Framework for covert and secret key expansion over classical-quantum channels

Mehrdad Tahmasbi[*] and Matthieu R. Bloch[†]
Georgia Institute of Technology, Atlanta, Georgia 30332, USA

(Received 26 November 2018; published 20 May 2019)

Covert and secret quantum key distribution aims at generating information-theoretically secret bits between distant legitimate parties in a manner that remains provably undetectable by an adversary. We propose a framework in which to precisely define and analyze such an operation, and we show that covert and secret key expansion is possible. For fixed and known classical-quantum wiretap channels, we develop and analyze protocols based on forward and reverse reconciliation. The crux of our approach is the use of information reconciliation and privacy amplification techniques that are able to process the sparse signals required for covert operation and the Shannon entropy of which scales as the square root of their length. In particular, our results show that the coordination required between legitimate parties to achieve covert communication can be achieved with a negligible number of secret key bits.

DOI: 10.1103/PhysRevA.99.052329

I. INTRODUCTION

Securing communications has become an essential requirement in modern communication systems. Secrecy, i.e, the ability to prevent unauthorized parties from extracting the information content of a signal, is typically enforced using conventional computationally secure encryption although quantum key distribution (QKD) remains to date the only approach to unconditional secrecy [1,2]. Another desirable feature of secure communications is covertness, i.e., the ability to hide the presence of communication signals from an unauthorized party and provably avoid detection [3]. While secrecy has been largely explored for quantum communications both theoretically and experimentally, the mechanisms required to achieve covertness are still much less understood.

Covertness, also referred to as low probability of detection, is conceptually related to classical and quantum steganography [4–7], by which legitimate parties embed a message into a covertext then disclosed to an adversary [8]. In many quantum steganography protocols, an innocent quantum state, in the form of a codeword from a quantum error-control code, is used as the cover to embed another quantum state. The embedding is performed to simulate the transmission of an innocent state through a noisy channel and relies on shared secret keys with well-characterized rates. A crucial assumption in these quantum steganography protocols is that the true physical channel is better than what the adversary expects. In covert communications, however, the role of the covertext is played by the communication channel, which introduces noise and imperfections that are outside the control of and only statistically known to the transmitter. There has been a recent surge of interest for covert communications, which has led to the discovery of a "square-root law" similar to that in steganography [5] in both classical [9–11] and quantum settings [12–15]. The square-root law, according to which the number of covert bits can only scale with the square root of the number of channel uses, has also been experimentally validated in an optical testbed [12]. The authors of [12] also showed that, for a bosonic channel, covert communication is impossible without sources of imperfection in the adversary's observations since the detection of a single photon would indicate with certainty the existence of the communication. The possibility of quantum covert and secret key generation was recently explored [16–18] but has led to the rather pessimistic conclusion that "covert QKD consumes more secret bits than it can generate" [16].

Our main contribution is to offer a more nuanced and optimistic perspective and show that covert and secret key expansion is actually possible over quantum channels. The intuition behind our approach is the following. In layman's terms, the covertness constraint requires the number of qubit transmissions to scale as $O(\sqrt{T})$ for T channel uses [12]. A crucial characteristic of earlier works [12,16] is that the scaling is ensured by having the legitimate parties *coordinate* the sparse transmission of $\sqrt{T}$ qubits in channel uses chosen secretly and uniformly at random out of T. Unfortunately, the secret key size required to select these secret channel uses scales as $\Omega(\sqrt{T}\ln T)$ and necessarily exceeds the number of covert bits that one can hope to obtain, which scales as $\Omega(\sqrt{T})$. In contrast, we introduce more sophisticated coding schemes for information reconciliation and privacy amplification that do not require such coordination and are able to directly process the sparse and diffuse statistical information content of covert signals. The protocols that we present do not yet offer the secrecy levels of state-of-the art QKD against coherent attacks but already achieve covert and secret key expansion over classical-quantum (cq) wiretap channels and might pave the way to more broadly applicable protocols.

Our results are developed in two steps as follows. We first lay out a precise model for quantum covert and secret key generation that captures a wide range of attacks by the adversary and protocols for legitimate parties, along with

[*] Corresponding author: mtahmasbi3@gatech.edu
[†] matthieu.bloch@ece.gatech.edu

quantifiable metrics to assess the performance of a covert and secret key generation protocol over quantum channels. The main distinction with previous models [16–18] is the inclusion of the public communication required for information reconciliation in the analysis; specifically, since an adversary may devise a hypothesis test for detection based on all its observations, the probability distribution of the public communication has to be considered jointly with the quantum measurements in evaluating covertness. We then proceed to analyze an instance of quantum covert and secret key generation over fixed and known cq wiretap channels, for which we can define and analyze the covert and secret key capacity. We lower bound the covert and secret key capacity by developing coding schemes using both forward and reverse reconciliation. The forward reconciliation scheme can be constructed by a suitable modification of established protocols for quantum covert communication [14] to guarantee secrecy. In contrast, the reverse reconciliation scheme requires a new approach because of technical challenges precluding the direct use of well-known results on information reconciliation and privacy amplification for the sparse distribution needed for covert communication. We do not instantiate explicit codes but recent progress in designing codes for covert communications [19] suggests that the protocols described here can be implemented with low complexity.

II. NOTATION

We briefly introduce the notation used throughout the paper. For a finite-dimensional Hilbert space $\mathcal{H}$, $\dim \mathcal{H}$ denotes the dimension of $\mathcal{H}$, and $\mathcal{L}(\mathcal{H})$ denotes the space of all linear operators from $\mathcal{H}$ to $\mathcal{H}$. We denote the adjoint of an operator $X \in \mathcal{L}(\mathcal{H})$ by $X^\dagger$, and call X Hermitian if $X = X^\dagger$. $X \in \mathcal{L}(\mathcal{H})$ is positive (non-negative) semidefinite, if it is Hermitian and all of its eigenvalues are positive (non-negative). $\mathcal{D}(\mathcal{H})$ denotes the set of all density operators on $\mathcal{H}$, i.e., all non-negative operators with unit trace. For $X, Y \in \mathcal{L}(\mathcal{H})$, we write $X \succ Y$ ($X \succeq Y$), if $X - Y$ is positive (non-negative) semidefinite. For $X \in \mathcal{H}$, let $\sigma_{\min}(X)$ and $\sigma_{\max}(X)$ denote the minimum and the maximum singular value of X, respectively, and if X is Hermitian let $\lambda_{\min}(X)$ and $\lambda_{\max}(X)$ denote the minimum and maximum eigenvalue of X. Furthermore, we define two norms of $X \in \mathcal{L}(\mathcal{H})$ as $\|X\|_1 \triangleq \operatorname{tr}(\sqrt{X^\dagger X})$ and $\|X\|_2 \triangleq \sqrt{\operatorname{tr}(X^\dagger X)}$. For a Hermitian operator $X \in \mathcal{L}(\mathcal{H})$ with eigendecomposition $X = \sum_x x|x\rangle\langle x|$, we define the projection $\{X \succeq 0\} \triangleq \sum_{x \geqslant 0} |x\rangle\langle x|$. A quantum channel $\mathcal{E}_{A\to B}$ is a completely positive and trace preserving linear map from $\mathcal{L}(\mathcal{H}^A)$ to $\mathcal{L}(\mathcal{H}^B)$. An isomorphic extension of $\mathcal{E}_{A\to B}$, $U_{A\to BE}$ satisfies $\mathcal{E}_{A\to B}(\rho^A) = \operatorname{tr}_E(U_{A\to BE}\rho^A U^\dagger_{A\to BE})$ for all $\rho^A \in \mathcal{D}(\mathcal{H}^A)$. A cq channel is a map from an abstract set $\mathcal{X}$ to $\mathcal{D}(\mathcal{H})$, denoted by $x \mapsto \rho_x$.

For $\rho^A \in \mathcal{D}(\mathcal{H}^A)$ we define von Neumann entropy $H(\rho^A) \triangleq \mathbb{H}(A)_\rho \triangleq -\operatorname{tr}(\rho^A \ln \rho^A)$. For $\rho^{AB} \in \mathcal{D}(\mathcal{H}^A \otimes \mathcal{H}^B)$, we define the conditional von Neumann entropy $\mathbb{H}(A|B)_\rho \triangleq H(\rho^{AB}) - H(\rho^B)$ where $\rho^B \triangleq \operatorname{tr}_A(\rho^{AB})$, and the quantum mutual information $\mathbb{I}(A;B)_\rho \triangleq H(\rho^A) + H(\rho^B) - H(\rho^{AB})$. Similarly, we define the conditional quantum mutual information $\mathbb{I}(A;B|C) \triangleq H(\rho^{AC}) + H(\rho^{BC}) - H(\rho^{ABC}) - H(\rho^C)$ for any $\rho^{ABC} \in \mathcal{D}(\mathcal{H}^A \otimes \mathcal{H}^B \otimes \mathcal{H}^C)$. If P_X is a distribution on $\mathcal{X}$ and $x \mapsto \rho_x$ is a cq channel, we denote the Holevo information by

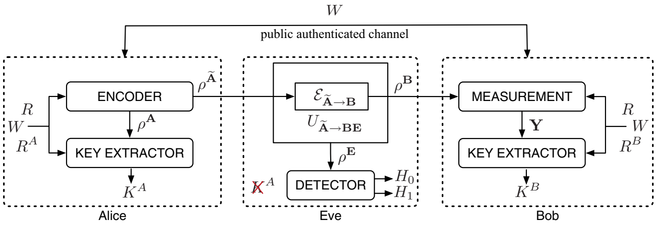

FIG. 1. Model of covert and secret key expansion.

$$I(P_X, \rho_x) \triangleq H\left(\sum_x P_X(x)\rho_x\right) - \sum_x P_X(x)H(\rho_x). \quad (1)$$

For $\rho, \sigma \in \mathcal{D}(\mathcal{H})$, the quantum relative entropy is

$$\mathbb{D}(\rho\|\sigma) \triangleq \begin{cases} \operatorname{tr}(\rho(\ln\rho - \ln\sigma)) & \text{if } \operatorname{supp}(\rho) \subset \operatorname{supp}(\sigma), \\ \infty & \text{otherwise}, \end{cases} \quad (2)$$

and the χ_2 distance is

$$\chi_2(\rho\|\sigma) \triangleq \begin{cases} \operatorname{tr}(\rho^2\sigma^{-1}) - 1 & \text{if } \operatorname{supp}(\rho) \subset \operatorname{supp}(\sigma), \\ \infty & \text{otherwise}. \end{cases} \quad (3)$$

III. FRAMEWORK FOR COVERT AND SECRET KEY GENERATION OVER cq WIRETAP CHANNELS

As illustrated in Fig. 1, we consider a setting in which two legitimate parties, Alice and Bob, desire to share a secret key while avoiding detection from an adversary, Eve, by exploiting a one-way quantum channel and a two-way classical authenticated public channel of unlimited capacity. Specifically, over T time steps, Alice prepares a cq state $\rho^{A\widetilde{A}}$, possibly depending on public communications, on a bipartite system described by a Hilbert space $\mathcal{H}^A \otimes \mathcal{H}^{\widetilde{A}}$ and sends the subsystem $\widetilde{A}$ to Bob. We assume that, for $\mathcal{X} \subset \mathbb{R}$, $\{|x\rangle^A\}_{x\in\mathcal{X}}$ is an orthonormal basis for $\mathcal{H}^A$, all eigenvectors of ρ^A are always in $\{|x\rangle^A\}_{x\in\mathcal{X}}$, and for any $x \in \mathcal{X}$ the conditional state $\rho_x^{\widetilde{A}}$ is fixed. For simplicity, we restrict our attention to a two-dimensional $\mathcal{H}^A$, i.e., $\mathcal{X} = \{0, 1\}$, in which zero represents an "innocent" symbol, corresponding to the absence of communication, while 1 represents a "noninnocent" symbol. We further assume that the "start" ($t = 1$) and "stop" ($t = T$) times of the protocol are known to all parties and obtained through other modalities, e.g., GPS signals. Eve expects the product state $(\rho_0^{\widetilde{A}})^{\otimes T}$ when there is no communication and may modify the states according to a quantum channel. We denote the entire state received by Bob and acting on the product Hilbert space $(\mathcal{H}^B)^{\otimes T}$ by $\rho^{\mathbf{B}}$.

For the purpose of covert communications, we need to distinguish protocols based on the type of Eve's attacks. In the most general case, Eve implements a *coherent attack* described by a quantum channel

$$\mathcal{E}_{\widetilde{\mathbf{A}}\to\mathbf{B}} : \mathcal{L}((\mathcal{H}^{\widetilde{A}})^{\otimes T}) \to \mathcal{L}((\mathcal{H}^B)^{\otimes T}), \quad (4)$$

with isomorphic extension $U_{\widetilde{\mathbf{A}}\to\mathbf{BE}}$, in which Bob receives $\rho^{\mathbf{B}} = \mathcal{E}_{\widetilde{\mathbf{A}}\to\mathbf{B}}(\rho^{\widetilde{\mathbf{A}}})$. In such a situation, Bob should refrain from transmitting information over the public channel until the end of the transmission to avoid improving Eve's detection capability on the quantum channel. Note that this has no impact on QKD since no useful information is shared until the end of the protocol. A less powerful Eve can only implement *collective attacks* described by quantum channels of the form $\mathcal{E}_{\widetilde{\mathbf{A}}\to\mathbf{B}} = \mathcal{E}_{\widetilde{A}\to B}^{\otimes T}$, i.e., Eve applies the same channel independently to each state transmitted by Alice. In this case, we can assume that Bob receives each state before Alice transmits the next state, which allows meaningful public communication during the transmission between Alice and Bob. Throughout the paper, we assume that Alice and Bob have exact knowledge of the attack. We can therefore define an effective cq wiretap channel $x \mapsto \rho_x^{BE}$, with marginal cq channels $x \to \rho_x^B$ and $x \to \rho_x^E$ from Alice to Bob and Eve, respectively. Finally, Alice and Bob have access to independent local sources of randomness, denoted by $R^A \in \mathcal{R}^A$ and $R^B \in \mathcal{R}^B$, respectively, as well as a source of secret key $R \in \mathcal{R}$.

For simplicity, we describe the protocols with only reverse public communication, but extension to the general case, in which forward public communication is also allowed, does not present any difficulty. A protocol for key generation operates in T time steps as follows. Alice and Bob draw realizations r^A, r^B, and r of their local and common randomness. Subsequently, in every state $t \in [\![1, T]\!]$, the following occur.

(1) Alice prepares a cq state $\rho^{A\widetilde{A}}$ as explained earlier using her local randomness r^A, the common randomness r, as well as past public messages from Bob denoted $(w_1, \cdots, w_{t-1})$ and sends $\rho^{\widetilde{A}}$ to Bob through the channel controlled by Eve.

(2) Bob performs a quantum measurement on his available quantum state to obtain a classical measurement $y_t \in \mathcal{Y} \subset \mathbb{R}$.

(3) Bob sends a message $W_t \in \mathcal{W}_t$ over the public channel using his local randomness r_B, the common randomness r, as well as past measurements y^{t-1}. The choice of alphabet $\mathcal{W}_t$ is part of the protocol design.

At the end of time step T, *when no further public communication happens*, Eve performs a measurement on her state $\rho^{\mathbf{E}}$, as an attempt to detect the communication and obtain information about the secret key, while Alice and Bob use all their available information and randomness to compute two long binary strings s^X and s^Y, respectively, as well as the number of bits ℓ^X and ℓ^Y, respectively, to use as a secret key. The length of s^X and s^Y is public and fixed at the beginning of the protocol. Alice finally sets her key k^X to be the first ℓ^X bits of s^X while Bob sets his key k^Y to be the first ℓ^Y bits of s^Y.

A protocol is called an (ϵ, δ, μ) protocol if the following properties hold. Let W, S^X, S^Y, K^X, and K^Y be the random variables representing the total public communication, Alice's random string, Bob's random string, Alice's key, and Bob's key, respectively. We require the following: (1) ϵ reliability—$P_e \triangleq \mathbb{P}(K^X \neq K^Y) \leqslant \epsilon$, which implicitly includes the condition $\ell^X = \ell^Y$; (2) δ secrecy—$S \triangleq \mathbb{D}(\rho^{\mathbf{E}WS^X} \| \rho^{\mathbf{E}W} \otimes \rho_{\text{unif}}^{S^X}) \leqslant \delta$, where $\rho^{\mathbf{E}WS^X}$ is the joint density matrix of the eavesdropper's observations, public messages, and Alice's random string and $\rho_{\text{unif}}^{S^X}$ is a mixed state for S^X corresponding to a uniform distribution; and (3) μ covertness—$C \triangleq \mathbb{D}(\rho^{\mathbf{E}W} \| (\rho_0^{\mathbf{E}}) \otimes \rho_{\text{unif}}^W) \leqslant \mu$, where $\rho_0^{\mathbf{E}}$ is the density matrix of the eavesdropper's observations when no communication takes place and ρ_{unif}^W is a mixed state for W corresponding to a uniform distribution on $\times_t \mathcal{W}_t$.

A protocol is *efficient* if it allows key expansion so that the number of key bits created exceeds the number of common randomness bits consumed. Our goal is to analyze under what conditions efficient (ϵ, μ, δ) protocols might exist.

A couple of remarks are in order regarding our protocol definition. Note that the choice of the key length is a part of the protocol. However, δ secrecy requires the string S^X to be secret and not just K^X. This is merely enforced for technical reasons, so that the relative entropy is a deterministic quantity irrespective of the length of the key. Since ϵ reliability only applies to the bits of K^X, Alice can always generate the remaining bits of S^X independently and uniformly at random using her local randomness, so that our definition does not incur any loss of generality. By convention, we assume that the public communication is not by itself a proof of communication. Instead, μ covertness only requires that the public bits look uniformly distributed and do not reveal communication on the quantum channel. We point out that δ secrecy and μ covertness are "one-shot" guarantees, in the sense that they only ensure a low probability of detection for a single execution of the protocol. In fact, by repeating the protocol k consecutive and independent times, a (ϵ, δ, μ) protocol gives rise to a $(k\epsilon, k\delta, k\mu)$ protocol. Additional postprocessing can reduce the constant $k\epsilon$ and $k\delta$ but cannot affect the constant $k\mu$. This suggests that the protocol should be designed for small values of μ and large values of T. Finally, the particular choice of the quantum state ρ_{unif}^W in the definition of covertness plays no role in our proofs. As long as there exists a specific state corresponding to no communication for the public communication, our proof holds and leads to a covert and secret key generation scheme.

IV. COVERT AND SECRET KEY GENERATION OVER A KNOWN cq CHANNEL

We address the situation in which the cq wiretap channels are *fixed* and known ahead of time, and in which the adversary is *passive*. Our analysis corresponds to "known collective attacks." In this special case, the length of the key can be computed ahead of time, and there is no need to distinguish between the random strings S^X and S^Y and the keys K^X and K^Y. Furthermore, it becomes possible to define a notion of covert and secret key capacity as follows. A throughput Θ is achievable if there exists a sequence of $(\epsilon_T, \delta_T, \mu_T)$ protocols generating ℓ_T bits of the secret key while consuming r_T bits of the secret key over T stages and such that

$$\lim_{T\to\infty} \epsilon_T = \lim_{T\to\infty} \delta_T = \lim_{T\to\infty} \mu_T = 0, \tag{5}$$

$$\ell_T = \omega(\ln T), \tag{6}$$

$$\text{and } \lim_{T\to\infty} \frac{\ell_T - r_T}{\sqrt{T\mu_T}} \geqslant \Theta. \tag{7}$$

The supremum of all achievable throughputs is called the *covert and secret key capacity* and denoted C_{qck}. Note that the definition of the throughput already captures the scaling of the throughput with the square root of the number of channel uses, $\sqrt{T}$. The scaling is justified *a posteriori* by our analysis that shows that C_{qck} is lower bounded by a constant that only depends on the channel parameters. The unit of C_{qck} is therefore in nats per channel use. Our main results are lower bounds on the covert capacity obtained by showing the existence of sequences of covert secret key generation protocols using reverse or forward reconciliation.

To analyze the performance of protocols with forward reconciliation, we build upon existing results for covert communication over cq channels [13,14] with appropriate extensions to guarantee secrecy. The innovative principle of our approach is best highlighted for protocols with reverse reconciliation as follows. In a first phase, Alice transmits a sequence of independent and identically distributed (iid) symbols $\mathbf{X}$ distributed according to a Bernoulli(α_T) distribution over the cq channel, where $\alpha_T \in \omega((\frac{\ln T}{T})^{\frac{2}{3}}) \cap o(\frac{1}{\sqrt{T}})$. Intuitively, the choice of $\{\alpha_T\}_{T\geqslant 1}$ must ensure that $\mathbf{X}$ is sparse, so that the warden cannot suspect the existence of information symbols, but not so sparse that Alice and Bob cannot extract a long enough key from their observation. We shall show that our choice of $\{\alpha_T\}_{T\geqslant 1}$ simultaneously satisfies both requirements. In a second phase, Bob measures his received quantum states in some basis and, based on the output of the measurements, generates two messages W and K, representing public information reconciliation and secret key, respectively. Bob subsequently sends W through the public channel, and Alice recovers K using W and $\mathbf{X}$. Although the second phase of the protocol seems deceptively similar to a standard application of information reconciliation and privacy amplification, there exists a technical difficulty because of the specific distributions of Alice's and Bob's observations, which precludes the use of standard tools. Specifically, consider the classical channel $W_{Y|X}$ and suppose that $\mathbf{Y}$ is the output of the channel to the input $\mathbf{X}$. The standard finite-length analysis of reconciliation requires the second-order penalty γ_T to satisfy [20]

$$\lim_{T\to\infty} \mathbb{P}\left(\sum_{i=1}^{T}\left(\ln\frac{1}{W_{Y|X}(Y_i|X_i)} - \mathbb{H}(Y_i|X_i)\right) \geqslant \gamma_T\right) = 0. \quad (8)$$

By the Central Limit Theorem, this also requires that $\gamma_T^2 = \omega(\sum_{i=1}^{T}\mathrm{Var}(\frac{1}{W_{Y|X}(Y_i|X_i)}))$. For our specific choice of α_T, one can check that $\mathrm{Var}(\frac{1}{W_{Y|X}(Y_i|X_i)}) = \Omega(1)$ so that the second-order penalty satisfies $\gamma_T = \omega(\sqrt{T})$. A similar reasoning holds for privacy amplification, which prevents us from establishing the desired first-order scaling of $o(\sqrt{T})$. We circumvent this difficulty by resorting to a technique called *likelihood encoder* [21], in which the encoders used to generate W and K are derived from different principles. In particular, the analysis of the likelihood encoder only requires the use of quantities depending on mutual information (instead of conditional entropy), which has the same scaling as the number of bits generated by a covert protocol. As we shall see later, instead of (8), the finite-length analysis of the likelihood encoder only requires the second-order penalty γ_T to satisfy

$$\lim_{T\to\infty} \mathbb{P}\left(\sum_{i=1}^{T}\left(\ln\frac{W_{Y|X}(Y_i|X_i)}{P_Y(Y_i)} - \mathbb{I}(X_i;Y_i)\right) \geqslant \gamma_T\right) = 0. \quad (9)$$

By the Central Limit Theorem, this now requires that $\gamma_T^2 = \omega(\sum_{i=1}^{T}\mathrm{Var}(\ln\frac{W_{Y|X}(Y_i|X_i)}{P_Y(Y_i)}))$. By our specific choice of α_T, one can check that $\mathrm{Var}(\ln\frac{W_{Y|X}(Y_i|X_i)}{P_Y(Y_i)}) = O(\alpha_T)$, which leads to $\gamma_T = \omega(\sqrt{T\alpha_T})$. The second-order penalty is now conveniently dominated by the first-order term $\sum_{i=1}^{T}\mathbb{I}(X_i;Y_i)$ which is of the order of $\Omega(T\alpha_T)$.

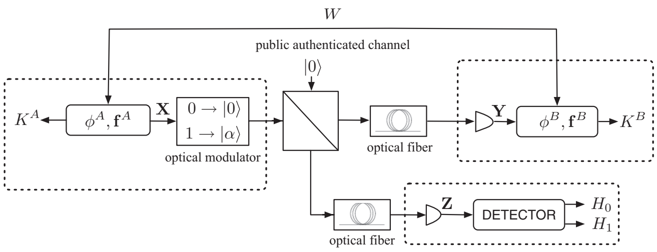

FIG. 2. Simplified model of a lossy bosonic channel.

The analysis of protocols with forward and reverse reconciliation leads to Theorem 1 below, the proof of which is given in Appendix A.

Theorem 1. Let $\{|y\rangle^B\}$ be any orthonormal basis for $\mathcal{H}^B$, and define $\widetilde{\rho}_x^{BE} \triangleq \sum_y (|y\rangle\langle y|^B \otimes I^E)\rho_x^{BE}(|y\rangle\langle y|^B \otimes I^E)$. Assume that $\mathcal{H}^B$ and $\mathcal{H}^E$ have finite dimension and $0 < \chi_2(\widetilde{\rho}_1^E\|\widetilde{\rho}_0^E) < \infty$. We have

$$C_{\mathrm{qck}} \geqslant \sqrt{\frac{2}{\chi_2(\widetilde{\rho}_1^E\|\widetilde{\rho}_0^E)}}\left(\mathbb{D}(\widetilde{\rho}_1^B\|\widetilde{\rho}_0^B) - \mathbb{D}(\widetilde{\rho}_1^E\|\widetilde{\rho}_0^E)\right), \quad (10)$$

and if $\widetilde{\rho}_0^{BE} = \widetilde{\rho}_0^B \otimes \widetilde{\rho}_0^E$ then

$$\begin{aligned} C_{\mathrm{qck}} \geqslant \sqrt{\frac{2}{\chi_2(\widetilde{\rho}_1^E\|\widetilde{\rho}_0^E)}}\Big(&\mathbb{D}(\widetilde{\rho}_1^{BE}\|\widetilde{\rho}_0^{BE}) - \mathbb{D}(\widetilde{\rho}_1^E\|\widetilde{\rho}_0^E) \\ &- \mathbb{D}(\widetilde{\rho}_1^{BE}\|\widetilde{\rho}_1^B \otimes \widetilde{\rho}_1^E)\Big), \end{aligned} \quad (11)$$

which simplifies when $\widetilde{\rho}_1^{BE} = \widetilde{\rho}_1^B \otimes \widetilde{\rho}_1^E$ as

$$C_{\mathrm{qck}} \geqslant \sqrt{\frac{2}{\chi_2(\widetilde{\rho}_1^E\|\widetilde{\rho}_0^E)}}\,\mathbb{D}(\widetilde{\rho}_1^B\|\widetilde{\rho}_0^B). \quad (12)$$

In addition, the lower bound in (10) is achieved without public communication using covert communication codes for cq channels [14] combined with wiretap coding techniques [11] while the lower bound in (11) is achieved with reverse reconciliation on the public channel.

While this result does not hold for the most general quantum setting, note that the covert secret key throughputs predicted hold with a precise definition of covertness that explicitly includes the public communication and demonstrate the existence of efficient protocols that allow key expansion. Perhaps more importantly, as apparent in the proof of the result, such protocols do *not* rely on a secret key to determine the instances in which Alice transmits nonzero states; in contrast, our proof shows the existence of reconciliation and key-extraction algorithms capable of *extracting* the diffuse secret correlations created by Alice's sparse transmission of noninnocent states. We finally point out that for $\widetilde{\rho}_1^{BE} = \widetilde{\rho}_1^B \otimes \widetilde{\rho}_1^E$ secrecy comes *almost for free* as the information leakage to Eve is asymptotically dominated by the information shared between Alice and Bob in reverse reconciliation.

As an illustration, we consider the situation depicted in Fig. 2 in which the input port of a balanced beam splitter is in control of Alice while Bob and Eve are each connected to one of the output ports through optical fibers of length d_{AB}

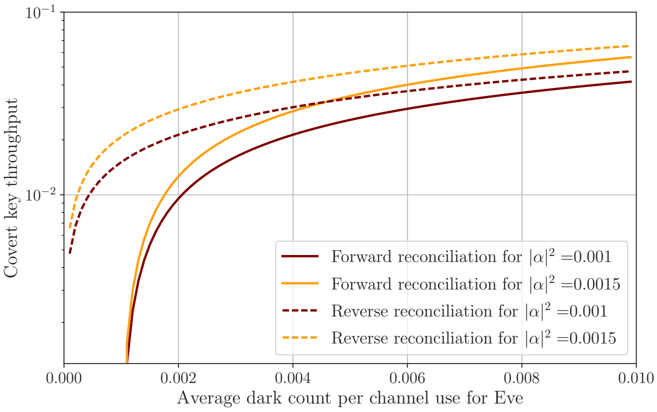

FIG. 3. Covert and secret key generation throughput as a function of Eve's dark count rate.

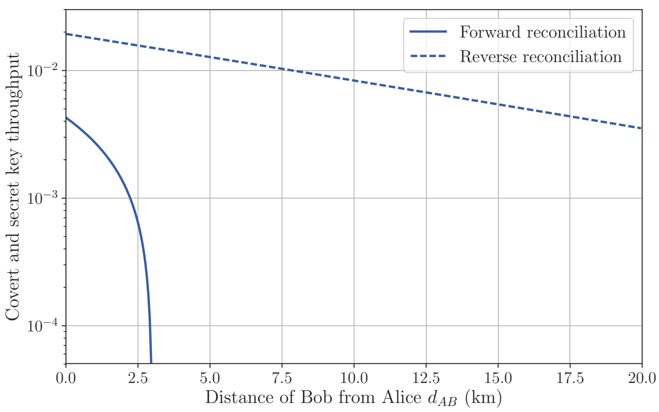

FIG. 4. Covert and secret key generation throughput for a lossy bosonic channel.

and d_{AE}, respectively, and loss γ dB/km. We further assume that the second input port is in the vacuum state, and that Alice uses the vacuum state $|0\rangle$ and a coherent state $|\alpha\rangle$ as the innocent and the information symbol, respectively. Bob and Eve measure their output ports with photodetectors to count the number of photons at each channel use. The photodetectors suffer from dark count that is beneficial for covert communication since detection of photons at Eve does not necessarily imply the existence of communication. Let η_B and η_E be Bob's and Eve's photodetector efficiencies, respectively, and let λ_B and λ_E be Bob's and Eve's photodetector dark count rates, respectively. The achievable covert and secret key throughputs can be obtained by substituting the quantities

$$\widetilde{\eta}_B \triangleq \eta_B 10^{-\frac{d_{AB}\gamma}{10}}, \tag{13}$$

$$\widetilde{\eta}_E \triangleq \eta_E 10^{-\frac{d_{AE}\gamma}{10}}, \tag{14}$$

$$\chi_2\big(\widetilde{\rho}_1^E \big\| \widetilde{\rho}_0^E\big) = e^{\frac{(\lambda_E+|\alpha|^2\widetilde{\eta}_E)^2}{\lambda_E}-\lambda_E+2|\alpha|^2\widetilde{\eta}_E}, \tag{15}$$

$$\mathbb{D}\big(\widetilde{\rho}_1^B \big\| \widetilde{\rho}_0^B\big) = (\lambda_B + |\alpha|^2\widetilde{\eta}_B)\ln(\lambda_B + |\alpha|^2\widetilde{\eta}_B) - |\alpha|^2\widetilde{\eta}_B, \tag{16}$$

$$\mathbb{D}\big(\widetilde{\rho}_1^E \big\| \widetilde{\rho}_0^E\big) = (\lambda_E + |\alpha|^2\widetilde{\eta}_E)\ln(\lambda_E + |\alpha|^2\widetilde{\eta}_E) - |\alpha|^2\widetilde{\eta}_E \tag{17}$$

in (10) and (12) for forward and reverse reconciliation, respectively. Note that the output states of this channel belong to infinite-dimensional spaces and, strictly speaking, one cannot directly apply Theorem 1. Nevertheless, since for the number states $\{|n\rangle\}_{n\geqslant 0}$, $\langle n|\rho|n\rangle$ decays exponentially for all output states ρ, one can construct a sequence of channels with finite-dimensional output states for which the quantities used in (10) and (12), as well as the performance of any covert and secret key generation protocol, tend to those of the original channel.

We illustrate in Fig. 3 the achievable covert and secret key throughput as a function of Eve's photodetector dark count rate λ_E for $\gamma = 0.2$ dB/km, $\eta_B = \eta_E = 0.97$, $\lambda_B = 0.001$, and $d_{AB} = d_{AE} = 3$ km. In Fig. 4, we also illustrate the achievable covert and secret key throughput as a function of the distance of Bob to Alice d_{AB} for $|\alpha|^2 = 0.001$, $\gamma = 0.2$ dB/km, $\eta_B = \eta_E = 0.97$, $\lambda_B = \lambda_E = 0.001$, and $d_{AE} = 3$ km. As expected, the secret and covert key throughputs are orders of magnitude lower than their counterparts without covertness constraint. This is an unfortunate but unavoidable byproduct of the covertness constraint, which severely limits how many useful bits can be embedded in transmitted signals.

V. DISCUSSION AND FUTURE WORK

We have introduced a comprehensive framework in which to analyze the possibility of covert quantum key generation. In the special case of cq wiretap channels, for which the adversary's attack is known, we have established two lower bounds on the optimal covert throughput of key generation based on forward and reverse reconciliation. While our results suggest that covert key expansion is possible over quantum channels, several lingering questions remain to be explored before envisioning an actual practical demonstration of covert quantum key distribution. This includes, in particular, extending our results to more general attacks with fewer assumptions regarding Eve's abilities, extending the analysis to infinite-dimensional systems that are closer to current technological implementations, and designing efficient coding schemes with provable finite length performance. With respect to the latter, an explicit construction of covert communication codes over classical channels has been recently developed [19], which provides a promising lead to design codes for the framework proposed in the present paper.

ACKNOWLEDGMENT

This work was supported in part by NSF Grant No. 1527074.

APPENDIX A: PROOF OF THEOREM 1

We prove Theorem 1 by generalizing the proof of Theorem 1 from [22] to the quantum setting. The most challenging part of this generalization is to establish a channel resolvability result for cq channels for distributions suitable for covert communications. We first introduce some preliminary concepts regarding covert communications mostly borrowed from [11]. We also note that the use of standard proof techniques for secret key generation such as source coding with side information and privacy amplification is challenging for covert communication as discussed in Sec. IV. We therefore resort to the likelihood encoder technique [21] in which we first define an auxiliary problem that can be analyzed using channel coding approaches, for which designing a code for the main problem is reduced to the design of code for the auxiliary problem.

1. Preliminaries

We define here required quantities used for our achievability proof. Suppose Alice sends iid symbols through her cq channel $x \mapsto \rho_x^{BE}$ with each symbol distributed according to $Q_X \sim \text{Bernoulli}(\alpha_T)$ for $\alpha_T \in (0,1)$. Upon receiving each state, Bob makes a measurement in a fixed orthonormal basis $\{|y\rangle^B\}$ for $\mathcal{H}^B$ to obtain a classical symbol y. In the following, we define equivalent cq channels from Bob to Alice and Eve that result in the same joint state for the three parties.

Definition 1. Let $\alpha_T \in [0,1]$. We define

$$Q_{Y|X}(y|x) \triangleq \langle y|^B \rho_x^B |y\rangle^B, \tag{A1}$$

$$\widetilde{\rho}_x^{BE} \triangleq \sum_y (|y\rangle\langle y|^B \otimes I^E)\rho_x^{BE}(|y\rangle\langle y|^B \otimes I^E), \tag{A2}$$

$$\widetilde{\rho}^{ABE} \triangleq \sum_x Q_X(x)|x\rangle\langle x|^A \otimes \widetilde{\rho}_x^{BE}, \tag{A3}$$

$$\widetilde{\rho}_{x,y}^{E} \triangleq \frac{\mathrm{tr}_B((|y\rangle\langle y|^B \otimes I^E)\rho_x^{BE}(|y\rangle\langle y|^B \otimes I^E))}{Q_{Y|X}(y|x)}, \tag{A4}$$

$$\widetilde{\rho}_y^{AE} \triangleq \sum_x Q_{X|Y}(x|y)|x\rangle\langle x|^A \otimes \widetilde{\rho}_{x,y}^{E}. \tag{A5}$$

Note that the state $\widetilde{\rho}^{ABE}$ is the joint state of all parties after Bob's measurement, which is classical for both Alice and Bob, and $\widetilde{\rho}_x^{BE}$, $\widetilde{\rho}_y^{AE}$, and $\widetilde{\rho}_{x,y}^{E}$ are the corresponding conditional quantum states.

The following lemma establishes useful properties of ρ_0^{BE} under the assumption $\widetilde{\rho}_0^{BE} = \widetilde{\rho}_0^{B} \otimes \widetilde{\rho}_0^{E}$.

Lemma 1. If $\widetilde{\rho}_0^{BE} = \widetilde{\rho}_0^{B} \otimes \widetilde{\rho}_0^{E}$ then, for all y, it holds that $\widetilde{\rho}_{0,y}^{E} = \widetilde{\rho}_0^{E}$. Furthermore, we have

$$\begin{aligned} I(Q_Y, \widetilde{\rho}_y^E) = \alpha_T \big(&\mathbb{D}(\widetilde{\rho}_1^B \| \widetilde{\rho}_0^B) + \mathbb{D}(\widetilde{\rho}_1^E \| \widetilde{\rho}_0^E) - \mathbb{D}(\widetilde{\rho}_1^{BE} \| \widetilde{\rho}_0^{BE}) \\ &+ \mathbb{D}(\widetilde{\rho}_1^{BE} \| \widetilde{\rho}_1^{B} \otimes \widetilde{\rho}_1^{E})\big) + O(\alpha_T^2). \end{aligned} \tag{A6}$$

Proof. By the spectral decomposition theorem, there exist orthonormal bases $\{|y\rangle^B\}$ and $\{|z\rangle^E\}$ for $\mathcal{H}^B$ and $\mathcal{H}^E$, respectively, such that

$$\widetilde{\rho}_0^B = \sum_y \lambda_y |y\rangle\langle y|^B, \tag{A7}$$

$$\widetilde{\rho}_0^E = \sum_z \lambda_z |z\rangle\langle z|^E, \tag{A8}$$

$$\widetilde{\rho}_0^{BE} = \sum_{y,y',z,z'} \lambda_{yy'zz'} |y\rangle\langle y'|^B \otimes |z\rangle\langle z'|^E. \tag{A9}$$

Our assumption that $\widetilde{\rho}_0^{BE} = \widetilde{\rho}_0^{B} \otimes \widetilde{\rho}_0^{E}$ implies that $\lambda_{yy'zz'} = \lambda_y\lambda_z\mathbb{1}\{y=y', z=z'\}$. Furthermore, for any y, we have by definition

$$\widetilde{\rho}_{0,y}^{E} \triangleq \frac{\mathrm{tr}_B((|y\rangle\langle y|^B \otimes I^E)\rho_0^{BE}(|y\rangle\langle y|^B \otimes I^E))}{Q_{Y|X}(y|0)} \tag{A10}$$

$$\begin{aligned} &= \frac{1}{Q_{Y|X}(y|0)}\mathrm{tr}_B\Bigg((|y\rangle\langle y|^B \otimes I^E) \\ &\quad \times \Bigg(\sum_{y',z'} \lambda_{y'}\lambda_{z'} |y'\rangle\langle y'|^B \otimes |z'\rangle\langle z'|^E\Bigg) \\ &\quad \times (|y\rangle\langle y|^B \otimes I^E)\Bigg) \end{aligned} \tag{A11}$$

$$= \frac{\mathrm{tr}_B\big(\sum_{z'} \lambda_y\lambda_{z'} |y\rangle\langle y|^B \otimes |z'\rangle\langle z'|^E\big)}{Q_{Y|X}(y|0)} \tag{A12}$$

$$= \frac{\lambda_y}{Q_{Y|X}(y|0)} \sum_{z'} \lambda_{z'} |z'\rangle\langle z'|^E \tag{A13}$$

$$= \frac{\lambda_y}{Q_{Y|X}(y|0)} \widetilde{\rho}_0^E. \tag{A14}$$

We also know that $\mathrm{tr}(\widetilde{\rho}_0^E) = \mathrm{tr}(\widetilde{\rho}_{0,y}^E) = 1$, which together with (A14) yields $\widetilde{\rho}_0^E = \widetilde{\rho}_{0,y}^E$.

To prove (A6), notice that

$$\begin{aligned} I(Q_Y, \widetilde{\rho}_y^E) &= \mathbb{I}(B;E)_{\widetilde{\rho}} \\ &= \mathbb{I}(A;B)_{\widetilde{\rho}} + \mathbb{I}(A;E)_{\widetilde{\rho}} - \mathbb{I}(A;BE)_{\widetilde{\rho}} + \mathbb{I}(B;E|A)_{\widetilde{\rho}}. \end{aligned} \tag{A15}$$

Moreover, for $\widetilde{\rho}_{\alpha_T}^B \triangleq (1-\alpha_T)\widetilde{\rho}_0^B + \alpha_T\widetilde{\rho}_1^B$, we can write

$$\mathbb{I}(A;B)_{\widetilde{\rho}} \tag{A16}$$

$$= H(\widetilde{\rho}_{\alpha_T}^B) - (1-\alpha_T)H(\widetilde{\rho}_0^B) - \alpha_T H(\widetilde{\rho}_1^B) \tag{A17}$$

$$\begin{aligned} &= -\mathrm{tr}\big(\widetilde{\rho}_{\alpha_T}^B \ln(\widetilde{\rho}_{\alpha_T}^B) - (1-\alpha_T)\widetilde{\rho}_0^B \ln(\widetilde{\rho}_0^B) \\ &\quad - \alpha_T\widetilde{\rho}_1^B \ln(\widetilde{\rho}_1^B)\big) \end{aligned} \tag{A18}$$

$$\begin{aligned} &= -\mathrm{tr}\big(\widetilde{\rho}_{\alpha_T}^B (\ln(\widetilde{\rho}_{\alpha_T}^B) - \ln(\widetilde{\rho}_0^B) + \ln(\widetilde{\rho}_0^B)) \\ &\quad - (1-\alpha_T)\widetilde{\rho}_0^B \ln(\widetilde{\rho}_0^B) - \alpha_T\widetilde{\rho}_1^B \ln(\widetilde{\rho}_1^B)\big) \end{aligned} \tag{A19}$$

$$\begin{aligned} &= -\mathrm{tr}\big(\widetilde{\rho}_{\alpha_T}^B (\ln\widetilde{\rho}_{\alpha_T}^B - \ln\widetilde{\rho}_0^B) \\ &\quad - \alpha_T\widetilde{\rho}_1^B (\ln\widetilde{\rho}_1^B - \ln\widetilde{\rho}_0^B)\big) \end{aligned} \tag{A20}$$

$$= \alpha_T\mathbb{D}(\widetilde{\rho}_1^B \| \widetilde{\rho}_0^B) - \mathbb{D}(\widetilde{\rho}_{\alpha_T}^B \| \widetilde{\rho}_0^B) \tag{A21}$$

$$\overset{(a)}{=} \alpha_T\mathbb{D}(\widetilde{\rho}_1^B \| \widetilde{\rho}_0^B) + O(\alpha_T^2), \tag{A22}$$

where (a) follows from Eq. (19) of [14]. Similarly, we obtain

$$\mathbb{I}(A;E)_{\widetilde{\rho}} = \alpha_T\mathbb{D}(\widetilde{\rho}_1^E \| \widetilde{\rho}_0^Z) + O(\alpha_T^2), \tag{A23}$$

$$\mathbb{I}(A;BE)_{\widetilde{\rho}} = \alpha_T\mathbb{D}(\widetilde{\rho}_1^{BE} \| \widetilde{\rho}_0^{BE}) + O(\alpha_T^2). \tag{A24}$$

Since X is classical, Eq. (11.92) of [23] yields

$$\mathbb{I}(B;E|Ax)_{\widetilde{\rho}} = (1-\alpha_T)\mathbb{I}(B;E)_{\widetilde{\rho}_0} + \alpha_T\mathbb{I}(B;E)_{\widetilde{\rho}_1} \tag{A25}$$

$$\overset{(a)}{=} \alpha_T\mathbb{I}(B;E)_{\widetilde{\rho}_1} \tag{A26}$$

$$= \alpha_T\mathbb{D}(\widetilde{\rho}_1^{BE} \| \widetilde{\rho}_1^B \otimes \widetilde{\rho}_1^E), \tag{A27}$$

where (a) follows from our assumption that $\widetilde{\rho}_0^{BE} = \widetilde{\rho}_0^{B} \otimes \widetilde{\rho}_0^{E}$. This completes the proof of (A6). ■

2. One-shot results

We recall here one-shot results for classical channel coding and classical channel resolvability (Lemma 2) and quantum channel resolvability (Lemma 3) that play a central role in our analysis. Given a classical channel $(\mathcal{X}, W_{Y|X}, \mathcal{Y})$, a message W uniformly distributed over $[\![1,M]\!]$, and an encoder $f : [\![1,M]\!] \to \mathcal{X}$, let $\widehat{P}_{WXY}(w,x,y) \triangleq \frac{1}{M}\mathbb{1}\{f(w)=x\}W_{Y|X}(y|x)$ be the induced probability mass function (PMF) of W, X, and Y, and let $\widehat{W} \triangleq \arg\max_{w\in[\![1,M]\!]} W_{Y|X}(Y|f(w))$ be the maximum likelihood decoder at the output.

Lemma 2 (one-shot bounds). If F is a random encoder such that $\{F(w)\}_{w\in[\![1,M]\!]}$ are iid according to a distribution P_X over $\mathcal{X}$, then for any $\gamma \in \mathbb{R}$ we have

$$\mathbb{E}_F(\mathbb{P}(\widehat{W} \neq W)) \leqslant \mathbb{P}_{P_X\times W_{Y|X}}\left(\ln \frac{W_{Y|X}(Y|X)}{(W_{Y|X}\circ P_X)(Y)} \leqslant \gamma\right) + \frac{M}{2^\gamma} \tag{A28}$$

and

$$\mathbb{E}_F(\mathbb{V}(\widehat{P}_Y; W_{Y|X}\circ P_X)) \leqslant \mathbb{P}_{P_X\times W_{Y|X}}\left(\ln \frac{W_{Y|X}(Y|X)}{(W_{Y|X}\circ P_X)(Y)} \geqslant \gamma\right) + \sqrt{\frac{2^\gamma}{M}}, \tag{A29}$$

where $(W_{Y|X}\circ P_X)(y) \triangleq \sum_x P_X(x)W_{Y|X}(y|x)$.

Proof. See [20] for (A28) and [24] for (A29). ■

Let $y \mapsto \rho_y$ denote a cq channel and let P_Y be a PMF over $\mathcal{Y}$. If $\overline{\rho} \triangleq \sum_y P_Y(y)\rho_y$, our objective is to find an encoder $f : [\![1,M]\!] \to \mathcal{Y}$ such that $\|\overline{\rho} - \widehat{\rho}\|_1$ is small, where $\widehat{\rho} \triangleq \frac{1}{M}\sum_{i=1}^M \rho_{f(i)}$.

Lemma 3. If $F : [\![1,M]\!] \to \mathcal{Y}$ is a random encoder the codewords of which are iid according to P_Y, then for all $s \leqslant 0$ and γ we have

$$\mathbb{E}_F(\|\overline{\rho} - \widehat{\rho}\|_1) \leqslant 2\sqrt{2^{\gamma s+\phi(s)}} + \sqrt{\frac{2^\gamma \nu}{M}}, \tag{A30}$$

where $\phi(s) \triangleq \ln\left(\sum_y P_Y(y)\mathrm{tr}(\rho_y^{1-s}\overline{\rho}^s)\right)$ and ν is the number of distinct eigenvalues of $\overline{\rho}$.

Proof. See Lemma 9.2 of [25]. ■

3. An auxiliary problem

To show the existence of good codes for our main problem, we use the likelihood encoder technique [21] and, in particular, define an auxiliary problem for which we can exploit channel coding instead of source coding. We then show how these two problems are related in Appendix A 4. Consider a cq channel $y \mapsto \widetilde{\rho}_y^{AE}$ from Bob to Alice and Eve as in Definition 1. Bob encodes three uniformly distributed messages $W_1 \in [\![1,M_1]\!]$, $W_2 \in [\![1,M_2]\!]$, and $W_3 \in [\![1,M_3]\!]$ into a codeword $\mathbf{Y}$ using an encoder $f : [\![1,M_1]\!] \times [\![1,M_2]\!] \times [\![1,M_3]\!] \to \mathcal{Y}^T$, transmits the codeword $\mathbf{Y}$ over the cq channel, and sends W_2 publicly. Alice subsequently performs a measurement on her received state $\rho_{\mathbf{Y}}^A$ in a fixed basis $\{|x\rangle\}$ to obtain $\mathbf{X}$, and uses $\mathbf{X}$ and W_2 to decode W_1 as $\widehat{W}_1$. If $P_{\mathbf{Y}}^a$ denotes the induced PMF of $\mathbf{Y}$, and $\rho_a^{\mathbf{ABE}W_1W_2W_3\widehat{W}_1}$ is the joint state in the auxiliary problem, our objective is to ensure that $\mathbb{P}(\widehat{W}_1 \neq W_1)$, $\mathbb{V}(P_{\mathbf{Y}}^a; Q_Y^{\otimes T})$, and $\|\rho^{\mathbf{E}W_1W_2} - \rho^{\mathbf{E}} \otimes \rho^{W_1W_2}\|_1$ are small.

Lemma 4. If for some $\zeta > 0$

$$\ln M_3 = \lfloor (1+\zeta)I(Q_Y, \widetilde{\rho}_y^E)T \rfloor, \tag{A31}$$

$$\ln M_1 + \ln M_2 + \ln M_3 = \lceil (1+\zeta)H(Q_Y)T \rceil, \tag{A32}$$

$$\ln M_1 + \ln M_3 = \lfloor (1-\zeta)I(Q_Y, Q_{X|Y})T \rfloor, \tag{A33}$$

then there exists a sequence of codes and a positive constant ξ such that

$$\mathbb{P}(\widehat{W}_1 \neq W_1) \leqslant 2^{-\xi\alpha_T T}, \tag{A34}$$

$$\mathbb{V}\left(P_{\mathbf{Y}}^a; Q_Y^{\otimes T}\right) \leqslant 2^{-\xi T}, \tag{A35}$$

$$\|\rho^{\mathbf{E}W_1W_2} - \rho^{\mathbf{E}} \otimes \rho^{W_1W_2}\|_1 \leqslant 2^{-\omega(\ln T)}. \tag{A36}$$

Proof. Let $F : [\![1,M_1]\!] \times [\![1,M_2]\!] \times [\![1,M_3]\!]$ be a random encoder the codewords of which are drawn independently according to $Q_Y^{\otimes T}$. By construction, Alice can assume that each symbol X_i is received as the output of a Discrete Memoryless Channel $(\mathcal{Y}, Q_{X|Y}, \mathcal{X})$ with input Y_i, and, therefore, Lemma 2 implies that

$$\begin{aligned}\mathbb{E}_F(\mathbb{P}(\widehat{W}_1 \neq W_1)) &= \frac{1}{M_2}\sum_{w_2}\mathbb{E}_F(\mathbb{P}(\widehat{W}_1 \neq W_1|W_2 = w_2))\\ &\overset{(a)}{\leqslant} \mathbb{P}_{Q_{X|Y}^{\otimes T}\times Q_Y^{\otimes T}}\left(\sum_{t=1}^T \ln\frac{Q_{X|Y}(X_t|Y_t)}{Q_X(X_t)} \leqslant \gamma\right)\\ &\quad + \frac{M_1M_3}{2^\gamma}\\ &= \mathbb{P}_{Q_{XY}^{\otimes T}}\left(\sum_{t=1}^T \ln\frac{Q_{Y|X}(Y_t|X_t)}{Q_Y(Y_t)} \leqslant \gamma\right)\\ &\quad + \frac{M_1M_3}{2^\gamma},\end{aligned} \tag{A37}$$

where (a) follows from applying Lemma 2 to the subcodebook $\{F(w_1,w_2,w_3) : w_1 \in [\![1,M_1]\!], w_3 \in [\![1,M_3]\!]\}$ for a particular w_2. By choosing

$$\ln M_1 + \ln M_3 = \lfloor (1-\zeta)I(Q_X, Q_{Y|X})T \rfloor, \tag{A38}$$

$$\gamma = \left(1 - \frac{\zeta}{2}\right)I(Q_X, Q_{Y|X})T, \tag{A39}$$

and using Bernstein's inequality [26], we obtain

$$\begin{aligned}&\mathbb{P}_{Q_{XY}^{\otimes T}}\left(\sum_{t=1}^T \ln\frac{Q_{Y|X}(Y_t|X_t)}{Q_Y(Y_t)} \leqslant \gamma\right) + \frac{M_1M_3}{2^\gamma}\\ &\leqslant \exp\left(-\frac{-\frac{1}{8}\zeta^2 I(Q_Y, Q_{X|Y})^2 T}{\mathrm{Var}\left(\ln\frac{Q_{Y|X}(Y|X)}{Q_Y(Y)}\right) + \frac{1}{3}C_3\zeta\,\mathbb{I}(X;Y)}\right)\\ &\quad + 2^{-\frac{\zeta}{2}\mathbb{I}(X;Y)T} \leqslant 2^{-\xi\alpha_T T},\end{aligned} \tag{A40}$$

for some $\xi > 0$. Next, by using Lemma 2 for the channel $(\mathcal{Y}, Q_{Y'|Y}, \mathcal{Y})$ with $Q_{Y'|Y}(y'|y) \triangleq \mathbb{1}\{y' = y\}$ and the distribution Q_Y, we obtain

$$\mathbb{E}_F\left(\mathbb{V}\left(P_{\mathbf{Y}}^a; Q_Y^{\otimes T}\right)\right) \leqslant \mathbb{P}_{Q_Y^{\otimes T}}\left(\sum_{t=1}^T \ln\frac{1}{Q_Y(Y_t)} \geqslant \gamma\right) + \sqrt{\frac{2^\gamma}{M_1M_2M_3}}. \tag{A41}$$

By choosing

$$\ln M_1 + \ln M_2 + \ln M_3 = \lceil (1+\zeta)\mathbb{H}(Y)T \rceil, \tag{A42}$$

$$\gamma = \left(1 + \frac{\zeta}{2}\right)\mathbb{H}(Y)T \tag{A43}$$

and using Hoeffding's inequality [27], with $\mu_Y \triangleq \min_{y:Q_Y(y)>0} Q_Y(y)$, we obtain

$$\begin{aligned}&\mathbb{P}_{Q_Y^{\otimes T}}\left(\sum_{t=1}^{T} \ln \frac{1}{Q_Y(Y_t)} \geqslant \gamma\right) + \sqrt{\frac{2^\gamma}{M_1M_2M_3}}\\ &\leqslant \exp\left(-\frac{\zeta^2\mathbb{H}(Y)^2T}{2\ln^2(\mu_Y)}\right) + 2^{-\frac{\zeta}{2}\mathbb{H}(Y)T} \leqslant 2^{-\xi T},\end{aligned} \tag{A44}$$

for $\xi > 0$ small enough.

Since W_1 and W_2 are classical, we can write

$$\rho^{W_1W_2\mathbf{E}} = \frac{1}{M_1M_2}\sum_{w_1,w_2} |w_1w_2\rangle\langle w_1w_2| \otimes \rho^{\mathbf{E}}_{w_1w_2}. \tag{A45}$$

To upper bound $\mathbb{E}_F(\|\rho^{\mathbf{E}W_1W_2} - \rho^{\mathbf{E}} \otimes \rho^{W_1W_2}\|_1)$, we apply Lemma 3 and obtain

$$\begin{aligned}&\mathbb{E}_F(\|\rho^{W_1W_2\mathbf{E}} - \rho^{W_1W_2} \otimes (\widetilde{\rho}^E)^{\otimes T}\|_1)\\ &= \frac{1}{M_1M_2}\sum_{w_1,w_2} \mathbb{E}_F(\|\rho^{\mathbf{E}}_{w_1,w_2} - (\widetilde{\rho}^E)^{\otimes T}\|_1)\\ &\leqslant \sqrt{2^{\gamma s + T\phi(s)}} + \sqrt{\frac{2^\gamma \nu}{M_3}},\end{aligned} \tag{A46}$$

where ν is the number of distinct eigenvalues of $(\widetilde{\rho}^E)^{\otimes T}$, and

$$\phi(s) = \ln\left(\sum_y Q_Y(y)\operatorname{tr}\left(\left(\widetilde{\rho}^E_y\right)^{1-s}(\widetilde{\rho}^E)^s\right)\right). \tag{A47}$$

Upon choosing

$$\ln M_3 = \left\lfloor I\left(Q_Y, \widetilde{\rho}^E_y\right)T + \zeta\alpha_T T\right\rfloor, \tag{A48}$$

$$\gamma = I\left(Q_Y, \widetilde{\rho}^E_y\right)T + \frac{\zeta}{2}\alpha_T T, \tag{A49}$$

we obtain

$$\begin{aligned}\sqrt{2^{\gamma s + T\phi(s)}} + \sqrt{\frac{2^\gamma \nu}{M_3}} &\leqslant \sqrt{2^{s\alpha_T T\left(\frac{I(Q_Y,\widetilde{\rho}^E_y)}{\alpha_T} + \frac{\zeta}{2} + \frac{\phi(s)}{s\alpha_T}\right)}} + \sqrt{2^{-\frac{\zeta}{2}\alpha_T T}\nu}\\ &\overset{(a)}{\leqslant} \sqrt{2^{s\alpha_T T\left(\frac{I(Q_Y,\widetilde{\rho}^E_y)}{\alpha_T} + \frac{\zeta}{2} + \frac{\phi(s)}{s\alpha_T}\right)}}\\ &\quad + \sqrt{2^{-\frac{\zeta}{2}\alpha_T T}(T+1)^{\dim \mathcal{H}^E}}\\ &\leqslant \sqrt{2^{s\alpha_T T\left(\frac{I(Q_Y,\widetilde{\rho}^E_y)}{\alpha_T} + \frac{\zeta}{2} + \frac{\phi(s)}{s\alpha_T}\right)}} + \frac{1}{2}2^{-\xi\alpha_T T},\end{aligned} \tag{A50}$$

where (a) follows from Lemma 3.7 of [25]. We now introduce the following technical lemma to simplify the above expression.

Lemma 5. Suppose $s < 0$; there exists a constant $B \geqslant 0$ such that for T large enough and $|s|$ small enough we have

$$\phi(s) > -I\left(Q_Y, \widetilde{\rho}^E_y\right)s - B(\alpha_T s^2 - s^3). \tag{A51}$$

Proof. See Appendix B. ■

Applying Lemma 5 to (A50), we obtain

$$\begin{aligned}&\sqrt{2^{s\alpha_T T\left(\frac{I(Q_Y,\widetilde{\rho}^E_y)}{\alpha_T} + \frac{\zeta}{2} + \frac{\phi(s)}{s\alpha_T}\right)}}\\ &\leqslant \sqrt{2^{s\alpha_T T\left(\frac{I(Q_Y,\widetilde{\rho}^E_y)}{\alpha_T} + \frac{\zeta}{2} + \frac{-I(Q_Y,\widetilde{\rho}^E_Y)s - B(\alpha_T s^2 - s^3)}{s\alpha_T}\right)}}\\ &= \sqrt{2^{s\alpha_T T\left(\frac{\zeta}{2} + \frac{B(\alpha_T s - s^2)}{\alpha_T}\right)}}\end{aligned} \tag{A52}$$

By choosing $s = o(\sqrt{\alpha_T}) \cap \omega(\frac{\ln T}{T\alpha_T})$ [28], the above expression goes to zero faster than any polynomial. Therefore, for a random encoder, we have

$$\mathbb{E}_F(\mathbb{P}(W_1 \neq \widehat{W}_1)) \leqslant 2^{-\xi\alpha_T T}, \tag{A53}$$

$$\mathbb{E}_F\left(\mathbb{V}\left(P^a_{\mathbf{Y}}; Q_Y^{\otimes T}\right)\right) \leqslant 2^{-\xi T}, \tag{A54}$$

$$\mathbb{E}_F(\|\rho^{W_1W_2\mathbf{E}} - (\widetilde{\rho}^E)^{\otimes T} \otimes \rho^{W_1W_2}\|_1) \leqslant 2^{-\omega(\ln T)}, \tag{A55}$$

if

$$\ln M_3 = \left\lfloor (1+\zeta)I\left(Q_Y, \widetilde{\rho}^E_y\right)T\right\rfloor, \tag{A56}$$

$$\ln M_1 + \ln M_2 + \ln M_3 = \lceil (1+\zeta)H(Q_Y)T\rceil, \tag{A57}$$

$$\ln M_1 + \ln M_3 = \lfloor (1-\zeta)I(Q_Y, Q_{X|Y})T\rfloor. \tag{A58}$$

Upon defining the events

$$\mathcal{E}_1 \triangleq \{\mathbb{P}(W_1 \neq \widehat{W}_1) \leqslant 4 \times 2^{-\xi\alpha_T T}\}, \tag{A59}$$

$$\mathcal{E}_2 \triangleq \left\{\mathbb{V}\left(P^a_{\mathbf{Y}}; Q_Y^{\otimes T}\right) \leqslant 4 \times 2^{-\xi T}\right\}, \tag{A60}$$

$$\mathcal{E}_3 \triangleq \{\|\rho^{W_1W_2\mathbf{E}} - (\widetilde{\rho}^E)^{\otimes T} \otimes \rho^{W_1W_2}\|_1 \leqslant 4 \times 2^{-\omega(\ln T)}\}, \tag{A61}$$

and using Markov inequality, we have

$$\begin{aligned}&\mathbb{P}_F(\mathcal{E}_1 \cap \mathcal{E}_2 \cap \mathcal{E}_3)\\ &\geqslant 1 - \mathbb{P}_F\left(\mathcal{E}_1^c\right) - \mathbb{P}_F\left(\mathcal{E}_2^c\right) - \mathbb{P}_F\left(\mathcal{E}_3^c\right)\\ &\geqslant 1 - \frac{\mathbb{E}_F(\mathbb{P}(W_1 \neq \widehat{W}_1))}{2^{-\xi\alpha_T T}} - \frac{\mathbb{E}_F\left(\mathbb{V}\left(P^a_{\mathbf{Y}}; Q_Y^{\otimes T}\right)\right)}{4 \times 2^{-\xi T}}\\ &\quad - \frac{\mathbb{E}_F(\|\rho^{W_1W_2\mathbf{E}} - (\widetilde{\rho}^E)^{\otimes T} \otimes \rho^{W_1W_2}\|_1)}{4 \times 2^{-\omega(\ln T)}}\\ &\geqslant \frac{1}{4}.\end{aligned} \tag{A62}$$

Therefore, there exists a realization f of F with

$$\mathbb{P}(W_1 \neq \widehat{W}_1) \leqslant 4 \times 2^{-\xi\alpha_T T}, \tag{A63}$$

$$\mathbb{V}\left(P^a_{\mathbf{Y}}; Q_Y^{\otimes T}\right) \leqslant 4 \times 2^{-\xi T}, \tag{A64}$$

$$\|\rho^{W_1W_2\mathbf{E}} - (\widetilde{\rho}^E)^{\otimes T} \otimes \rho^{W_1W_2}\|_1 \leqslant 4 \times 2^{-\omega(\ln T)}. \tag{A65}$$

4. Proof of Theorem 1

Using the likelihood encoder technique, we first prove the lower bound in (11). Consider a specific code for the auxiliary problem in Appendix A 3 and let $\widetilde{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1}$ be the corresponding induced joint quantum state. Because all random variables W_1, W_2, $\mathbf{X}$, and $\mathbf{Y}$ are classical, we can define their induced joint PMF denoted by $\widetilde{P}_{W_1W_2\mathbf{XY}}$. We then use the conditional PMFs $\widetilde{P}_{W_1W_2|\mathbf{Y}}$ and $\widetilde{P}_{\widehat{W}_1|\mathbf{X}W_2}$ as the encoder and decoder, respectively, in the main problem, which results in the induced joint quantum state $\widehat{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1}$. By our construction, we can decompose $\widetilde{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1}$ as

$$\begin{aligned}\widetilde{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1} = \sum_{w_1,w_2,\widehat{w}_1,\mathbf{y},\mathbf{x}} & \widetilde{P}_{\mathbf{Y}}(\mathbf{y}) \\ & \times \widetilde{P}_{W_1W_2|\mathbf{Y}}(w_1, w_2|\mathbf{y})Q_{X|Y}^{\otimes T}(\mathbf{x}|\mathbf{y})\widetilde{P}_{\widehat{W}_1|\mathbf{X}W_2} \\ & \times (\widehat{w}_1|\mathbf{x}, w_2) \\ & \times |\mathbf{yx}w_1w_2\widehat{w}_1\rangle\langle\mathbf{yx}w_1w_2\widehat{w}_1| \otimes \widetilde{\rho}_{\mathbf{x},\mathbf{y}}^{\mathbf{E}} \end{aligned} \tag{A66}$$

and $\widehat{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1}$ as

$$\begin{aligned}\widehat{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1} = \sum_{w_1,w_2,\widehat{w}_1,\mathbf{y},\mathbf{x}} & Q_Y^{\otimes T}(\mathbf{y}) \\ & \times \widetilde{P}_{W_1W_2|\mathbf{Y}}(w_1, w_2|\mathbf{y})Q_{X|Y}^{\otimes T}(\mathbf{x}|\mathbf{y})\widetilde{P}_{\widehat{W}_1|\mathbf{X}W_2} \\ & \times (\widehat{w}_1|\mathbf{x}, w_2) \\ & \times |\mathbf{yx}w_1w_2\widehat{w}_1\rangle\langle\mathbf{yx}w_1w_2\widehat{w}_1| \otimes \widetilde{\rho}_{\mathbf{x},\mathbf{y}}^{\mathbf{E}}. \end{aligned} \tag{A67}$$

Since they differ only in the distribution of $\mathbf{Y}$, we have

$$\|\widetilde{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1} - \widehat{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1}\|_1 \leqslant 2\mathbb{V}\big(\widetilde{P}_{\mathbf{Y}}^a; Q_Y^{\otimes T}\big) \overset{(a)}{\leqslant} 2^{-\xi T}, \tag{A68}$$

where (a) follows from (A54). Thus, we upper bound the probability of error in the main problem as

$$\begin{aligned}\mathbb{P}_{\widehat{P}}(W_1 \neq W_2) &\leqslant \mathbb{P}_{\widetilde{P}}(W_1 \neq W_2) \\ &\quad + \|\widetilde{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1} - \widehat{\rho}^{\mathbf{ABE}W_1W_2\widehat{W}_1}\|_1 \\ &\leqslant 2^{-\zeta\alpha_T T} + 2^{-\zeta T} \end{aligned} \tag{A69}$$

and upper bound the sum of secrecy and covertness as

$$\begin{aligned} S + C &\triangleq \mathbb{D}\big(\widehat{\rho}^{W_1W_2\mathbf{E}}\big\|\rho_{\text{unif}}^{W_1} \otimes \widehat{\rho}^{W_2\mathbf{E}}\big) \\ &\quad + \mathbb{D}\big(\widehat{\rho}^{W_2\mathbf{E}}\big\|\rho_{\text{unif}}^{W_2} \otimes \rho_0^{\otimes T}\big) & \text{(A70)} \\ &= \mathbb{D}\big(\widehat{\rho}^{W_1W_2\mathbf{E}}\big\|\rho_{\text{unif}}^{W_1W_2} \otimes \widehat{\rho}^{\mathbf{E}}\big) + \mathbb{D}\big(\widehat{\rho}^{\mathbf{E}}\big\|\rho_0^{\otimes T}\big) & \text{(A71)} \\ &\overset{\text{(a)}}{=} \mathbb{D}\big(\widehat{\rho}^{W_1W_2\mathbf{E}}\big\|\rho_{\text{unif}}^{W_1W_2} \otimes \widehat{\rho}^{\mathbf{E}}\big) \\ &\quad + \frac{1}{2}\alpha_T^2\chi_2\big(\rho_1^E\big\|\rho_0^E\big)T + O\big(\alpha_T^3 T\big) & \text{(A72)} \\ &\overset{\text{(b)}}{\leqslant} \big\|\widehat{\rho}^{W_1W_2\mathbf{E}} - \rho_{\text{unif}}^{W_1W_2} \otimes \widehat{\rho}^{\mathbf{E}}\big\|_1 \\ &\quad \times \ln \frac{M_1M_2(\dim \mathcal{H}^E)^T}{\frac{1}{M_1M_2}\lambda_{\min}(\widetilde{\rho}^E)^T \big\|\widehat{\rho}^{W_1W_2\mathbf{E}} - \rho_{\text{unif}}^{W_1W_2} \otimes \widehat{\rho}^{\mathbf{E}}\big\|_1} \\ &\quad + \frac{1}{2}\alpha_T^2\chi_2\big(\rho_1^E\big\|\rho_0^E\big)T + O\big(\alpha_T^3 T\big) & \text{(A73)} \\ &= \big\|\widehat{\rho}^{W_1W_2\mathbf{E}} - \rho_{\text{unif}}^{W_1W_2} \otimes \widehat{\rho}^{\mathbf{E}}\big\|_1 \\ &\quad \times \big(O(T) - \ln\big\|\widehat{\rho}^{W_1W_2\mathbf{E}} - \rho_{\text{unif}}^{W_1W_2} \otimes \widehat{\rho}^{\mathbf{E}}\big\|_1\big) \\ &\quad + \frac{1}{2}\alpha_T^2\chi_2\big(\rho_1^E\big\|\rho_0^E\big)T + O\big(\alpha_T^3 T\big) & \text{(A74)} \\ &\overset{\text{(c)}}{\leqslant} (2^{-\zeta\alpha_T T} + 2^{-\zeta T})O(T) \\ &\quad + \frac{1}{2}\alpha_T^2\chi_2\big(\rho_1^E\big\|\rho_0^E\big)T + O\big(\alpha_T^3 T\big), & \text{(A75)} \end{aligned}$$

where (a) follows from Lemma 7 of [14], (b) follows from Lemma 6 in Appendix C, and (c) follows from

$$\begin{aligned}\big\|\widehat{\rho}^{W_1W_2\mathbf{E}} - \rho_{\text{unif}}^{W_1W_2} \otimes \widehat{\rho}^{\mathbf{E}}\big\|_1 &\leqslant \big\|\widetilde{\rho}^{W_1W_2\mathbf{E}} - \rho_{\text{unif}}^{W_1W_2} \otimes \widehat{\rho}^{\mathbf{E}}\big\|_1 \\ &\quad + \|\widehat{\rho}^{W_1W_2\mathbf{E}} - \widetilde{\rho}^{W_1W_2\mathbf{E}}\|_1 \\ &\leqslant 2^{-\zeta\alpha_T T} + 2^{-\zeta T}. \end{aligned} \tag{A76}$$

The throughput of the coding scheme is lower bounded by (A79) shown below:

$$\begin{aligned}\frac{\ln M_1}{\sqrt{TC}} &\geqslant \frac{\ln M_1}{\sqrt{T\big((2^{-\zeta\alpha_T T} + 2^{-\zeta T})O(T) + \frac{1}{2}\alpha_T^2\chi_2\big(\rho_1^E\big\|\rho_0^E\big)T + O\big(\alpha_T^3 T\big)\big)}} & \text{(A77)} \\ &\geqslant \sqrt{\frac{2}{\chi_2\big(\rho_1^E\big\|\rho_0^E\big)}}\frac{\lfloor(1-\zeta)\mathbb{I}(A;B)_{\widetilde{\rho}}T\rfloor - \lceil\mathbb{I}(B;E)_{\widetilde{\rho}}T + \zeta\alpha_T T\rceil}{T\alpha_T(1+o(1))} & \text{(A78)} \\ &= \sqrt{\frac{2}{\chi_2\big(\widetilde{\rho}_1^E\big\|\widetilde{\rho}_0^E\big)}}\big(\mathbb{D}\big(\widetilde{\rho}_1^{BE}\big\|\widetilde{\rho}_0^{BE}\big) - \mathbb{D}\big(\widetilde{\rho}_1^E\big\|\widetilde{\rho}_0^E\big) - \mathbb{D}\big(\widetilde{\rho}_1^{BE}\big\|\widetilde{\rho}_1^B \otimes \widetilde{\rho}_1^E\big)\big) + o(1). & \text{(A79)} \end{aligned}$$

We finally turn to the proof of the lower bound in (10). Note that if $\mathbb{D}(\widetilde{\rho}_1^B\|\widetilde{\rho}_0^B) \leqslant \mathbb{D}(\widetilde{\rho}_1^E\|\widetilde{\rho}_0^E)$ the result is trivial. Therefore, we can assume that $\mathbb{D}(\widetilde{\rho}_1^B\|\widetilde{\rho}_0^B) > \mathbb{D}(\widetilde{\rho}_1^E\|\widetilde{\rho}_0^E)$. Let M_1 and M_2 be such that

$$\ln M_1 + \ln M_2 = \big\lfloor(1-\zeta)I\big(Q_X, \widetilde{\rho}_y^B\big)\big\rfloor, \tag{A80}$$

$$\ln M_2 = \big\lceil(1+\zeta)I\big(Q_X, \widetilde{\rho}_y^E\big)\big\rceil. \tag{A81}$$

The protocol is then as follows. Alice chooses a random binary string of length $\ln M_1 + \ln M_2$ and transmits this string through a covert code introduced in [14]. Alice and Bob subsequently extract the first $\ln M_1$ bits of the string as the key. The reliability and covertness proof follows exactly from [14]. For secrecy, note that

$$\begin{aligned}\mathbb{D}\big(\rho^{\mathbf{EM}S^X}\big\|\rho^{\mathbf{EM}} \otimes \rho_{\text{unif}}^{S^X}\big) &\triangleq \mathbb{D}\big(\rho^{\mathbf{E}S^X}\big\|\rho^{\mathbf{E}} \otimes \rho_{\text{unif}}^{S^X}\big) \\ &= \frac{1}{M_1}\sum_{w_1=1}^{M_1}\mathbb{D}\big(\rho_{w_1}^{\mathbf{E}}\big\|\rho^{\mathbf{E}}\big). \end{aligned} \tag{A82}$$

Similar to the proof of (A55), one can show that the above expression is upper bounded by $2^{-\omega(\ln T)}$

provided that $\ln M_2 = \lceil (1+\zeta) I(Q_X, \widetilde{\rho}_y^E) \rceil$. Lower bounding the throughput as in (A79) using (A80) and (A81) concludes the proof. Note that unlike the proof of (11) the protocol used here does not use the public communication channel.

APPENDIX B: ERROR EXPONENT CALCULATIONS

Proof of Lemma 5. For a fix T, applying Taylor's theorem on ϕ defined in (A47), we have

$$\phi(s) = \phi(0) + \phi'(0)s + \frac{\phi''(0)}{2}s^2 + \frac{\phi'''(\eta)}{6}s^3, \tag{B1}$$

for some $s \leqslant \eta \leqslant 0$. To compute derivatives of ϕ, let us define

$$A_y(s) \triangleq \left(\widetilde{\rho}_y^E\right)^{1-s} (\widetilde{\rho}^E)^s, \tag{B2}$$

$$g(s) \triangleq \sum_y Q_Y(y) \mathrm{tr}(A_y(s)). \tag{B3}$$

One can check that $\phi(s) = \ln g(s)$. Hence, we obtain

$$\phi'(s) = \frac{g'(s)}{g(s)}, \tag{B4}$$

$$\phi''(s) = \frac{g''(s)}{g(s)} - \left(\frac{g'(s)}{g(s)}\right)^2, \tag{B5}$$

$$\phi'''(s) = \frac{g'''(s)}{g(s)} - 3\frac{g'(s)g''(s)}{g^2(s)} + 2\left(\frac{g'(s)}{g(s)}\right)^3. \tag{B6}$$

Moreover, since $A_y'(s) = -\ln(\widetilde{\rho}_y^E) A_y(s) + A_y(s) \ln(\widetilde{\rho}^E)$, we have

$$g'(s) = \sum_y Q_Y(y) \mathrm{tr}\big(-\ln(\widetilde{\rho}_y^E) A_y(s) + A_y(s) \ln(\widetilde{\rho}^E)\big), \tag{B7}$$

$$\begin{aligned} g''(s) = \sum_y Q_Y(y) \mathrm{tr}\Big(&\big(\ln(\widetilde{\rho}_y^E)\big)^2 A_y(s) \\ &- 2\ln(\widetilde{\rho}_y^E) A_y(s) \ln(\widetilde{\rho}^E) + A_y(s)(\ln(\widetilde{\rho}^E))^2\Big), \end{aligned} \tag{B8}$$

and

$$\begin{aligned} g'''(s) = \sum_y Q_Y(y) \mathrm{tr}\Big(&- \big(\ln(\widetilde{\rho}_y^E)\big)^3 A_y(s) \\ &+ 3\big(\ln(\widetilde{\rho}_y^Z)\big)^2 A_y(s) \ln(\widetilde{\rho}^E) \\ &- 3\ln(\widetilde{\rho}_y^E) A_y(s) (\ln(\widetilde{\rho}^E))^2 + A_y(s)(\ln(\widetilde{\rho}^E))^3\Big). \end{aligned}$$

Using $A_y(0) = \widetilde{\rho}_y^E$ combined with the above expressions, we obtain

$$g(0) = \sum_y Q_Y(y) \mathrm{tr}\big(\widetilde{\rho}_y^E\big) = 1, \tag{B9}$$

$$g'(0) = \sum_y Q_Y(y) \mathrm{tr}\big(-\ln(\widetilde{\rho}_y^E)\widetilde{\rho}_y^E + \widetilde{\rho}_y^E \ln(\widetilde{\rho}^E)\big) \tag{B10}$$

$$= -I\big(Q_Y, \widetilde{\rho}_y^E\big), \tag{B11}$$

$$\begin{aligned} g''(0) = \sum_y Q_Y(y) \mathrm{tr}\Big(&\big(\ln(\widetilde{\rho}_y^E)\big)^2 \widetilde{\rho}_y^E \\ &- 2\ln(\widetilde{\rho}_y^E)\widetilde{\rho}_y^E \ln(\widetilde{\rho}^E) + \widetilde{\rho}_y^E (\ln(\widetilde{\rho}^E))^2\Big). \end{aligned} \tag{B12}$$

Hence, we have

$$\phi(0) = \ln(g(0)) = 0, \tag{B13}$$

$$\phi'(0) = \frac{g'(0)}{g(0)} = -I\big(Q_Y, \widetilde{\rho}_y^E\big), \tag{B14}$$

$$\phi''(0) = \frac{g''(0)}{g(0)} - \left(\frac{g'(0)}{g(0)}\right)^2, \tag{B15}$$

$$\begin{aligned} = \sum_y Q_Y(y) \mathrm{tr}\Big(&\big(\ln(\widetilde{\rho}_y^E)\big)^2 \widetilde{\rho}_y^E \\ &- 2\ln(\widetilde{\rho}_y^E)\widetilde{\rho}_y^E \ln(\widetilde{\rho}^E) + \widetilde{\rho}_y^E (\ln(\widetilde{\rho}^E))^2\Big) \\ &- I\big(Q_Y, \widetilde{\rho}_y^E\big)^2. \end{aligned} \tag{B16}$$

Note that $\phi''(0)$ implicitly depends on α_T, the probability that the input is 1. Let us define

$$\begin{aligned} h(\alpha) \triangleq \sum_y Q_Y(y) \mathrm{tr}\Big(&\big(\ln(\widetilde{\rho}_y^E)\big)^2 \widetilde{\rho}_y^E \\ &- 2\ln(\widetilde{\rho}_y^E)\widetilde{\rho}_y^E \ln(\widetilde{\rho}^E) + \widetilde{\rho}_y^E (\ln(\widetilde{\rho}^E))^2\Big) \end{aligned} \tag{B17}$$

when the input distribution is Bernoulli (α). One can check that $Q_Y(y)$, $\widetilde{\rho}_y^E$, $\ln(\widetilde{\rho}_y^E)$, and $\ln(\widetilde{\rho}^E)$ are continuously differentiable with respect to α, and so is h. Moreover, we have

$$\begin{aligned} h(0) = \sum_y Q_{Y|X}(y|0) \mathrm{tr}\Big(&\big(\ln(\widetilde{\rho}_{0,y}^E)\big)^2 \widetilde{\rho}_{0,y}^E \\ &- 2\ln(\widetilde{\rho}_{0,y}^E)\widetilde{\rho}_{0,y}^E \ln(\widetilde{\rho}^E) + \widetilde{\rho}_{0,y}^E (\ln(\widetilde{\rho}^E))^2\Big) \end{aligned} \tag{B18}$$

$$\begin{aligned} \overset{(a)}{=} \sum_y Q_{Y|X}(y|0) \mathrm{tr}\big(&(\ln(\widetilde{\rho}^E))^2 \widetilde{\rho}^E \\ &- 2\ln(\widetilde{\rho}^E)\widetilde{\rho}^E \ln(\widetilde{\rho}^E) + \widetilde{\rho}^E (\ln(\widetilde{\rho}^E))^2\big) = 0, \end{aligned} \tag{B19}$$

where (a) follows from Lemma 1. By the mean value theorem, we know that $|h(\alpha) - h(0)| = |h(\alpha)| = h'(\beta)\alpha$ for some $0 < \beta < \alpha$. Since h' is continuous for a small neighborhood around zero, it is bounded and therefore we have $|h(\alpha_T)| = O(\alpha_T)$. Furthermore, Lemma 1 implies that $I(Q_Y, \widetilde{\rho}_y^E)^2 = O(\alpha_T^2)$. Thus, there exists $B > 0$ such that $|\phi''(0)| \leqslant B\alpha_T$ for T large enough. Notice next that g, g', g'', and g''' are jointly continuous functions of both variables s and α_T in a neighborhood around $(0, 0)$. Additionally, since $g(0) = 1$ when $\alpha = 0$, we conclude that ϕ''' is also continuous in both s and α_T in a neighborhood around $(0, 0)$. Therefore, for B large enough, $|s|$ small enough, and T large enough, we have $|\phi'''(s)| \leqslant B$. Combining $\phi(0) = 0$, $\phi'(0) = -I(Q_Y, \widetilde{\rho}_y^E)$, $|\phi''(0)| \leqslant B\alpha_T$, and $|\phi'''(\eta)| \leqslant B$ with (B1), we obtain the desired result.

APPENDIX C: TECHNICAL LEMMA

Lemma 6. Suppose ρ and σ are two density matrices on a Hilbert space $\mathcal{H}$ with $\dim \mathcal{H} = d$ such that $\mathrm{supp}\rho \subset \mathrm{supp}\sigma$ and $\|\rho - \sigma\|_1 \leqslant \epsilon \leqslant e^{-1}$. Then,

$$\mathbb{D}(\rho\|\sigma) \leqslant \epsilon \ln \frac{d}{\lambda_{\min}(\sigma)\epsilon}. \tag{C1}$$

Proof. Since $\text{supp}(\rho) \subset \text{supp}(\sigma)$, we have

$$\mathbb{D}(\rho\|\sigma) = \text{tr}(\rho(\ln\rho - \ln\sigma)) \tag{C2}$$

$$= -H(\rho) + H(\sigma) - \text{tr}((\rho-\sigma)\ln\sigma) \tag{C3}$$

$$\overset{(a)}{\leqslant} \epsilon\ln\frac{d}{\epsilon} - \text{tr}((\rho-\sigma)\ln\sigma) \tag{C4}$$

$$\leqslant \epsilon\ln\frac{d}{\epsilon} + \epsilon\ln\frac{1}{\lambda_{\min}(\sigma)}, \tag{C5}$$

where (a) follows from Fannes inequality.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[3] B. A. Bash, D. Goeckel, D. Towsley, and S. Guha, IEEE Commun. Mag. **53**, 26 (2015).

[4] C. Cachin, Inf. Comput. **192**, 41 (2004).

[5] A. D. Ker, IEEE Signal Process. Lett. **14**, 525 (2007).

[6] B. A. Shaw and T. A. Brun, Phys. Rev. A **83**, 022310 (2011).

[7] B. Sanguinetti, G. Traverso, J. Lavoie, A. Martin, and H. Zbinden, Phys. Rev. A **93**, 012336 (2016).

[8] In [6], secrecy and covertness are referred to as security and secrecy, respectively. We adopt here a different terminology more in line with common usage in information-theoretical security.

[9] B. Bash, D. Goeckel, and D. Towsley, IEEE J. Sel. Areas Commun. **31**, 1921 (2013).

[10] L. Wang, G. W. Wornell, and L. Zheng, IEEE Trans. Info. Theory **62**, 3493 (2016).

[11] M. R. Bloch, IEEE Trans. Info. Theory **62**, 2334 (2016).

[12] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, Nat. Commun. **6**, 8626 (2015).

[13] L. Wang, in *Proceedings of the IEEE Information Theory Workshop* (IEEE, 2016), pp. 364–368.

[14] A. Sheikholeslami, B. A. Bash, D. Towsley, D. Goeckel, and S. Guha, in *Proceedings of the IEEE International Symposium on Information Theory* (IEEE, Piscataway, New Jersey, 2016), pp. 2064–2068.

[15] K. Bradler, T. Kalajdzievski, G. Siopsis, and C. Weedbrook, arXiv:1607.05916 (2016).

[16] J. M. Arrazola and V. Scarani, Phys. Rev. Lett. **117**, 250503 (2016).

[17] J. M. Arrazola and R. Amiri, Phys. Rev. A **97**, 022325 (2018).

[18] Y. Liu, J. M. Arrazola, W.-Z. Liu, W. Zhang, I. W. Primaatmaja, H. Li, L. You, Z. Wang, V. Scarani, Q. Zhang, and J.-W. Pan, arXiv:1709.06755v1 (2017).

[19] I. A. Kadampot, M. Tahmasbi, and M. R. Bloch, in *Proceedings of the IEEE International Symposium on Information Theory* (IEEE, 2018), pp. 1864–1868.

[20] Y. Polyanskiy, H. V. Poor, and S. Verdú, IEEE Trans. Inf. Theory **56**, 2307 (2010).

[21] E. C. Song, P. Cuff, and H. V. Poor, IEEE Trans. Info. Theory **62**, 1836 (2016).

[22] M. Tahmasbi and M. R. Bloch, in *Proceedings of the IEEE Conference on Communications and Network Security (CNS)* (IEEE, 2017), pp. 540–544.

[23] M. M. Wilde, *Quantum Information Theory* (Cambridge University, Cambridge, England, 2013).

[24] M. Hayashi, IEEE Trans. Inf. Theory **52**, 1562 (2006).

[25] M. Hayashi, *Quantum Information* (Springer, New York, 2006).

[26] S. Bernstein, Ann. Sci. Inst. Sav. Ukraine, Sect. Math **1**, 38 (1924).

[27] W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).

[28] To find such s, it is required that $\sqrt{\alpha_T} = \omega(\frac{\log T}{T\alpha_T})$ or equivalently $\alpha_T = \omega((\frac{\log T}{T})^{\frac{2}{3}})$.