaling approach. This implies that the key rate is infinite in their coding scheme. Here, on the other hand, we do not use a key.

Example 1. Consider the excitation channel, $\mathcal{N}(\rho) = K_0\rho K_0^\dagger + K_1\rho K_1^\dagger$, where $K_0 = \sqrt{1-\gamma}\,|0\rangle\langle 0| + |1\rangle\langle 1|$, $K_1 = \sqrt{\gamma}\,|1\rangle\langle 0|$, for $\gamma \in (0,1]$. By Theorem 2, the covert entanglement-generation capacity is given by $C_{\mathrm{EG}}(\mathcal{N}) = \log\left(\frac{1-\gamma}{\gamma}\right)\sqrt{\frac{2(1-\gamma)}{\gamma}}$ if $\gamma \in \left(0, \frac{1}{2}\right)$, else 0. See Figure 3. As $\gamma \to 0$, covertness becomes trivial, hence the number of EPR pairs is linear in n, and the capacity in the scale of $O(\sqrt{n})$ tends to infinity. For $\gamma \geq \frac{1}{2}$, the channel is anti-degradable [60], in which case entanglement generation is impossible, thus the capacity is zero.

IV. Proof Outline for Theorem 1

Consider a c-q channel $\mathcal{P}_{X\to BW}$.

Proposition 3. Consider a covert memoryless c-q channel such that $\mathrm{supp}(\sigma_1) \subseteq \mathrm{supp}(\sigma_0)$, $\mathrm{supp}(\omega_1) \subseteq \mathrm{supp}(\omega_0)$ and

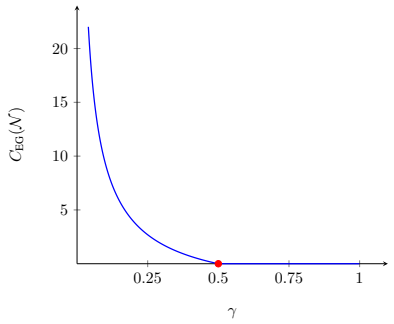

Fig. 3. Covert entanglement-generation capacity of the excitation channel. The red marker indicates the transition point at $\gamma = 0.5$, beyond which the channel is anti-degradable and entanglement generation is impossible.

$\omega_1 \neq \omega_0$. Let $\alpha_n = \frac{\gamma_n}{\sqrt{n}}$ with $\gamma_n \in o(1) \cap \omega\left(\frac{(\log n)^{\frac{7}{3}}}{n^{\frac{1}{6}}}\right)$. Then, for any $\zeta_n \in o(1) \cap \omega\left((\log n)^{-\frac{2}{3}}\right)$, there exist $\zeta_n^{(1)} \in \omega\left((\log n)^{-\frac{4}{3}} n^{-\frac{1}{3}}\right), \zeta_n^{(2)} \in \omega\left((\log n)^{-2}\right), \zeta_n^{(3)} \in \omega\left((\log n)^{-1}\right)$, and a c-q covert secrecy code such that, for n sufficiently large:

$$\begin{aligned} \log|\mathcal{M}||\mathcal{L}| &= (1-\zeta_n)\gamma_n\sqrt{n}D\left(\sigma_1||\sigma_0\right), \\ \log|\mathcal{L}| &= (1+\zeta_n)\gamma_n\sqrt{n}D\left(\omega_1||\omega_0\right) \end{aligned} \tag{12}$$

and

$$\overline{P}_e^{(n)} \leq e^{-\zeta_n^{(1)}\gamma_n\sqrt{n}}, \tag{13a}$$

$$\left|D\left(\overline{\rho}_{W^n}||\omega_0^{\otimes n}\right) - D\left(\omega_{\alpha_n}^{\otimes n}||\omega_0^{\otimes n}\right)\right| \leq e^{-\zeta_n^{(2)}\gamma_n^{\frac{3}{2}}n^{\frac{1}{4}}}, \tag{13b}$$

$$\frac{1}{|\mathcal{M}|}\sum_{m\in\mathcal{M}}\left\|\rho_{W^n}^{(m)} - \omega_{\alpha_n}^{\otimes n}\right\|_1 \leq e^{-\zeta_n^{(3)}\gamma_n^{\frac{3}{2}}n^{\frac{1}{4}}}. \tag{13c}$$

Proof. We follow similar steps as in the classical work by Bloch [17]. Assume $(1-\zeta_n)D\left(\sigma_1||\sigma_0\right) > (1+\zeta_n)D\left(\omega_1||\omega_0\right)$. In this case, covertness without secrecy can be achieved without a key (see [24, Th. 1]).

Classical codebook generation: Select codewords $\mathbf{c}(m,\ell) \in \{0,1\}^n$, independently at random, for $(m,\ell) \in \mathcal{M}\times\mathcal{L}$, each i.i.d. $\sim$ Bernoulli(α_n). Reveal the codebook. We denote $\mathscr{C} = \{\mathbf{c}(m,\ell)\}$.

Encoder: Given the overall "message" $\breve{m} = (m,\ell)$, transmit $\mathbf{x}^n = \mathbf{c}(m,\ell)$.

Decoder: We use the same decoding map as in [24].

The error and covertness derivations follow the previous results without secrecy, due to Bullock et al. [24], and are thus omitted. The main novelty of our analysis is in the derivation of secrecy, which was not considered in [24]. To ensure secrecy, we combine the binning and quantum channel resolvability techniques.

First, we set

$$\log|\mathcal{L}| = (1+\zeta_n)\gamma_n\sqrt{n}D\left(\omega_1||\omega_0\right). \tag{14}$$

Then, we divide the random code $\mathscr{C}$ into $|\mathcal{M}|$ bins, $\mathscr{C}_m$ for $m \in \mathcal{M}$, each of size $|\mathcal{L}|$. ℓ serves as the codeword index within each bin $\mathscr{C}_m$. In order to establish secrecy, we apply the quantum channel resolvability (see [59, Lemma 9.2] [61]),

$$\begin{aligned} \mathop{\mathbb{E}}_{\mathscr{C}}\left[\left\|\rho_{W^n}^{(m)} - \omega_{\alpha_n}^{\otimes n}\right\|_1\right] &= \mathop{\mathbb{E}}_{\mathscr{C}}\left[\left\|\frac{1}{|\mathcal{L}|}\sum_{\ell\in\mathcal{L}}\omega_{\mathbf{c}(m,\ell)} - \omega_{\alpha_n}^{\otimes n}\right\|_1\right] \\ &\leq 2\sqrt{\exp\left[\beta_n s_n + n\phi(s_n,\alpha_n)\right]} + \sqrt{\frac{e^{\beta_n}\nu_n}{|\mathcal{L}|}}, \end{aligned} \tag{15}$$

where the expectation is with respect to the random codebook, and ν_n is the number of distinct eigenvalues of $\omega_{\alpha_n}^{\otimes n}$. See details in [55, Sec. S.3]. We show that this vanishes for $|\mathcal{L}|$ as in (14). Based on standard arguments, there exists a deterministic codebook that satisfies the desired properties.

This completes the achievability proof outline for covert secrecy. The converse proof is given in [55, Sec. S.3]. □

V. Summary and Discussion

We study covert entanglement generation, where the transmission is hidden from the adversary (see Figure 1). Our approach is fundamentally different from that in Anderson et al. [45, 46]. First, we consider the combined setting of covert and secret communication of classical information. We derive the covert secrecy capacity in Theorem 1, generalizing Bloch's classical result [17, Sec. VII-C]. Then, we construct an entanglement-generation code from the secrecy code. As a result, our covert entanglement-generation rate in Theorem 2 is the same as the secret classical information rate. Remarkably, we establish a single-letter formula for both capacities. Unlike Anderson et al. [46], our scheme does not require a pre-shared secret key. Separately, we extend this to continuous-variable bosonic channels [62].

Several open questions remain. Extending covertness to arbitrary quantum state transmission is challenging due to induced non-uniform input distributions, which fall outside standard covert analyses. A full characterization of resource trade-offs between secret, public, entanglement, and key rates also remains open. Additionally, relaxing the isometric channel assumption (where Willie observes the full environment) may enable higher covert rates, but requires new analytical tools. Further directions include regimes where our assumptions do not hold, such as scenarios with an unfair advantage for Bob, which may lead to improvements beyond the square-root law, as well as the covertness of composite protocols (e.g., teleportation-based schemes).

Acknowledgments

The authors wish to thank Marco Tomamichel, Ian George, Matthieu Bloch, Evan J.D. Anderson, and Michael S. Bullock for useful and helpful discussions. This work was supported by ISF n. 939/23 and 2691/23, DIP n. 2032991, OMC n. 86160946, QERNEL (VATAT) n. 2072651, in part by HDQC at Technion n. 2033613, and by NSF n. CCF-2006679, EEC-1941583 and CNS-2107265.

References

[1] A. J. Menezes, S. A. Vanstone, and P. C. V. Oorschot, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, Inc., 1996.

[2] J. Talbot and D. Welsh, *Complexity and Cryptography: An Introduction*. Cambridge University Press, 2006.

[3] H. Boche, M. Cai, N. Cai, and C. Deppe, "Secrecy capacities of compound quantum wiretap channels and applications," *Phys. Rev. A*, vol. 89, no. 5, p. 052320, 2014.

[4] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, "Quantum enigma machines and the locking capacity of a quantum channel," *Phys. Rev. X*, vol. 4, no. 1, p. 011016, 2014.

[5] R. F. Schaefer, A. Khisti, and H. V. Poor, "Secure broadcasting using independent secret keys," *IEEE Trans. Commun.*, vol. 66, no. 2, pp. 644–661, 2018.

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

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

[8] K. Adhikari and C. Deppe, "Quantum information spreading and scrambling in a distributed quantum network," in *28th Eur. Wireless Conf.*, 2023, pp. 358–363.

[9] M. Ahmadipour, M. Wigger, and S. Shamai, "Integrated communication and receiver sensing with security constraints on message and state," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2023, pp. 2738–2743.

[10] F. Seitz, M. Rosati, Á. Vázquez-Castro, and J. Nötzel, "Private communication over a bosonic compound channel," *arXiv preprint arXiv:2411.10292*, 2024.

[11] P. Munar-Vallespir, J. Nötzel, and F. Seitz, "Joint communication and eavesdropper detection on the lossy bosonic channel," in *IEEE Global Commun. Conf.*, 2024.

[12] 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.

[13] B. A. Bash, D. Goeckel, and D. Towsley, "Square root law for communication with low probability of detection on AWGN channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Cambridge, MA, Jul. 2012.

[14] ——, "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.

[15] 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, p. 8626, 2015.

[16] 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.

[17] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2334–2354, 2016, See correction at https://bloch.ece.gatech.edu/blog/2020/errata/.

[18] M. Tahmasbi and M. R. Bloch, "Framework for covert and secret key expansion over classical-quantum channels," *Phys. Rev. A*, vol. 99, p. 052329, May 2019.

[19] ——, "Covert and secret key expansion over quantum channels under collective attacks," *IEEE Tran. Inf. Theory*, vol. 66, no. 11, pp. 7113–7131, 2020.

[20] 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.

[21] M. Tahmasbi and M. R. Bloch, "Steganography protocols for quantum channels," *J. Math. Phys.*, vol. 61, no. 8, 2020.

[22] H. ZivariFard, R. A. Chou, and X. Wang, "Covert communication over a quantum mac with a helper," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2025.

[23] A. Sheikholeslami, B. A. Bash, D. Towsley, D. Goeckel, and S. Guha, "Covert communication over classical-quantum channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2016, pp. 2064–2068.

[24] M. S. Bullock, A. Sheikholeslami, M. Tahmasbi, R. C. Macdonald, S. Guha, and B. A. Bash, "Fundamental limits of covert communication over classical-quantum channels," *IEEE Trans. Inf. Theory*, vol. 71, no. 4, pp. 2741–2762, Apr. 2025.

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

[26] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Commun. Surv. Tut.*, vol. 25, no. 2, pp. 1173–1198, 2023.

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

[28] F. Leditzky, M. A. Alhejji, J. Levin, and G. Smith, "Playing games with multiple access channels," *Nat. Commun.*, vol. 11, no. 1, p. 1497, 2020.

[29] U. Pereg, C. Deppe, and H. Boche, "Quantum broadcast channels with cooperating decoders: An information-theoretic perspective on quantum repeaters," *J. Math. Phys.*, vol. 62, no. 6, p. 062204, 06 2021.

[30] O. Fawzi and P. Fermé, "Multiple-access channel coding with non-signaling correlations," *IEEE Trans. Inf. Theory*, vol. 70, no. 3, pp. 1693–1719, 2024.

[31] M. Lederman and U. Pereg, "Semantic security with unreliable entanglement assistance: Interception and loss," in *Proc. IEEE Inf. Theory Workshop (ITW)*, 2024, pp.

693–698.

[32] O. Fawzi and P. Fermé, "Broadcast channel coding: Algorithmic aspects and non-signaling assistance," *IEEE Trans. Inf. Theory*, vol. 70, no. 11, pp. 7563–7580, 2024.

[33] L. H. Wolff, P. Belzig, M. Christandl, B. Durhuus, and M. Tomamichel, "Fundamental limit on the power of entanglement assistance in quantum communication," *Phys. Rev. Lett.*, vol. 134, p. 020802, Jan 2025.

[34] Y. Yao and S. A. Jafar, "Can non-signaling assistance increase the degrees of freedom of a wireless network?" *arXiv preprint arXiv:2503.08597*, 2025.

[35] U. Pereg, C. Deppe, and H. Boche, "The multiple-access channel with entangled transmitters," *IEEE Tran. Inf. Theory*, vol. 71, no. 2, pp. 1096–1120, 2025.

[36] C. Bennett, P. Shor, J. Smolin, and A. Thapliyal, "Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem," *IEEE Trans. Inf. Theory*, vol. 48, no. 10, pp. 2637–2655, 2002.

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

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

[39] 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, 2020.

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

[41] S.-Y. Wang, S.-J. Su, and M. R. Bloch, "Resource-efficient entanglement-assisted covert communications over bosonic channels," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2024, pp. 3106–3111.

[42] S. Lloyd, "Capacity of the noisy quantum channel," *Phys. Rev. A*, vol. 55, no. 3, p. 1613, 1997.

[43] P. W. Shor, "The quantum channel capacity and coherent information," in *lecture notes, MSRI Workshop Quantum Comput.*, 2002.

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

[45] E. J. D. Anderson, C. K. Eyre, I. M. Dailey, F. Rozpędek, and B. A. Bash, "Square root law for covert quantum communication over optical channels," in *Proc. IEEE Int. Conf. Quantum Comput. Eng. (QCE)*, Montréal, QC, Canada, 2024, pp. 1817–1823.

[46] E. J. D. Anderson, M. S. Bullock, F. Rozpędek, and B. A. Bash, "Achievability of covert quantum communication," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, 2025.

[47] S. Watanabe, "Private and quantum capacities of more capable and less noisy quantum channels," *Phys. Rev. A*, vol. 85, p. 012326, Jan 2012.

[48] S. Singh and N. Datta, "Information storage and transmission under markovian noise," *PRX Quantum*, vol. 7, no. 2, p. 020312, 2026.

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

[50] P. Hayden, M. Horodecki, A. Winter, and J. Yard, "A decoupling approach to the quantum capacity," *Open Syst. Inf. Dyn*, vol. 15, no. 01, pp. 7–19, 2008.

[51] F. Dupuis, M. Berta, J. Wullschleger, and R. Renner, "One-shot decoupling," *Commun. Math. Phys.*, vol. 328, pp. 251–284, 2014.

[52] 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.

[53] E. Zlotnick, "Entanglement-assisted covert communication via qubit depolarizing channels," M.Sc. Thesis, Technion - Israel Institute of Technology, Haifa, Apr 2024, https://qcomm.ece.technion.ac.il/wp-content/uploads/2024/08/Technion_thesis___Elyakim_Zlotnick.pdf.

[54] E. J. Anderson, M. S. Bullock, O. Kimelfeld, C. K. Eyre, F. Rozpędek, U. Pereg, and B. A. Bash, "Covert entanglement generation over bosonic channels," *IEEE J. Sel. Areas Commun.*, 2025.

[55] O. Kimelfeld, B. A. Bash, and U. Pereg, "Covert entanglement generation and secrecy," arXiv:2503.21002 [quant-ph], 2025.

[56] T. H. Cormen, C. E. Leiserson, R. L. Rivest, and C. Stein, *Introduction to algorithms*, 3rd ed. MIT press, 2009.

[57] C. Hirche and M. Tomamichel, "Quantum rényi and f-divergences from integral representations," *Commun. Math. Phys.*, vol. 405, no. 9, Sep. 2024.

[58] M. Tahmasbi, S. Guha, B. A. Bash, and M. R. Bloch, "Signaling for covert quantum sensing," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, virtual, Jul. 2021.

[59] M. Hayashi, *Quantum Information*. Springer, 2006.

[60] S. Khatri, K. Sharma, and M. M. Wilde, "Information-theoretic aspects of the generalized amplitude-damping channel," *Phys. Rev. A*, vol. 102, p. 012401, Jul 2020.

[61] 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.

[62] E. J. Anderson, M. S. Bullock, O. Kimelfeld, C. K. Eyre, F. Rozpędek, and B. A. Bash, "Covert entanglement generation over bosonic channels," arXiv:2506.09474 [quant-ph], 2025.