Towards Undetectable Quantum Key Distribution over Bosonic Channels

Mehrdad Tahmasbi and Matthieu R. Bloch, *Senior Member, IEEE*

Abstract

We propose a protocol based on pulse-position modulation and multi-level coding that allows one to bootstrap traditional quantum key distribution protocols while ensuring covertness, in the sense that no statistical test by the adversary can detect the presence of communication over the quantum channel better than a random guess. When run over a bosonic channel, our protocol can leverage existing discrete-modulated continuous-variable protocols. Since existing techniques to bound Eve's information do not directly apply, we develop a new bound that results in positive, although very low, throughput for a range of channel parameters. The analysis of the protocol performance shows that covert secret key expansion is possible using a public authenticated classical channel and a quantum channel largely but not fully under the control of an adversary, which we precisely define. We also establish a converse result showing that, under the golden standard of quantum key distribution, by which the adversary completely controls the quantum channel, no covert key generation is possible.

I. Introduction

The combination of quantum mechanics and information theory has led to several intriguing applications. In particular, there have been significant advances in Quantum Key Distribution (QKD) [1], which has now been successfully implemented and deployed in the field [2]. QKD finds its foundations in two pioneering papers [3], [4], which discovered that non-classical signaling allows two parties (Alice and Bob) to exploit the laws of quantum mechanics and bound the information leaked to any adversary (Eve); when combined with classical information-theoretic tools, such as information reconciliation and privacy amplification, this observation can lead to protocols for the distillation of secure key bits [5]. More precisely, QKD protocols allow

The authors are with the Georgia Institute of Technology, Atlanta, GA 30332 USA (e-mail: tahmasbi@ece.gatech.edu; matthieu.bloch@ece.gatech.edu)

secret key expansion, in the sense that the number of distilled key bits exceeds the number of consumed key bits. The security proofs of QKD have evolved from considering simple attacks, in which Eve could only perform a measurement on each transmitted signal and send another state to Bob, to accounting for all attacks that could be described in the framework of quantum mechanics, known as *coherent* attacks [5]; recent proofs even consider an adversary who tampers with the legitimate users' measurement devices [6].

Although QKD ensures the *confidentiality* of the generated keys in an extremely strong sense, Alice and Bob might desire other security features. One such feature that has recently attracted attention is covertness [7], [8], [9], i.e., the ability to prevent an adversary from distinguishing whether a communication protocol is running or not by analyzing its observations. Covertness could be a desirable feature for situations in which the mere act of creating and communicating information may become a liability. As a concrete illustration, covert QKD would allow the parties that generate a key to have *plausible deniability* even if the key were disclosed later on, since an adversary would not be able to tie the origin of the key to the observations obtained when the QKD protocol was run. For memoryless classical and classical-quantum (cq) channels, over which Alice aims at sending a message, a square root law for covert communication has been established [7], [10], [11] and states that the optimal number of bits that can be reliably and covertly transmitted scales as the square root of the number of channel uses. This contrasts with the limits of confidential communication, for which a linear scaling is feasible. The main intuition behind the square root law is that the central limit theorem ensures the presence of statistical uncertainty in Eve's observations, on the order of the square root of the number of channel uses, in which the transmitter can hide its signals.

The first attempts at covert QKD [12], [13] have ensured covertness with *fully coordinated* protocols, in which information-bearing qubits are only communicated over a secret random subset of channel uses upon which Alice and Bob secretly agree prior to communication; in the remaining channel uses Alice transmits an "idle" state corresponding to no communication. If n denotes the total number of channel uses and t denotes the number of channel uses over which communication happens, fully coordinated protocols [12], [13] require $t = \Theta(\sqrt{n})$[1] to generate $\Omega(\sqrt{n})$ bits of secret key. Although the processing complexity is identical to that of standard QKD protocols, fully coordinated protocols require Alice and Bob to share $\log \binom{n}{t} = \Theta(\sqrt{n} \log n)$

[1]We use standard asymptotic notations $\Theta(\cdot)$, $\omega(\cdot)$, $\Omega(\cdot)$, $o(\cdot)$, and $O(\cdot)$ throughout the paper.

secret bits prior to communication, so that the number of required key bits asymptotically dominates the number of generated key bits, thereby forbidding secret key expansion.

To circumvent the impossibility of covert and secret key expansion with fully coordinated protocols, we have recently proposed [14] to achieve covertness with an *uncoordinated* protocol based on the use of "sparse signaling" for quantum state distribution, which operates as follows. If $\alpha_n \triangleq O(n^{-\frac{1}{2}})$ and if P_X denotes the Bernoulli(α_n) distribution, Alice generates an i.i.d. sequence $X^n = (X_1, \cdots, X_n)$ according to $P_X^{\otimes n}$, which is then modulated by mapping zero to the idle state and one to another state. A technical subtlety, however, prevents Alice and Bob from performing classical information reconciliation and privacy amplification to obtain a secret key from their shared quantum states. While the asymptotic key rate is $O(n^{-\frac{1}{2}})$ by the square root law, the finite length penalty of privacy amplification is of the order of $\omega(n^{-\frac{1}{2}})$ [15], which dominates the asymptotic rate. For a *known adversary's attack*, our uncoordinated protocol circumvents this difficulty and ensures secret key expansion using a likelihood encoder [14] but the classical post-processing of the protocol *is much more complex than for typical QKD protocols*.

To reap the benefits of both fully coordinated and uncoordinated protocols and achieve secret key expansion without increasing processing complexity, we develop here a *partially coordinated* protocol inspired by our prior construction of low-complexity codes for covert communication over classical channels with Pulse-Position Modulation (PPM) and MultiLevel Coding (MLC) [16]. This approach is more aligned with traditional low-complexity information reconciliation and privacy amplification algorithms and we analyze the covertness and the security under an unknown attack by the adversary. We restrict, however, the adversary's attack by requiring that a portion of the channel be out of the adversary's control (e.g., the part of the channel in Alice's laboratory). We prove that such a requirement is fundamentally necessary to establish any covertness result. Since we were not able to use any standard technique to bound Eve's information, we present a new bound, which we use to show the existence of positive throughputs for some range of bosonic channel parameters. While our results are slightly disappointing in that the range of useful parameters is limited, our analysis opens the way to experimental demonstrations of covert QKD.

Our covert QKD protocol relies on a classical authenticated public communication similar to most existing QKD protocols. While it is well-known that public communication should not reveal the content of the generated key, there is no standard covertness criterion on public

communication to the best of our knowledge. In this work, we impose two constraints on public communication: 1) public messages should be uniformly distributed over the set of all possible public messages; 2) public communication should be independent of the communication on the quantum channel. The operational justification for this approach is the presence of ongoing independent classical communications, which do not raise the suspicion of the adversary regarding the existence of a QKD protocol. We note that this assumption might be restrictive in certain scenarios and developing QKD protocols with fully covert public communication is an intriguing avenue for future work.

We conclude this introduction by clarifying the connection between our work and [17], in which a message is covertly modulated in the position of a single pulse within several optical modes and in which a secret key shared between the transmitter and the receiver helps them narrow down the position of the pulse. Our model differs from [17] not only by explicitly accounting for channel estimation and reconciliation but also by operating over multiple coded PPM pulses. While the protocol in [17] allows the number of secret-key bits to scale at best *logarithmically* with the number of modes, our protocol enables the number of secret-key bits to scale with the *square-root* of the number of modes.

II. Notation

A system (e.g. A) is described by a finite-dimensional Hilbert space (e.g. $\mathcal{H}_A$). Let $\mathbf{1}_A$ be the identity map on $\mathcal{H}_A$ and $\rho_A^{\text{unif}} \triangleq \frac{\mathbf{1}_A}{\dim \mathcal{H}_A}$, where $\dim \mathcal{H}_A$ is the dimension of $\mathcal{H}_A$. $\mathcal{B}(\mathcal{H}_A)$ denotes the set of all bounded linear operators from $\mathcal{H}_A$ to $\mathcal{H}_A$, $\mathcal{P}(\mathcal{H}_A)$ denotes the set of all positive operators in $\mathcal{B}(\mathcal{H}_A)$, and $\mathcal{D}(\mathcal{H}_A)$ denotes the set of all density operators on $\mathcal{H}_A$. For $X \in \mathcal{B}(\mathcal{H}_A)$, the trace norm of X is $\|X\|_1 \triangleq \text{tr}\,(\sqrt{X^\dagger X})$, and $\nu(X)$ denotes the number of *distinct* eigenvalues of X. We also define the support of $X \in \mathcal{B}(\mathcal{H}_A)$ as the subspace orthogonal to $\text{Ker}\,(X)$, which we denote by $\text{supp}(X)$. We write $X \succeq Y$ for $X, Y \in \mathcal{B}(\mathcal{H}_A)$ when $X - Y \in \mathcal{P}(\mathcal{H}_A)$. We recall the definition of the von Neumann entropic quantities $H(\rho_A) \triangleq \mathbb{H}(A)_\rho \triangleq -\text{tr}\,(\rho_A \log \rho_A)$, $\mathbb{H}(A|B)_\rho \triangleq \mathbb{H}(AB)_\rho - \mathbb{H}(B)_\rho$, and $\mathbb{I}(A;B)_\rho \triangleq \mathbb{H}(A)_\rho - \mathbb{H}(A|B)_\rho$. We also use the definition of smooth min-entropy from [5]. In particular, for two states $\rho_{AB} \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_B)$ and $\sigma_B \in \mathcal{P}(\mathcal{H}_B)$,

let

$$H_{\min}(\rho_{AB}|\sigma_B) \triangleq \sup_{\lambda\in\mathbb{R}:\lambda\mathbf{1}_A\otimes\sigma_A-\rho_{AB}\succeq 0} -\log\lambda \tag{1}$$

$$H^{\epsilon}_{\min}(\rho_{AB}|\sigma_B) \triangleq \sup_{\widetilde{\rho}_{AB}\in\mathcal{P}(\mathcal{H}_A\otimes\mathcal{H}_B):\|\widetilde{\rho}_{AB}-\rho_{AB}\|_1\leqslant\epsilon} H_{\min}(\widetilde{\rho}_{AB}|\sigma_B) \tag{2}$$

$$\mathbb{H}^{\epsilon}_{\min}(A|B)_\rho \triangleq \sup_{\widetilde{\sigma}_B\in\mathcal{D}(\mathcal{H}_B)} H^{\epsilon}_{\min}(\rho_{AB}|\widetilde{\sigma}_B) \tag{3}$$

We further define $\mathbb{H}_{\max}(A)_\rho \triangleq \log\left(\dim \operatorname{supp}(\rho_A)\right)$. The fidelity between two density operators ρ_A and σ_A is defined as $F(\rho_A,\sigma_A) \triangleq \|\sqrt{\rho_A}\sqrt{\sigma_A}\|_1^2$. We further define $C(\rho_A,\sigma_A) \triangleq \sqrt{1-F(\rho_A,\sigma_A)}$, which satisfies the triangle inequality [18, Proposition 3.3]. A quantum channel $\mathcal{N}_{A\to B}$ is a linear trace-preserving completely positive map from $\mathcal{B}(\mathcal{H}_A)$ to $\mathcal{B}(\mathcal{H}_B)$. An isometric extension of the quantum channel $\mathcal{N}_{A\to B}$ consists of an auxiliary system E and an isometry $V_{A\to BE}:\mathcal{H}_A\to\mathcal{H}_B\otimes\mathcal{H}_E$ such that $\mathcal{N}_{A\to B}(X)=\operatorname{tr}_E\left(V_{A\to BE}XV^\dagger_{A\to BE}\right)$ for all $X\in\mathcal{B}(\mathcal{H}_A)$. The complementary channel of $\mathcal{N}_{A\to B}$ is defined by $X\mapsto\operatorname{tr}_B\left(V_{A\to BE}XV^\dagger_{A\to BE}\right)$. Both the isometric extension and the complementary channel exist and are unique up to a unitary operation [19]. Let id_A be the identity channel on $\mathcal{B}(\mathcal{H}_A)$. For two states ρ and σ, we define

$$\chi_2\left(\rho\|\sigma\right) \triangleq \begin{cases} \operatorname{tr}\left(\rho^2\sigma^{-1}\right)-1 & \text{if } \operatorname{supp}(\rho)\subset\operatorname{supp}(\sigma), \\ \infty & \text{otherwise.}\end{cases} \tag{4}$$

For a non-empty finite set $\mathcal{X}$, let $\mathcal{H}_X$ be a Hilbert space defined by an orthonormal basis $\{|x\rangle : x\in\mathcal{X}\}$. For a function $f:\mathcal{X}\to\mathcal{Y}$, we define the channel

$$\begin{aligned}\mathcal{E}^f_{X\to Y}:\mathcal{B}(\mathcal{H}_X)&\to\mathcal{B}(\mathcal{H}_Y)\\ \rho_X&\mapsto\sum_{x\in\mathcal{X}}|f(x)\rangle\langle x|\rho_X|x\rangle\langle f(x)|.\end{aligned} \tag{5}$$

We define $\mathbb{H}_b\left(x\right)\triangleq -x\log x-(1-x)\log(1-x)$ for $x\in[0,1]$ and $[\![m,n]\!]\triangleq\{i\in\mathbb{Z}:m\leqslant i\leqslant n\}$. We conclude this section by reviewing some concepts associated families of hash functions. Let $\mathcal{X}$ and $\mathcal{Z}$ be two finite non-empty sets and $\mathcal{F}$ be a non-empty family of functions from $\mathcal{X}$ to $\mathcal{Z}$. $\mathcal{F}$ is called *two-universal* if for all distinct $x,x'\in\mathcal{X}$, we have

$$\frac{1}{|\mathcal{F}|}\sum_{f\in\mathcal{F}}\mathbb{1}\{f(x)=f(x')\}\leqslant\frac{1}{|\mathcal{Z}|}. \tag{6}$$

$\mathcal{F}$ is called *efficient* if 1) $|\mathcal{F}|$ is upper-bounded by a polynomial function of $\max(|\mathcal{X}|,|\mathcal{Z}|)$; 2) there exists a bijective map $\phi:\mathcal{F}\to[\![1,|\mathcal{F}|]\!]$ such that given $i\in[\![1,|\mathcal{F}|]\!]$ and $x\in\mathcal{X}$, one can

compute $(\phi(i))(x)$ in time polynomial in $\max(|\mathcal{X}|, |\mathcal{Z}|)$ (the existence of ϕ ensures that we can efficiently sample from $\mathcal{F}$ at random). $\mathcal{F}$ is called *invertible* if 1) $|\mathcal{Z}|$ divides $|\mathcal{X}|$; 2) there exists a family of functions from $\mathcal{Z} \times [\![1, |\mathcal{X}| / |\mathcal{Z}|]\!]$ to $\mathcal{X}$ that we denote by $\mathcal{F}^{-1}$ (with slight abuse of notation because it is not unique) such that there exists a bijective function $\phi : \mathcal{F} \to \mathcal{F}^{-1}$ with $f^{-1}(z) = \{\phi(f)(z, i) : i \in [\![1, |\mathcal{X}| / |\mathcal{Z}|]\!]\}$. $\mathcal{F}$ is called *efficiently invertible* if $\mathcal{F}^{-1}$ is efficient.

III. Covert QKD Setup

Alice and Bob aim at *covertly* expanding a *secret* key using the following generic setup and protocol. Let R_A and R_B be Alice's and Bob's local randomness, respectively, and let R be secret common randomness. As depicted in Figure 1, Alice has a transmitter in her laboratory to send quantum states to Bob. At any time instant, the state of the transmitter is described by a density operator on a Hilbert space $\mathcal{H}_Q$. A pure state $|0\rangle\langle 0|$ identifies the "idle" state of the transmitter when there is no communication.[2] Alice prepares a quantum state $\widetilde{\sigma}_{AQ^n} = \mathrm{tr}_{RR_AR_B}\left(\widetilde{\sigma}_{RR_AR_BAQ^n}\right)$ and sends $\widetilde{\sigma}_{Q^n}$ to Bob by n uses of her transmitter. The adversary Eve is assumed to receive the state through a known memoryless quantum channel, which we call *probe*, $\mathcal{E}_{Q\to Q}$ that is *outside its control*. Eve, therefore, obtains the output of $\mathcal{E}_{Q\to Q}^{\otimes n}$ for the input $\widetilde{\sigma}_{Q^n}$, which then interacts with an ancilla E^n in Eve's lab before being transmitted to Bob. The whole operation can be described by an isometry $U_{Q^n\to Q^nE^n}$ (with associated quantum channel $\mathcal{U}_{Q^n\to Q^nE^n}$), in which E^n stays with Eve, while Q^n is passed on to Bob. We call this phase *quantum state distribution*, which results in the joint quantum state

$$\sigma_{RR_AR_BAQ^nE^n} \triangleq (\mathrm{id}_{RR_AR_BA} \otimes \mathcal{U}_{Q^n\to Q^nE^n} \circ \mathcal{E}_{Q\to Q}^{\otimes n})(\widetilde{\sigma}_{RR_AR_BAQ^n}) \tag{7}$$

[2]One can associate a mixed state to no communication, but in bosonic systems, the natural choice for the idle state is a pure vacuum state.

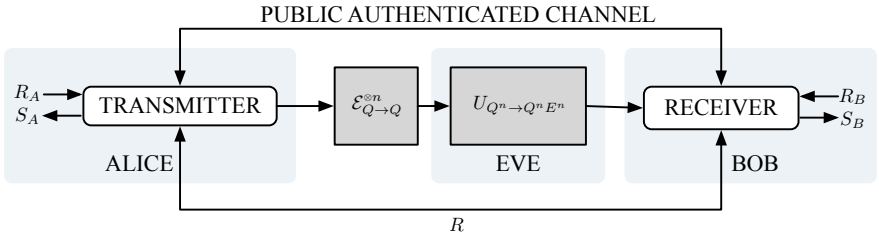

Fig. 1. Covert quantum key expansion model in the presence of Eve

between Alice, Bob, and Eve, respectively. After establishing a shared quantum state, Alice and Bob may interactively communicate over an authenticated classical public channel and perform measurements on their available state to generate keys S_A and S_B, respectively. The target joint distribution of S_A and S_B is such that both S_A and S_B have uniform distribution and they are equal with probability one. We call this phase *quantum key distillation* and formally describe it by a quantum channel $\mathcal{D}_{R_A R_B R A Q^n \to C S_A S_B}$, where C denotes all public communication. The final state is then

$$\sigma_{C S_A S_B E^n} \triangleq (\mathrm{id}_{E^n} \otimes \mathcal{D}_{R_A R_B R A Q^n \to C S_A S_B})(\sigma_{R R_A R_B A Q^n E^n}). \tag{8}$$

Finally, we assume that, in the absence of an adversary, Alice and Bob expect to be connected through the "honest" channel $\mathcal{N}_{Q\to Q}$ *after the probe* (see Fig 2). Alice and Bob can also abort the protocol at any time and do not generate secret keys.

For a particular protocol inducing the final joint state $\sigma_{C S_A S_B E^n}$, we assess the performance of the protocol with the following five quantities:

1) the effective number of generated key bits, i.e., $\mathbb{H}(S_A) - \mathbb{H}(R)$;
2) the probability of error $\mathbb{P}(S_A \neq S_B | \text{not abort})$;
3) the information leakage $\frac{1}{2}\left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \sigma_{E^n C}\right\|_1$;
4) the covertness $\frac{1}{2}\left\|\sigma_{C E^n} - \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1$, where $\rho^{0}_{E^n} \triangleq \mathcal{U}_{Q^n \to E^n}(\mathcal{E}^{\otimes n}_{Q\to Q}(|0\rangle\langle 0|^{\otimes n}))$; and
5) the robustness $\mathbb{P}(\text{abort})$ in the presence of the honest channel $\mathcal{N}_{Q\to Q}$.

Remark 1. *We briefly highlight how the secrecy and the covertness constraints are related. First, note that there exist protocols that satisfy one but not the other. For example, standard QKD protocols are secure but not necessarily covert, and the protocol, in which Alice always transmits* $|0\rangle$ *on the quantum channel and transmits the key over the public channel, is perfectly covert but reveals*

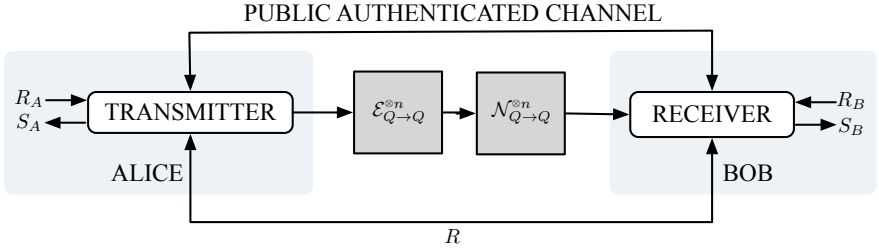

Fig. 2. Covert quantum key expansion model in the absence of Eve

the key to the adversary. Second, an alternative way of formalizing both secrecy and covertness criteria is asking for the single *quantity* $\frac{1}{2}\left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1$ *to be small.*[3] *Guaranteeing that* $\frac{1}{2}\left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1$ *is small implies that* $\frac{1}{2}\left\|\sigma_{E^n C} - \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1$ *and* $\frac{1}{2}\left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \sigma_{E^n C}\right\|_1$ *are small and vice versa because*

$$\left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1 \leqslant \left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \sigma_{E^n C}\right\|_1 + \left\|\rho^{\text{unif}}_{S_A} \otimes \sigma_{E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1 \tag{9}$$

$$= \left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \sigma_{E^n C}\right\|_1 + \left\|\sigma_{E^n C} - \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1, \tag{10}$$

and by the data processing inequality and the triangle inequality,

$$\left\|\sigma_{E^n C} - \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1 \leqslant \left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1 \tag{11}$$

$$\left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \sigma_{E^n C}\right\|_1 \leqslant \left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1 + \left\|\rho^{\text{unif}}_{S_A} \otimes \sigma_{E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1 \tag{12}$$

$$= \left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1 + \left\|\sigma_{E^n C} - \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1 \tag{13}$$

$$\leqslant 2\left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1. \tag{14}$$

We explain here three crucial distinctions between our model and traditional QKD.

1) As covertness is of no concern in QKD, the idle state of the transmitter is not specified in a QKD model.
2) Unlike QKD, in which the quantum channel is in complete control of the adversary, we restrict Eve's observations to result from a known probe $\mathcal{E}_{Q\to Q}$. We discuss this limitation of our model in Section IV.
3) To the best of our knowledge, there is no standard way of defining covertness in the presence of public communication in the literature. We use a covertness criterion similar to [14], in which the mere existence of public communication does not reveal the existence of the protocol; however, when our covertness metric $\frac{1}{2}\left\|\sigma_{C E^n} - \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1$ is small, we effectively require negligible dependence between public communication and σ_{E^n} and that public communication be distributed according to a pre-specified distribution, which

[3]Let S_A have uniform distribution. We can then write $\frac{1}{2}\left\|\sigma_{S_A E^n C} - \rho^{\text{unif}}_{S_A} \otimes \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1 = \frac{1}{K}\sum_s \frac{1}{2}\left\|\sigma^{\text{s}}_{E^n C} - \rho^{\text{unif}}_{C} \otimes \rho^{0}_{E^n}\right\|_1$, where K is the size of the key and $\sigma^{\text{s}}_{E^n C}$ is the state of $E^n C$ when $S_A = s$. This is related to criterion [17, Eq. (5)], which requires $\frac{1}{2}\left\|\sigma^{\text{s}}_{E^n} - \rho^{0}_{E^n}\right\|_1$ to be small for all s.

we choose to be the uniform distribution ρ_C^{unif} for simplicity. These two requirements are critical to ensure that public communication does not help Eve detect the communication over the quantum channel.

IV. Role of the Probe

We now establish a no-go result in the absence of the probe. We measure here the information leakage and the covertness through the relaxed metrics $\frac{1}{2}\left\|\sigma_{S_A C} - \rho_{S_A}^{\text{unif}} \otimes \sigma_C\right\|_1$ and $\frac{1}{2}\|\widetilde{\sigma}_{Q^n} - \rho_{E^n}^0\|_1$, respectively, instead of $\frac{1}{2}\left\|\sigma_{S_A E^n C} - \rho_{S_A}^{\text{unif}} \otimes \sigma_{E^n C}\right\|_1$ and $\frac{1}{2}\left\|\sigma_{C E^n} - \rho_C^{\text{unif}} \otimes \rho_{E^n}^0\right\|_1$. Note that $\frac{1}{2}\left\|\sigma_{S_A C} - \rho_{S_A}^{\text{unif}} \otimes \sigma_C\right\|_1 \leqslant \frac{1}{2}\left\|\sigma_{S_A E^n C} - \rho_{S_A}^{\text{unif}} \otimes \sigma_{E^n C}\right\|_1$ and $\frac{1}{2}\|\widetilde{\sigma}_{Q^n} - \rho_{E^n}^0\|_1 \leqslant \frac{1}{2}\|\sigma_{C E^n} - \rho_C^{\text{unif}} \otimes \rho_{E^n}^0\|_1$ by the data processing inequality. Thus, a converse for the relaxed secrecy and covertness constraints implies a converse for the constraint as defined in Section III.

Theorem 1. *Let $\mathcal{E}_{Q\to Q} = \mathrm{id}_Q$ and define $K \triangleq \log\dim\mathcal{H}_{S_A}$. Consider a protocol that operates as in Section III with $\mathbb{P}(S_A \neq S_B) \leqslant \epsilon$, $\frac{1}{2}\left\|\sigma_{S_A C} - \rho_{S_A}^{\text{unif}} \otimes \sigma_C\right\|_1 \leqslant \delta$, and $\frac{1}{2}\left\|\widetilde{\sigma}_{Q^n} - |0\rangle\langle 0|^{\otimes n}\right\|_1 \leqslant \mu$. We then have*

$$(1 - 5\sqrt{\mu} - \epsilon - 4\delta)K \leqslant \mathbb{H}_b\left(\sqrt{\mu}\right) + \mathbb{H}_b\left(\epsilon + \sqrt{\mu}\right) + 2\left(1 + \sqrt{\mu}\right)\mathbb{H}_b\left(\frac{\sqrt{\mu}}{1+\sqrt{\mu}}\right). \tag{15}$$

Proof. See Appendix A. □

Consequently, if $\epsilon, \delta, \mu \to 0$ then K vanishes, as well. Theorem 1 therefore shows that giving the *complete* control of the channel to the adversary is too stringent to establish covertness. A probe is therefore necessary and could be created with some part of the channel that is protected from the adversary, for example, the portion of an optical fiber that lies inside Alice's laboratory.

Remark 2. *Note that the process modeled as a probe in our formulation should be out of Alice's control. If this were not the case, Alice could always send idle state $|0\rangle$, keep the output of the "environment" of the probe, and run a protocol with Bob to covertly generate a secret key with a* positive *rate.*

V. Description of PPM-MLC-based Protocol

We first provide a high-level description of the role of pulse-position modulation (PPM) and multi-level coding (MLC) in our PPM-MLC-based protocol. The principle of PPM is to split the whole transmission block into smaller sub-blocks and to transmit exactly one non-idle state

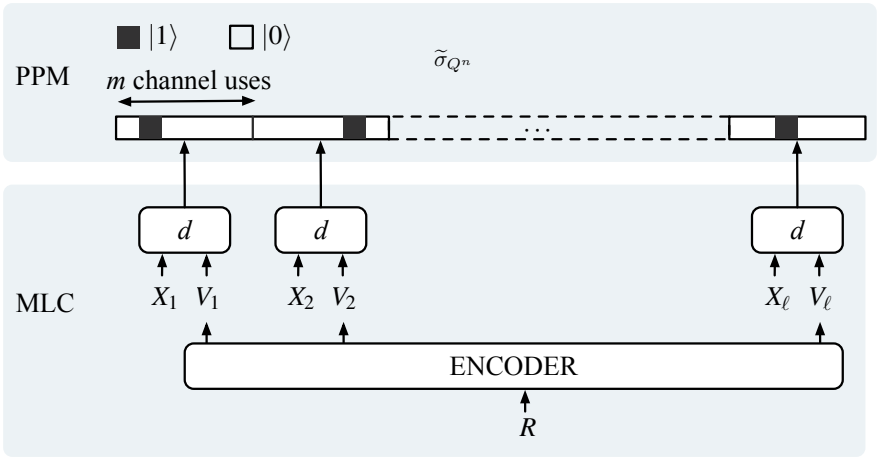

Fig. 3. Covert quantum state distribution through PPM and MLC

in a position chosen uniformly at random in each sub-block. The number of sub-blocks and the size of each sub-block should both be $O(\sqrt{n})$ to achieve covertness [20]. The idea behind MLC is to further split the randomness used to specify the position of the non-idle state into two parts: one part with a fixed size independent of n, generated locally by Alice and used for key generation, and another part of size growing with n, generated secretly and jointly by Alice and Bob and used for mimicking the uniform distribution. This splitting allows Alice and Bob to *partially* coordinate without paying the penalty incurred by a full coordination. The use of MLC converts the problem of covert QKD into a traditional QKD problem over an effective block-length scaling as $O(\sqrt{n})$, for which low-complexity processing is possible. In particular, the last steps of the PPM-MLC-based protocol are similar to a traditional QKD protocol with the additional constraint that the public communication to be uniformly distributed and independent of Eve's observation during the quantum communication phase.

We now elaborate on the details of the partially coordinated PPM-MLC-based protocol (See Appendix E).

a) Quantum state distribution: We fix a non-idle state $|\phi\rangle$ for the transmitter such that

$$\langle\phi|0\rangle \neq 0, \tag{16}$$

$$\operatorname{supp}\left(\mathcal{E}_{Q\to Q}(|\phi\rangle\langle\phi|)\right) \subseteq \operatorname{supp}\left(\mathcal{E}_{Q\to Q}(|0\rangle\langle 0|)\right). \tag{17}$$

We divide the transmissions into ℓ sub-blocks of m channel uses with $n \triangleq m\ell$. Alice transmits $|\phi\rangle$ exactly once in each sub-block and remains idle for the rest of the sub-block, choosing

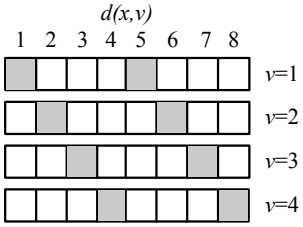

Fig. 4. Illustration of encoding procedure: Gray squares indicate the possible values of $d(x, v)$ for a given value of v when $|\mathcal{X}| = 2$ and $|\mathcal{V}| = 4$.

the position of non-idle state as follows. Let $\mathcal{X}$ and $\mathcal{V}$ be two sets such that $|\mathcal{X}|\,|\mathcal{V}| = m$ and $d : \mathcal{X} \times \mathcal{V} \to [\![1, m]\!]$ be bijective. In the i^{th} sub-block, Alice transmits

$$|0\rangle^{\otimes d(X_i,V_i)-1} \otimes |\phi\rangle \otimes |0\rangle^{\otimes m-d(X_i,V_i)}, \tag{18}$$

where $X^\ell = (X_1, \cdots, X_\ell) \in \mathcal{X}^\ell$ and $V^\ell = (V_1, \cdots, V_\ell) \in \mathcal{V}^\ell$ are sequences generated randomly according to distributions specified below. The crux of the PPM-MLC-based protocol is to generate the sequences X^ℓ and V^ℓ using *different mechanisms:* X^ℓ is generated locally by Alice i.i.d. according to the uniform distribution over $\mathcal{X}$ while V^ℓ is generated jointly by Alice and Bob using an invertible family of hash functions and a common randomness $R \in [\![1, h]\!]$ described as follows. In particular, let $\mathcal{G}$ be an efficiently-invertible two-universal family of hash functions from $\mathcal{V}^\ell \to \mathcal{Z}$ where $\mathcal{Z} = [\![1, \frac{|\mathcal{V}|^\ell}{h}]\!]$ with inverse set denoted by $\mathcal{G}^{-1}$. Bob samples $G^{-1} \in \mathcal{G}^{-1}$ and $Z \in \mathcal{Z}$ uniformly at random and transmits them over the public channel. Alice and Bob then set $V^\ell = G^{-1}(Z, R)$. Bob can discard $m - |\mathcal{X}|$ of his sub-systems in each sub-block of length m, for which he knows that the state $|0\rangle$ is sent (see Fig. 4 for an illustration). We shall later account for the partial coordination through R by subtracting $\log h$ from the number of generated key bits. For each sub-block, Alice therefore obtains the classical state X_i while Bob obtains $|\mathcal{X}|$ received states. We denote the whole state shared between Alice and Bob in ℓ sub-blocks by $\sigma_{X^\ell(Q^{|\mathcal{X}|})^\ell}$.

Remark 3. *We show in Appendix C that Alice and Bob can fix Z to any value z when $|\mathcal{V}|$ is a power of a prime and for a specific $\mathcal{G}$, thereby avoiding the need for transmission of Z over the public channel.*

Remark 4. *In our protocol, we ensure that the state of the output of the probe is close to the*

state of the output of the probe when V^ℓ has uniform distribution. Given the uniform distribution for X, we can define an effective cq-channel from v to the output of the probe described by

$$v \mapsto \frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}} \mathcal{E}^{\otimes|\mathcal{X}|}\left(|0\rangle\langle 0|^{\otimes d(x,v)-1}\otimes|\phi\rangle\langle\phi|\otimes|0\rangle\langle 0|^{\otimes m-d(x,v)}\right). \tag{19}$$

The problem can be then re-stated as choosing a codebook such that the output state of the channel is close to that induced by a uniform input distribution. This is known as quantum channel resolvability and its information-theoretic limits have been characterized [21]. We explicitly constructed here a low-complexity quantum channel resolvability code when the input distribution is uniform similar to [22].

b) Parameter estimation: Let $\sigma_{X^\ell E^n}$ denote the joint state of X^ℓ and Eve's observation from quantum channel. The goal of this phase is to lower-bound $\mathbb{H}^\delta_{\min}(X^\ell|E^n)_\sigma$. We restrict ourselves to attacks in which Eve performs an arbitrary operation on $|\mathcal{X}|$ signals that kept by Bob in a sub-block, but the operation is independent and the same over all sub-blocks (See Remark 5 for a discussion on these attacks). We can then assume that $\sigma_{X^\ell(Q^{|\mathcal{X}|})^\ell E^n} = \tau^{\otimes\ell}_{XQ^{|\mathcal{X}|}E^m}$ for some $\tau_{XQ^{|\mathcal{X}|}E^m}$. Let $\rho^0_{Q^{|\mathcal{X}|}}$ be Bob's observation under the same Eve's attack when Alice sends $|0\rangle\langle 0|^{\otimes|\mathcal{X}|}$. We shall state a lower-bound on $\mathbb{H}^\delta_{\min}(X^\ell|E^n)_\sigma$ in in terms of $F(\tau^x_{Q^{|\mathcal{X}|}}, \rho^0_{Q^{|\mathcal{X}|}})$, which we prove in Section VI-B.

Theorem 2. *We have*

$$\frac{1}{\ell}\mathbb{H}^\delta_{\min}(X^\ell|E^n)_\sigma \geqslant \log|\mathcal{X}| - \mathbb{D}\big(\rho^1_Q\|\rho^0_Q\big) + \frac{1}{|\mathcal{X}|}\sum_x \log\left(1-\eta^x\right) - \left(2\log|\mathcal{X}|+3\right)\sqrt{\frac{\log\frac{1}{\delta}+1}{\ell}}, \tag{20}$$

for all η^x such that

$$F(\tau^x_{Q^{|\mathcal{X}|}}, \rho^0_{Q^{|\mathcal{X}|}}) \leqslant \aleph(\lambda^x, F(|0\rangle\langle 0|, |\phi\rangle\langle\phi|)) - 2\sqrt{1-F(|0\rangle\langle 0|, |\phi\rangle\langle\phi|)}\delta - \delta^2, \tag{21}$$

where

$$\aleph(x,y) \triangleq 1 - \frac{2\sqrt{1-y}x + x^2}{y} - 2\sqrt{\frac{2\sqrt{1-y}x + x^2}{y}}x - x^2, \tag{22}$$

$$\lambda^x \triangleq 2\delta_0 + \sqrt{\eta^x + 4\sqrt{\eta^x}\delta_1 + 4(\delta_1)^2}, \tag{23}$$

$$\delta_1 \triangleq C(|\phi\rangle\langle\phi|, \rho_Q^1), \tag{24}$$

$$\delta_0 \triangleq C(|0\rangle\langle 0|, \rho_Q^0), \tag{25}$$

$$\delta \triangleq \delta_0 + \delta_1. \tag{26}$$

To estimate $F(\tau^x_{Q|\mathcal{X}|}, \rho^0_{Q|\mathcal{X}|})$, Alice selects ℓ_1 positions at random and sends these positions together with the value of X^ℓ at these positions one-time-padded with a secret key over the public channel. Bob then employs a tomography protocol TG (See Table VI) to estimate $F(\tau^x_{Q|\mathcal{X}|}, \rho^0_{Q|\mathcal{X}|})$ for all x. In the sequel, we assume for simplicity that this estimation is perfect. Bob finally computes the lower-bound on $\mathbb{H}^\delta_{\min}(X^\ell|E^n)_\sigma$ as $\widehat{\mathbb{H}}^\delta_{\min}(X^\ell|E^n)_\sigma$ and sends $\lfloor \widehat{\mathbb{H}}^\delta_{\min}(X^\ell|E^n)_\sigma \rfloor$ one-time-padded with a secret key over the public channel. Alice and Bob discard all sub-blocks used in this phase at the end.

Remark 5. *Note that the power of attacks that we consider is somewhere between that of collective and coherent attacks [23]. In particular, these attacks are more powerful than collective attacks because Eve can apply an arbitrary operation* within *each sub-block. One could try the methods developed in [24], [25], [26] to carry over the security analysis to coherent attacks.*

Remark 6. *The right hand side of* (20) *only depends on quantities that are either specified by the protocol and the probe, or could be calculated from Alice's and Bob's observations.*

Remark 7. *The difficulty in obtaining a bound on the adversary's information is the following. Note first that, as detailed in [14], reverse reconciliation only leads to a positive covert throughput if Eve's and Bob's observations are independent when $|0\rangle$ is sent. This is unfortunately not the case when the channel is a beam-splitter. To the best of our knowledge, there exist two standard methods to bound Eve's information for continuous variable QKD protocols. The first method leverages the optimality of the Gaussian attack, which results in a sub-optimal bound on Eve's information for discrete-variable protocols. Since Alice's measurement is not Gaussian (in the entanglement-based version), it is not straightforward to calculate the bound*

for forward reconciliation protocols. The second method exploits entropic uncertainty relations, which would require finding an entanglement-based version with two different measurements at Alice. We could not find such a version of our specific quantum state distribution.

Remark 8. *Note that, in the absence of the adversary,* $\mathbb{I}\big(X;Q^{|\mathcal{X}|}\big)_\sigma = \mathbb{D}\big(\mathcal{N}(\rho_Q^1)\|\mathcal{N}(\rho_Q^0)\big) + O(1/|\mathcal{X}|)$ *[27]. Excluding finite-length effects, we achieve positive covert throughput when*

$$\mathbb{D}\big(\rho_Q^1\|\rho_Q^0\big) - \mathbb{D}\big(\mathcal{N}(\rho_Q^1)\|\mathcal{N}(\rho_Q^0)\big) \leqslant \frac{1}{|\mathcal{X}|}\sum_x \log(1-\eta_x). \tag{27}$$

This inequality holds when $\eta_x > 0$ *and* $\mathcal{N}$ *is close to a noiseless channel.*

c) Information reconciliation: Alice and Bob communicate over the public channel so that Bob decodes X^{ℓ_2} as $\widehat{X}^{\ell_2}$. We assume the existence of an information reconciliation protocol as detailed in Table V. More details to justify the existence of low-complexity reconciliation protocols can be found in [28] and references therein. Furthermore, it is shown in [29] that the public communication could be uniformly distributed and independent of the adversary's observations by using a negligible amount of key.

d) Privacy amplification: As in standard QKD, Alice and Bob use two-universal hash functions to obtain keys with negligible dependence to Eve's observation. Specifically, let $t \triangleq \lfloor \widehat{\mathbb{H}}_{\min}^{\delta}(X^\ell|E^n)_\sigma \rfloor - \mathsf{leak}_{\mathsf{IR}} - 2\log\frac{1}{\delta}$ and $\mathcal{F}_t$ be a family of two-universal hash functions from $\mathcal{X}^{\ell_2}$ to $\{0,1\}^t$. Alice samples a function F from $\mathcal{F}_t$ and transmits F over the public channel. Alice and Bob then set $S_A = F(X^{\ell_A})$ and $S_B = F(\widehat{X}^{\ell_2})$, respectively.

VI. Analysis of PPM-MLC-based Protocol

We analyze the performance of the PPM-MLC-based protocol in this section. Upon defining $\rho_Q^0 \triangleq \mathcal{E}(|0\rangle\langle 0|)$, $\rho_Q^1 \triangleq \mathcal{E}(|\phi\rangle\langle\phi|)$, and $\mu' \triangleq \mu - \sqrt{\frac{\ell}{m}\chi_2(\rho_Q^1\|\rho_Q^0)} - \epsilon_{\mathsf{IR}}^3$, we summarize the performance of the PPM-MLC-based protocol in Table I. We only prove the upper-bound on the covertness constrain in Section VI-A and lower-bound on smooth min-entropy in Section VI-B. The reliability and robustness of the protocol follows from the properties of the information reconciliation protocol in Table V, and the secrecy follows from [5, Lemma 6.4.1].

We now discuss the asymptotic performance of our protocol. Let $\delta, \mu', \epsilon_{\mathsf{IR}}^1, \epsilon_{\mathsf{IR}}^2, \epsilon_{\mathsf{IR}}^3$ be vanishing fast enough with the block-length (e.g., be of order of $2^{-\omega(\log n)}$) and μ arbitrary fixed but small number. We have to set $\ell = \sqrt{\frac{(\mu-\mu'-\epsilon_{\mathsf{IR}}^3)n}{\chi_2(\rho_Q^1\|\rho_Q^0)}}$ to achieve covertness μ. Note that the number of

TABLE I

PERFORMANCE OF THE PPM-MLC-BASED PROTOCOL

Consumed key size	$\frac{\ell}{\lvert\mathcal{X}\rvert}\chi_2(\rho_Q^1\|\rho_Q^0) + \sqrt{\ell}\,(2\log\lvert\mathcal{V}\rvert + 3)\sqrt{\log\frac{2}{\mu'} + 1} + 2\log\frac{1}{\mu'} + O(\ell_1(\log\ell + \log m))$
Generated key size	$\mathbb{H}_{\min}^{\delta}(X^{\ell_2}\lvert E^{m\ell})_\sigma - \mathsf{leak}_{\mathsf{IR}} - 2\log(1/\delta)$
$\mathbb{P}(S_A \neq S_B\lvert\text{not abort})$	ϵ_{IR}^1
$\frac{1}{2}\left\lVert\sigma_{S_A CE^n} - \rho_{S_A}^{\text{unif}} \otimes \sigma_{CE^n}\right\rVert_1$	$3\delta/2$
$\frac{1}{2}\left\lVert\sigma_{CE^n} - \rho_C^{\text{unif}} \otimes \rho_{E^n}^0\right\rVert_1$	μ
$\mathbb{P}(\text{abort}\lvert\text{honest channel})$	ϵ_{IR}^2

generated key is asymptotically $\Theta(\ell_2)$, which is greater than $\alpha\ell_2$ for some $\alpha > 0$. By choosing $\ell_1 = o(\ell/(\log\ell + \log m))$ and $|\mathcal{X}| = \beta\chi_2(\rho_Q^1\|\rho_Q^0)$ for an arbitrary $\beta > 0$ independent of ℓ, the effective number of generated key bits is $(\alpha - \beta^{-1})\ell + o(\ell) = (\alpha - \beta^{-1})\sqrt{\frac{(\mu)n}{\chi_2(\rho_Q^1\|\rho_Q^0)}} + o(\sqrt{n})$ for arbitrary small β^{-1}.

A. Covertness

Theorem 3. *Let $\rho_Q^0 \triangleq \mathcal{E}(|0\rangle\langle 0|)$ and $\rho_Q^1 \triangleq \mathcal{E}(|\phi\rangle\langle\phi|)$. Let μ and h be such that*

$$\mu' \triangleq \mu - \sqrt{\frac{\ell}{m}\chi_2(\rho_Q^1\|\rho_Q^0)} - \epsilon_{\mathsf{IR}}^3 > 0 \tag{28}$$

$$\log h \geqslant \frac{\ell}{|\mathcal{X}|}\chi_2(\rho_Q^1\|\rho_Q^0) + \sqrt{\ell}\,(2\log|\mathcal{V}| + 3)\sqrt{\log\frac{2}{\mu'} + 1} + 2\log\frac{1}{\mu'}. \tag{29}$$

We then have

$$\frac{1}{2}\left\|\sigma_{E^n C} - \rho_{E^n}^0 \otimes \rho_C^{\text{unif}}\right\|_1 \leqslant \mu. \tag{30}$$

Proof. We exclude from our analysis the public communication for parameter estimation phase because it is one-time-padded with a secret shared key as well as transmission of F over the public channel for privacy amplification because it has uniform distribution and is independent of all previous randomness in the protocol. Hence, we assume that $C = (G^{-1}, Z, C_{\mathsf{IR}})$ where G^{-1} and Z are defined in Section V and C_{IR} is the public communication during information

reconciliation phase. We can thus write

$$\frac{1}{2}\left\|\sigma_{E^nC} - \rho^0_{E^n} \otimes \rho^{\text{unif}}_C\right\|_1 \tag{31}$$

$$\overset{(a)}{=} \frac{1}{2}\left\|\sigma_{E^nG^{-1}ZC_{\mathsf{IR}}} - \rho^0_{E^n} \otimes \rho^{\text{unif}}_{G^{-1}} \otimes \rho^{\text{unif}}_Z \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}}\right\|_1 \tag{32}$$

$$\overset{(b)}{=} \frac{1}{2}\left\|\sigma_{E^nG^{-1}ZC_{\mathsf{IR}}} - \sigma_{E^nG^{-1}Z} \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}}\right\|_1 + \frac{1}{2}\left\|\sigma_{E^nG^{-1}Z} \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}} - \rho^0_{E^n} \otimes \rho^{\text{unif}}_{G^{-1}} \otimes \rho^{\text{unif}}_Z \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}}\right\|_1 \tag{33}$$

$$\overset{(c)}{\leqslant} \frac{1}{2}\left\|\sigma_{E^nC_{\mathsf{IR}}} - \sigma_{E^n} \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}}\right\|_1 + \frac{1}{2}\left\|\sigma_{E^nG^{-1}Z} \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}} - \rho^0_{E^n} \otimes \rho^{\text{unif}}_{G^{-1}} \otimes \rho^{\text{unif}}_Z \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}}\right\|_1 \tag{34}$$

$$\overset{(d)}{\leqslant} \epsilon^3_{\mathsf{IR}} + \frac{1}{2}\left\|\sigma_{E^nG^{-1}Z} \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}} - \rho^0_{E^n} \otimes \rho^{\text{unif}}_{G^{-1}} \otimes \rho^{\text{unif}}_Z \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}}\right\|_1 \tag{35}$$

$$\overset{(e)}{=} \epsilon^3_{\mathsf{IR}} + \frac{1}{2}\left\|\sigma_{E^nG^{-1}Z} - \rho^0_{E^n} \otimes \rho^{\text{unif}}_{G^{-1}} \otimes \rho^{\text{unif}}_Z\right\|_1, \tag{36}$$

where (a) follows from $\rho^{\text{unif}}_C = \rho^{\text{unif}}_{G^{-1}} \otimes \rho^{\text{unif}}_Z \otimes \rho^{\text{unif}}_{C_{\mathsf{IR}}}$ by definition of uniform distributions, (b) follows from the triangle inequality, (c) follows since IR does not depend on G^{-1} and Z, (d) follows from our assumption about IR (See Table V), and (e) follows since $\|\rho \otimes \omega - \sigma \otimes \omega\|_1 = \|\rho - \sigma\|_1$ for all density operators ρ, σ, ω.

We need some notation before proceeding further. We first define

$$\rho^{x^\ell, v^\ell}_{Q^n} \triangleq \bigotimes_{i=1}^{\ell} \mathcal{E}^{\otimes|\mathcal{X}|}\left(|0\rangle\langle 0|^{\otimes d(x_i,v_i)-1} \otimes |\phi\rangle\langle\phi| \otimes |0\rangle\langle 0|^{\otimes m-d(x_i,v_i)}\right) \tag{37}$$

$$\rho_{Q^nV^\ell} \triangleq \frac{1}{|\mathcal{X}|^\ell |\mathcal{V}|^\ell} \sum_{x^\ell, v^\ell} \rho^{x^\ell, v^\ell}_{Q^n} \otimes |v^\ell\rangle\langle v^\ell|. \tag{38}$$

In other words, $\rho^{x^\ell, v^\ell}_{Q^n}$ is the output state of the probe when $X^\ell = x^\ell$ and $V^\ell = v^\ell$ in our protocol. We also define $\widetilde{\tau}_{Q^nG^{-1}Z}$ as the joint state of the probe output, G^{-1} and Z, which can be written as

$$\frac{1}{h\,|\mathcal{Z}|\,|\mathcal{G}^{-1}|\,|\mathcal{X}|^\ell} \sum_{r\in[\![1,h]\!], z\in\mathcal{Z}, g^{-1}\in\mathcal{G}^{-1}, x^\ell\in\mathcal{X}^\ell} \rho^{x^n, g^{-1}(z,r)}_{Q^n} \otimes |g^{-1}, z\rangle\langle g^{-1}, z|. \tag{39}$$

Note that

$$\frac{1}{2}\left\|\sigma_{E^nG^{-1}Z} - \rho^0_{E^n} \otimes \rho^{\text{unif}}_{G^{-1}} \otimes \rho^{\text{unif}}_Z\right\|_1 \overset{(a)}{\leqslant} \frac{1}{2}\left\|\sigma_{Q^nE^nG^{-1}Z} - \rho^0_{Q^nE^n} \otimes \rho^{\text{unif}}_{G^{-1}} \otimes \rho^{\text{unif}}_Z\right\|_1 \tag{40}$$

$$\overset{(b)}{=} \frac{1}{2}\left\|\widetilde{\tau}_{Q^nG^{-1}Z} - \left(\rho^0_Q\right)^{\otimes n} \otimes \rho^{\text{unif}}_{G^{-1}} \otimes \rho^{\text{unif}}_Z\right\|_1, \tag{41}$$

where (a) follows by monotonicity of the trace norm w.r.t. partial trace, and (b) follows since the map $U^{\dagger}_{Q^nE^n}U_{Q^n\to Q^nE^n}$ restricted to $\mathrm{im}(U_{Q^n\to Q^nE^n})$ is unitary and hence the trace norm is invariant under this map. We also have

$$\frac{1}{2}\big\|\widetilde{\tau}_{Q^nG^{-1}Z}-\big(\rho_Q^0\big)^{\otimes n}\otimes\rho_{G^{-1}}^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}\big\|_1 \tag{42}$$

$$\leqslant\frac{1}{2}\big\|\widetilde{\tau}_{Q^nG^{-1}Z}-\rho_{Q^n}\otimes\rho_{G^{-1}}^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}\big\|_1+\frac{1}{2}\big\|\rho_{Q^n}\otimes\rho_{G^{-1}}^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}-\big(\rho_Q^0\big)^{\otimes n}\otimes\rho_{G^{-1}}^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}\big\|_1. \tag{43}$$

We first upper-bound the second term in Eq. (43) as

$$\frac{1}{2}\big\|\rho_{Q^n}\otimes\rho_{G^{-1}}^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}-\big(\rho_Q^0\big)^{\otimes n}\otimes\rho_{G^{-1}}^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}\big\|_1=\frac{1}{2}\big\|\rho_{Q^n}-\big(\rho_Q^0\big)^{\otimes n}\big\|_1 \tag{44}$$

$$\overset{(a)}{\leqslant}\sqrt{\frac{1}{2}\mathbb{D}\big(\rho_{Q^n}\|\,\big(\rho_Q^0\big)^{\otimes n}\big)} \tag{45}$$

$$\overset{(b)}{\leqslant}\sqrt{\frac{\ell}{2m}\chi_2(\rho_Q^1\|\rho_Q^0)}, \tag{46}$$

where (a) follows from Pinsker's inequality [19, Th. 11.9.1], and (b) follows from [30, Eq. (B144)].[4]

Therefore, establishing covertness amounts to proving that the state $\widetilde{\tau}_{Q^nG^{-1}Z}$ generated by the protocol is nearly identical to $\rho_{Q^n}\otimes\rho_{G^{-1}}^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}$. We recall $\mu'\triangleq\mu-\sqrt{\frac{\ell}{m}\chi_2(\rho_Q^1\|\rho_Q^0)}-\epsilon_{\mathsf{IR}}^3$. We now deploy Lemma 2 in Appendix B to obtain

$$\frac{1}{2}\big\|\widetilde{\tau}_{Q^nG^{-1}Z}-\rho_{Q^n}\otimes\rho_{G^{-1}}^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}\big\|_1\leqslant\mu-\sqrt{\frac{\ell}{m}\chi_2(\mathcal{E}(|\phi\rangle\langle\phi|)\|\mathcal{E}(|0\rangle\langle0|))}-\epsilon_{\mathsf{IR}}^3=\mu', \tag{47}$$

provided that

$$\log h\geqslant\log\big|\mathcal{V}^\ell\big|+\mathbb{H}_{\min}^{\frac{\mu'}{2}}(V^\ell|Q^n)_\rho+2\log\frac{1}{\mu'}. \tag{48}$$

Hence, it remains to show that our assumption in Eq. (29) implies Eq. (48). Note that the state $\rho_{Q^nV^\ell}$ defined in Eq (38) has product structure, i.e., $\rho_{Q^nV^\ell}=(\rho'_{Q^mV})^{\otimes\ell}$, where

$$\rho'_{Q^mV}\triangleq\frac{1}{|\mathcal{X}|\,|\mathcal{V}|}\sum_{x,v}\mathcal{E}^{\otimes|\mathcal{X}|}\left(|0\rangle\langle0|^{\otimes d(x,v)-1}\otimes|\phi\rangle\langle\phi|\otimes|0\rangle\langle0|^{\otimes m-d(x,v)}\right)\otimes|v\rangle\langle v| \tag{49}$$

[4]In the classical setting, the authors of [27] showed the upper-bound with a factor of $1/2$ on the right hand side. While we conjecture that an extension of such upper-bound to the quantum setting is possible, we could only prove the upper-bound without the factor $1/2$.

We therefore have

$$\log|\mathcal{V}|^{\ell}-\mathbb{H}_{\min}^{\frac{\mu'}{2}}(V^{\ell}|Q^{n})_{\rho}\overset{(a)}{\leqslant}\log|\mathcal{V}|^{\ell}-\ell\left(\mathbb{H}(V|Q^{m})_{\rho'}-(2\mathbb{H}_{\max}(V)_{\rho'}+3)\sqrt{\frac{\log\frac{2}{\mu'}+1}{\ell}}\right) \tag{50}$$

$$\overset{(b)}{=}\ell\mathbb{I}(V;Q^{m})_{\rho'}+\sqrt{\ell}\,(2\log|\mathcal{V}|+3)\sqrt{\log\frac{2}{\mu'}+1}, \tag{51}$$

where (a) follows from [5, Corollary 3.3.7] and (b) follows since ${\rho'}_V$ is a mixed state. We also upper-bound $\mathbb{I}(V;Q^m)_{\rho'}$ by

$$\mathbb{I}(V;Q^{m})_{\rho'}=\mathbb{D}\big({\rho'}_{VQ^m}\|\rho'_V\otimes\rho'_{Q^m}\big) \tag{52}$$

$$=\mathbb{D}\big(\rho'_{VQ^m}\|\rho'_V\otimes\big(\rho_Q^0\big)^{\otimes m}\big)-\mathbb{D}\big(\rho'_{Q^m}\|\big(\rho_Q^0\big)^{\otimes m}\big) \tag{53}$$

$$\leqslant\mathbb{D}\big(\rho'_{VQ^m}\|\rho'_V\otimes\big(\rho_Q^0\big)^{\otimes m}\big) \tag{54}$$

$$\overset{(a)}{=}\frac{1}{|\mathcal{V}|}\sum_{v\in\mathcal{V}}\mathbb{D}\left(\frac{1}{|\mathcal{X}|\,|\mathcal{V}|}\sum_{x,v}\mathcal{E}^{\otimes|\mathcal{X}|}\left(|0\rangle\langle 0|^{\otimes d(x,v)-1}\otimes|\phi\rangle\langle\phi|\otimes|0\rangle\langle 0|^{\otimes m-d(x,v)}\right)\|\left(\rho_Q^0\right)^{\otimes m}\right) \tag{55}$$

$$\overset{(b)}{\leqslant}\frac{1}{|\mathcal{X}|}\chi_2(\rho_Q^1\|\rho_Q^0), \tag{56}$$

where (a) follows from $\mathbb{D}(\rho_{XA}\|\rho_X\otimes\sigma_A)=\sum_x P_X(x)\mathbb{D}(\rho_A^x\|\sigma_A)$ for any cq-state $\rho_{XA}=\sum_x P_X(x)|x\rangle\langle x|\otimes\rho_A^x$ and any state σ_A and (b) follows from the symmetry in the definition of ρ_{VQ^m} and [30, Eq. (B144)]. □

B. Security

The objective of this section is proving Theorem 2, which provides a lower-bound on the smooth min-entropy of Alice's data X^ℓ given Eve's observations. We first state a general upper bound for the relative entropy between the outputs of the complementary channel for two fixed states.

Theorem 4. *Let A and B be two possibly infinite dimensional quantum systems such that system A is a composition of two sub-systems A' and A''. Let ρ_A^0 and ρ_A^1 be in $\mathcal{D}(\mathcal{H}_A)$ such that for two pure states $|\phi^0\rangle_{A'}$ and $|\phi^1\rangle_{A'}$ in $\mathcal{H}_{A'}$ and a mixed state $\nu_{A''}$ in $\mathcal{D}(\mathcal{H}_{A''})$, we have*

$C(\phi^x_{A'} \otimes \nu_{A''}, \rho^x_A) \leqslant \delta_x$. *Let* $\mathcal{N} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$ *be a quantum channel with a complementary channel* $\mathcal{E} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_E)$. *Suppose that* $\eta > 0$ *satisfies*

$$F(\mathcal{N}(\rho^1_A), \mathcal{N}(\rho^0_A)) \leqslant \aleph(\lambda, F(\phi^1_{A'}, \phi^0_{A'})) - 2\sqrt{1 - F(\phi^1_{A'}, \phi^0_{A'})}\delta - \delta^2 \tag{57}$$

where $\lambda \triangleq 2\delta_0 + \sqrt{\eta + 4\sqrt{\eta}\delta_1 + 4\delta_1^2}$, $\delta \triangleq \delta_0 + \delta_1$.

We then have

$$\mathbb{D}\big(\mathcal{E}(\rho^1_A) \| \mathcal{E}(\rho^0_A)\big) \leqslant \mathbb{D}\big(\rho^1_A \| \rho^0_A\big) + \log(1 - \eta). \tag{58}$$

Proof. See Appendix D. □

We are now ready to prove Theorem 2. By [5, Corollary 3.3.7], we have

$$\frac{1}{\ell}\mathbb{H}^{\delta}_{\min}\left(X^\ell | E^n\right)_\sigma \geqslant \mathbb{H}(X|E^m)_\tau - (2\mathbb{H}_{\max}(X)_\tau + 3)\sqrt{\frac{\log\frac{1}{\delta} + 1}{\ell}} \tag{59}$$

$$= \mathbb{H}(X|E^m)_\tau - (2\log|\mathcal{X}| + 3)\sqrt{\frac{\log\frac{1}{\delta} + 1}{\ell}}. \tag{60}$$

Furthermore,

$$\mathbb{H}(X|E^m)_\tau = \mathbb{H}(X)_\tau - \mathbb{I}(X; E^m)_\tau = \log|\mathcal{X}| - \mathbb{I}(X; E^m)_\tau. \tag{61}$$

Note now that

$$\mathbb{I}(X; E^m)_\tau = \mathbb{D}(\tau_{XE^m} \| \tau_X \otimes \tau_{E^m}) \tag{62}$$

$$= \mathbb{D}\big(\tau_{XE^m} \| \tau_X \otimes \rho^0_{E^m}\big) - \mathbb{D}\big(\tau_{E^m} \| \rho^0_{E^m}\big) \tag{63}$$

$$\leqslant \mathbb{D}\big(\tau_{XE^m} \| \tau_X \otimes \rho^0_{E^m}\big) \tag{64}$$

$$\overset{(a)}{=} \frac{1}{|\mathcal{X}|}\sum_{x=1}^{|\mathcal{X}|} \mathbb{D}\big(\tau^x_{E^m} \| \rho^0_{E^m}\big), \tag{65}$$

where (a) follows from $\mathbb{D}(\rho_{XA} \| \rho_X \otimes \sigma_A) = \sum_x P_X(x)\mathbb{D}(\rho^x_A \| \sigma_A)$ for any cq-state $\rho_{XA} = \sum_x P_X(x)|x\rangle\langle x| \otimes \rho^x_A$ and any state σ_A. Since η_x satisfies the condition in (57) by (21), We can apply Theorem 4 to obtain

$$\mathbb{D}\big(\tau^x_{E^m} \| \rho^0_{E^m}\big) \leqslant \mathbb{D}\big(\rho^1_Q \| \rho^0_Q\big) + \log(1 - \eta_x). \tag{66}$$

Combining the above inequalities, we obtain the result.

C. Example

We present here an experimental setup over which our proposed scheme could be executed. As illustrated in Fig. 5, Alice's transmitter is a laser whose output is a single-mode bosonic system. The idle state is $|0\rangle$ and we choose a *coherent* state $|\alpha\rangle$ as the non-idle state. The probe and the honest channel are both beam-splitters with transmissivity τ_E and τ_N, respectively, and excess noise $\overline{n}_E$ and $\overline{n}_N$, respectively. In Fig. 6, we plot the number of bits per PPM symbol versus τ_N for $\tau_E = 0.9994$, $\alpha = 0.6$, $\overline{n}_E = 11$, and $\overline{n}_N = 0.01$. For these parameters, we also have $\chi_2(\mathcal{E}(|0\rangle\langle 0|)\|\mathcal{E}(|\alpha\rangle\langle\alpha|)) = 5.9881934 \times 10^7$, which controls the covertness through Theorem 3. This example shows the possibility of covert and secret key expansion over a practical quantum channel although the efficiency is very low.

CONCLUSION

We have developed a protocol based on PPM and MLC for the expansion of a secret key, for which we established information-theoretic secrecy of the generated keys and covertness of the protocol with respect to an adversary restricted to observing the output of a probe outside its control but otherwise only limited by the laws of quantum mechanics. We have also demonstrated the performance of our protocol for a bosonic channel. Although the range of channel parameters is narrow and the efficiency is very low, this example shows the possibility of covert QKD in settings not envisioned earlier. We believe that two factors cause the low efficiency of our protocol: the stringent constraint of covertness and our sub-optimal bounds on Eve's information. The former factor is, in our opinion, more crucial because the optimal throughput under covertness constraint is small even with the knowledge of Eve's attack (See Fig. 6). There is a loss of order $\approx 10^{-2}$ to $\approx 10^{-3}$ because of the estimation of Eve's attack. Using many optical modes at once [31] and developing tighter bounds for Eve's information could mitigate this low efficiency.

ACKNOWLEDGEMENT

This work was supported by NSF under Award 1910859.

APPENDIX A
PROOF OF THEOREM 1

We first prove a quantum counterpart of [32, Lemma 2.2].

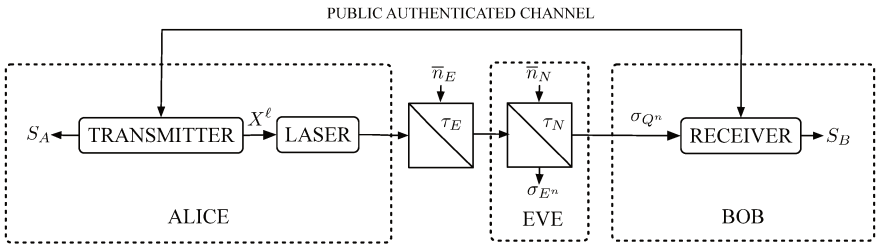

Fig. 5. Experimental setup for our protocol.

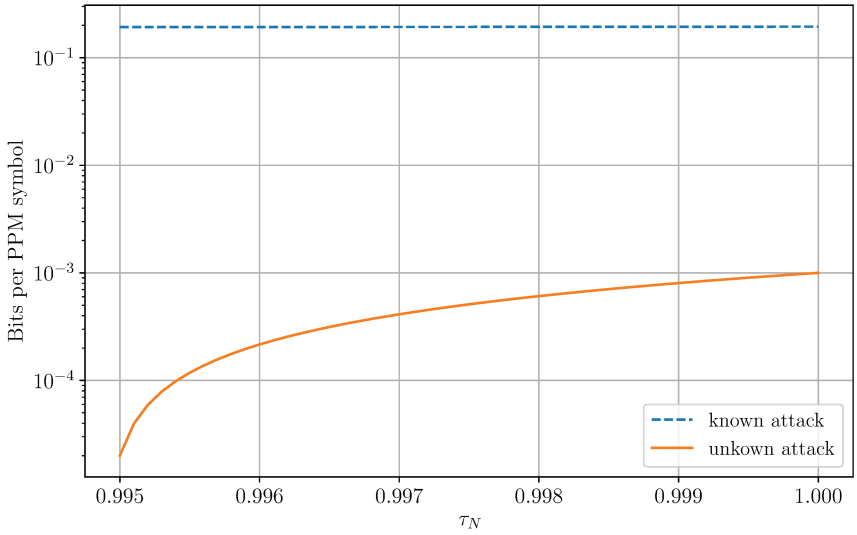

Fig. 6. Achievable number of key bits per PPM symbol.

Lemma 1. *Let ρ_{AB} be a bipartite state and $\mathcal{E}_{A\to AF}$ be a quantum channel. We then have*

$$\mathbb{I}(A;B)_{\rho} \geqslant \mathbb{I}(A;B|F)_{\rho'}, \tag{67}$$

where $\rho'_{ABF} \triangleq (\mathcal{E}_{A\to AF} \otimes \mathrm{id}_B)(\rho_{AB})$.

Proof. We have

$$\mathbb{I}(A;B|F)_{\rho'} = \mathbb{H}(B|F)_{\rho'} - \mathbb{H}(B|FA)_{\rho'} \tag{68}$$

$$\overset{(a)}{\leqslant} \mathbb{H}(B)_{\rho'} - \mathbb{H}(B|FA)_{\rho'} \tag{69}$$

$$= \mathbb{I}(AF;B)_{\rho'} \tag{70}$$

$$= \mathbb{D}(\rho'_{ABF}\|\rho'_{AF}\otimes\rho') \tag{71}$$

$$\overset{(b)}{\leqslant} \mathbb{D}(\rho_{AB}\|\rho_A\otimes\rho_B) = \mathbb{I}(A;B)_{\rho}, \tag{72}$$

where (a) follows from the sub-additivity of the von Neumann entropy, and (b) follows from the data processing inequality. □

Proof of Theorem 1. Let $\widetilde{\sigma}_{AQ^n}$ be the state initially prepared by Alice such that $\frac{1}{2}\left\|\widetilde{\sigma}_{Q^n} - |0\rangle\langle 0|^{\otimes n}\right\|_1 \leqslant \mu$. We then have

$$F(\widetilde{\sigma}_{Q^n}, |0\rangle\langle 0|^{\otimes n}) \geqslant 1-\mu. \tag{73}$$

Let $\widetilde{\sigma}_{RAQ^n}$ be a purification of $\widetilde{\sigma}_{AQ^n}$. By Uhlmann's theorem, there exists a unit vector $|\phi\rangle_{RA}$ such that

$$F(\widetilde{\sigma}_{RAQ^n}, \phi_{RA}\otimes|0\rangle\langle 0|^{\otimes n}) \geqslant 1-\mu. \tag{74}$$

Let $\widetilde{\tau}_{AQ^n} \triangleq \mathrm{tr}_R\left(|\phi\rangle\langle\phi|_{RA}\right)\otimes|0\rangle\langle 0|^{\otimes n}$ and $\tau_{CS_AS_BE^n}$ be the output of the protocol if Alice initially prepares $\widetilde{\tau}_{AQ^n}$ instead of $\widetilde{\sigma}_{AQ^n}$. By monotonicity of the fidelity, we have $F(\widetilde{\tau}_{AQ^n}, \widetilde{\sigma}_{AQ^n}) \geqslant 1-\mu$, and therefore, $\frac{1}{2}\|\widetilde{\tau}_{AQ^n} - \widetilde{\sigma}_{AQ^n}\|_1 \leqslant \sqrt{\mu}$. By the data processing inequality, we also have $\frac{1}{2}\|\tau_{CS_AS_BE^n} - \sigma_{CS_AS_BE^n}\|_1 \leqslant \sqrt{\mu}$. This implies that $\mathbb{P}(S_A \neq S_B)_\tau \leqslant \epsilon + \sqrt{\mu}$. We can write the number of generated bits as

$$K = \mathbb{H}(S_A)_\sigma + \mathbb{D}\big(\sigma_{S_A}\|\rho^{\mathrm{unif}}_{S_A}\big) \tag{75}$$

$$\overset{(a)}{\leqslant} \mathbb{H}(S_A)_\sigma + \left\|\sigma_{S_A} - \rho^{\mathrm{unif}}_{S_A}\right\|_1 K \tag{76}$$

$$\overset{(b)}{\leqslant} \mathbb{H}(S_A)_\sigma + \left\|\sigma_{S_AC} - \rho^{\mathrm{unif}}_{S_A}\otimes\sigma_C\right\|_1 K \tag{77}$$

$$\leqslant \mathbb{H}(S_A)_\sigma + 2\delta K \tag{78}$$

$$\overset{(c)}{\leqslant} \mathbb{H}(S_A)_\tau + \sqrt{\mu}K + \mathbb{H}_b\left(\sqrt{\mu}\right) + 2\delta K \tag{79}$$

$$= \mathbb{H}(S_A|C)_\tau + \mathbb{I}(S_A;C)_\tau + \sqrt{\mu}K + \mathbb{H}_b\left(\sqrt{\mu}\right) + 2\delta K, \tag{80}$$

where (a) follows from [33, Eq. (360)], (b) follows from the data processing inequality, and (c) follows from Fannes' inequality. By [19, Exercise 11.10.2], we also have

$$\mathbb{I}(S_A;C)_\tau \leqslant \mathbb{I}(S_A;C)_\sigma + 3\sqrt{\mu}K + 2(1+\sqrt{\mu})\mathbb{H}_b\left(\frac{\sqrt{\mu}}{1+\sqrt{\mu}}\right). \tag{81}$$

Writing the classical state σ_{S_AC} as $\sum_c P_C(c)\sigma^c_{S_A}\otimes|c\rangle\langle c|$, we have

$$\begin{aligned}
\mathbb{I}(S_A;C)_\sigma &\leqslant \mathbb{D}\big(\sigma_{S_AC}\|\rho^{\text{unif}}_{S_A}\otimes\sigma_C\big) && (82)\\
&= \sum_c P_C(c)\mathbb{D}\big(\sigma^c_{S_A}\|\rho^{\text{unif}}_{S_A}\big) && (83)\\
&\overset{(a)}{\leqslant} \sum_c P_C(c)\big\|\sigma^c_{S_A}-\rho^{\text{unif}}_{S_A}\big\|_1 K && (84)\\
&= \big\|\sigma_{S_AC}-\rho^{\text{unif}}_{S_A}\otimes\sigma_C\big\|_1 K && (85)\\
&\leqslant 2\delta K, && (86)
\end{aligned}$$

where (a) follows from [33, Eq. (360)].

Using Fano's inequality, we obtain

$$\begin{aligned}
\mathbb{H}(S_A|C)_\tau &\leqslant \mathbb{I}(S_A;S_B|C)_\tau + \mathbb{H}_b\left(\epsilon+\sqrt{\mu}\right) + \left(\epsilon+\sqrt{\mu}\right)K && (87)\\
&\overset{(a)}{\leqslant} \mathbb{I}(A;Q^n)_\tau + \mathbb{H}_b\left(\epsilon+\sqrt{\mu}\right) + \left(\epsilon+\sqrt{\mu}\right)K && (88)\\
&\overset{(b)}{\leqslant} \mathbb{I}(A;Q^n)_{\widetilde{\tau}} + \mathbb{H}_b\left(\epsilon+\sqrt{\mu}\right) + \left(\epsilon+\sqrt{\mu}\right)K && (89)\\
&\overset{(c)}{=} \mathbb{H}_b\left(\epsilon+\sqrt{\mu}\right) + \left(\epsilon+\sqrt{\mu}\right)K, && (90)
\end{aligned}$$

where (a) follows from using Lemma 1 for each use of the public channel, (b) follows from data processing inequality, and (c) follows since $\widetilde{\tau}_{AQ^n} = \widetilde{\tau}_A\otimes\widetilde{\tau}_{Q^n}$. Combining (80), (81), (86), and (90), we obtain the desired bound. □

APPENDIX B
A QUANTUM RESOLVABILITY RESULT

We prove a quantum channel resolvability result based on the privacy amplification result of [5]. Note that we cannot use the standard quantum resolvability result of [21, Lemma 9.2] since the construction is not low-complexity and also the bound depends on the dimension of the output space, which itself grows exponentially. We start by recalling a privacy amplification result.

Proposition 1 ([5]). *Let ρ_{XA} be a cq state on $\mathcal{H}_X \otimes \mathcal{H}_A$ with respect to an orthonormal basis $\{|x\rangle : x \in \mathcal{X}\}$ for $\mathcal{H}_X$, and $\mathcal{G}$ be a two-universal family of functions from $\mathcal{X}$ to $\mathcal{Z}$. We then have*

$$\frac{1}{2}\left\| \frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}} (\mathrm{id}_G \otimes \mathcal{E}^g_{X\to Z} \otimes \mathrm{id}_A)(|g\rangle\langle g| \otimes \rho_{XA}) - \rho_G^{\mathrm{unif}} \otimes \rho_Z^{\mathrm{unif}} \otimes \rho_A \right\|_1 \leqslant \inf_{\epsilon\geqslant 0}\left[\epsilon + 2^{-\frac{1}{2}\left(\mathbb{H}^\epsilon_{\min}(X|A)_\rho - \log|\mathcal{Z}|\right)-1}\right] \quad (91)$$

We are now ready to establish the main result of this section, which shows the existence of a resolvability code. The classical counter-part of this result was proved in [16].

Let $\rho_{XA} = \sum_{x\in\mathcal{X}} \frac{1}{|\mathcal{X}|}|x\rangle\langle x| \otimes \rho_A^x$ be a cq state on $\mathcal{H}_X \otimes \mathcal{H}_A$. Let $\mathcal{G}$ be an invertible two-universal family of hash functions from $\mathcal{X}$ to $\mathcal{Z}$ Let G^{-1}, Z and R be independent and be uniformly distributed over $\mathcal{G}^{-1}$, $\mathcal{Z}$, and $[\![1, |\mathcal{X}|\,/\,|\mathcal{Z}|]\!]$, respectively. We define $\rho_{AG^{-1}ZR} \triangleq \sum_{g^{-1},z,r} \frac{1}{|\mathcal{G}^{-1}||\mathcal{X}|}\rho_A^{g^{-1}(z,r)}|g^{-1},z,r\rangle\langle g^{-1},z,r|$ (one can check that this is consistent with definition of ρ_{AX}).

Lemma 2. *Let $\delta > 0$ be such that*

$$\log\frac{|\mathcal{X}|}{|\mathcal{Z}|} \geqslant \log|\mathcal{X}| - \mathbb{H}^{\frac{\delta}{2}}_{\min}(X|A)_\rho + 2\log\frac{1}{\delta}. \quad (92)$$

We then have

$$\frac{1}{2}\left\|\rho_{AG^{-1}Z} - \rho_A \otimes \rho^{\mathrm{unif}}_{G^{-1}} \otimes \rho^{\mathrm{unif}}_Z\right\|_1 \leqslant \delta. \quad (93)$$

Proof. Note that

$$\frac{1}{2}\left\|\rho_{AG^{-1}Z} - \rho_A \otimes \rho^{\mathrm{unif}}_{G^{-1}} \otimes \rho^{\mathrm{unif}}_Z\right\|_1 \overset{(a)}{=} \frac{1}{|\mathcal{G}^{-1}|\,|\mathcal{Z}|}\sum_{g^{-1},z}\frac{1}{2}\left\|\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{r\in[\![1,|\mathcal{X}|/|\mathcal{Z}|]\!]}\rho_A^{g^{-1}(z,r)} - \rho_A\right\|_1 \quad (94)$$

$$\overset{(b)}{=} \frac{1}{|\mathcal{G}|\,|\mathcal{Z}|}\sum_{g,z}\frac{1}{2}\left\|\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{x\in g^{-1}(z)}\rho_A^x - \rho_A\right\|_1 \quad (95)$$

where (a) follows from $\|\sigma_{XA} - \sigma_X \otimes \tau_A\|_1 = \sum_x P_X(x)\|\sigma_A^x - \tau_A\|_1$ for any cq state $\sigma_{XA} = \sum_x P_X(x)|x\rangle\langle x| \otimes \sigma_A^x$ and quantum state τ_A, and (b) follows from the definition of $\mathcal{G}^{-1}$ (See

Section II). We also have

$$\frac{1}{|\mathcal{G}|\,|\mathcal{Z}|}\sum_{g,z}\frac{1}{2}\left\|\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{x\in g^{-1}(z)}\rho_A^x-\rho_A\right\|_1 \tag{96}$$

$$=\frac{1}{2}\left\|\frac{1}{|\mathcal{G}|\,|\mathcal{Z}|}\sum_{g\in\mathcal{G},z\in\mathcal{Z}}|g,z\rangle\langle g,z|\otimes\left(\frac{1}{h}\sum_{x\in g^{-1}(z)}\rho_A^x-\rho_A\right)\right\|_1 \tag{97}$$

$$\overset{(a)}{=}\frac{1}{2}\left\|\frac{1}{|\mathcal{G}|}\sum_{g\in\mathcal{G}}(\mathrm{id}_G\otimes\mathcal{E}^g_{X\to Z}\otimes\mathrm{id}_A)(|g\rangle\langle g|\otimes\rho_{XA})-\rho_G^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}\otimes\rho_A\right\|_1, \tag{98}$$

where (a) follows since by definition of $\mathcal{E}^g_{X\to Z}$ and ρ_{XA}, we have

$$(\mathcal{E}^g_{X\to Z}\otimes\mathrm{id}_A)(\rho_{XA})=\frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}}|g(x)\rangle\langle g(x)|\otimes\rho_A^x \tag{99}$$

$$=\frac{1}{|\mathcal{Z}|}\sum_{z\in\mathcal{Z}}|z\rangle\langle z|\otimes\left(\frac{1}{h}\sum_{x\in g^{-1}(z)}\rho_A^x\right). \tag{100}$$

Employing Proposition 1 and setting $\epsilon=\delta/2$ complete the proof. □

APPENDIX C
REDUCING PUBLIC COMMUNICATION WHEN $|\mathcal{V}|$ IS A POWER OF PRIME

In the setting of Lemma 2 in Appendix B, we show that the choice of z does not matter under symmetry conditions on $\mathcal{G}$ and ρ_{XA},.

Lemma 3. *Suppose that for all $g\in\mathcal{G}$, $z,z'\in\mathcal{Z}$, there exist a bijection $\phi:\mathcal{X}\to\mathcal{X}$ and unitary U acting on $\mathcal{H}_A$ (depending on z, z', and g) such that*

$$\phi(g^{-1}(z))=g^{-1}(z') \tag{101}$$

$$\rho_A^{\phi(x)}=U\rho_A^xU^\dagger. \tag{102}$$

We then have

$$\frac{1}{2}\left\|\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{x\in g^{-1}(z)}\rho_A^x-\rho_A\right\|_1=\frac{1}{2}\left\|\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{x\in g^{-1}(z')}\rho_A^x-\rho_A\right\|_1. \tag{103}$$

In particular,

$$\frac{1}{2}\left\|\rho_{AG^{-1}Z}-\rho_A\otimes\rho_{G^{-1}}^{\mathrm{unif}}\otimes\rho_Z^{\mathrm{unif}}\right\|_1=\frac{1}{2}\left\|\rho_{AG^{-1}}^z-\rho_A\otimes\rho_{G^{-1}}^{\mathrm{unif}}\right\|_1, \tag{104}$$

for all $z\in\mathcal{Z}$ where $\rho_{AG^{-1}Z}=\frac{1}{\mathcal{Z}}\sum_{z\in\mathcal{Z}}\rho_{AG^{-1}}^z\otimes|z\rangle\langle z|$

Proof. Note that

$$\frac{1}{2}\left\|\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{x\in g^{-1}(z)}\rho_A^x-\rho_A\right\|_1=\left\|U\left(\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{x\in g^{-1}(z)}\rho_A^x-\rho_A\right)U^\dagger\right\|_1 \tag{105}$$

$$=\frac{1}{2}\left\|\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{x\in g^{-1}(z)}U\rho_A^xU^\dagger-U\rho_AU^\dagger\right\|_1 \tag{106}$$

$$=\frac{1}{2}\left\|\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{x\in g^{-1}(z)}\rho_A^{\phi(x)}-U\rho_AU^\dagger\right\|_1 \tag{107}$$

$$=\frac{1}{2}\left\|\frac{|\mathcal{Z}|}{|\mathcal{X}|}\sum_{x\in g^{-1}(z')}\rho_A^{x}-U\rho_AU^\dagger\right\|_1. \tag{108}$$

Moreover, we have

$$U\rho_AU^\dagger=U\left(\frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}}\rho_A^x\right)U^\dagger=\frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}}U\rho_A^xU^\dagger \tag{109}$$

$$=\frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}}\rho_A^{\phi(x)} \tag{110}$$

$$=\frac{1}{|\mathcal{X}|}\sum_{x\in\mathcal{X}}\rho_A^{x}=\rho_A. \tag{111}$$

Therefore, we obtain (103). □

When $|\mathcal{V}|$ is a power of a prime, we provide an example from [22] of two-universal hash functions satisfying the conditions of Lemma 3. We assume in this paragraph only that $\mathcal{V}=[\![0,|\mathcal{V}|-1]\!]$ to be consistent with the standard notation for finite fields. Note first that $\mathcal{V}^\ell$ is a field with component-wise addition modulo $|\mathcal{V}|$ and a multiplication operation denoted by $\odot$. We use the short-hand 0^m for the all-zero sequence of length m and $\cdot|\cdot$ for the concatenation of two sequences. For $k\in[\![1,\ell]\!]$ and $u^\ell\in\mathcal{V}^\ell$, let $g_{u^\ell}(v^\ell)$ be the first k elements of $u^\ell\odot v^\ell$. By [22], [34], $\mathcal{G}=\left\{g_{u^\ell}:u^\ell\in\mathcal{V}^\ell\setminus\left\{0^\ell\right\}\right\}$ is a efficiently-invertible two-universal class of hash functions. Moreover, for any $u^\ell\in\mathcal{V}^\ell\setminus\{0\}$, $z^k,z'^k\in\mathcal{V}^k$, we define $\phi(v^\ell)=((z'^k-z^k)|0^{\ell-k})\odot(u^\ell)^{-1}+v^\ell$.

We show that ϕ satisfies (101) and (102). Note that

$$\phi\left(g_{u^\ell}^{-1}(z^k)\right) = \phi\left(\left\{v^\ell : \exists r^{\ell-k} : z^k | r^{\ell-k} = u^\ell \odot v^\ell\right\}\right) \tag{112}$$

$$= \left\{v^\ell + ((z'^k - z^k)|0^{\ell-k}) \odot (u^\ell)^{-1} : \exists r^{\ell-k} : z^k | r^{\ell-k} = u^\ell \odot v^\ell\right\} \tag{113}$$

$$= \left\{v^\ell : \exists r^{\ell-k} : z^k | r^{\ell-k} = u^\ell \odot (v^\ell - ((z'^k - z^k)|0^{\ell-k}) \odot (u^\ell)^{-1})\right\} \tag{114}$$

$$= \left\{v^\ell : \exists r^{\ell-k} : z'^k | r^{\ell-k} = u^\ell \odot v^\ell\right\} \tag{115}$$

$$= g_{u^\ell}^{-1}(z'^k) \tag{116}$$

Furthermore, let $U_{\rm CS}$ be the unitary operation on $\mathcal{H}_Q^{\otimes m}$ corresponding to cyclic shift of length 1, i.e., $|\phi_1\rangle \otimes \cdots \otimes |\phi_m\rangle \mapsto |\phi_m\rangle \otimes |\phi_1\rangle \otimes \cdots |\phi_{m-1}\rangle$. By definition of $d(x,v)$ and $\rho_{Q^n}^{v^\ell}$, we have

$$\rho_{Q^n}^{v^\ell + v'^\ell} = \left(U_{\rm CS}^{v'_1} \otimes \cdots \otimes U_{\rm CS}^{v'_\ell}\right) \rho_{Q^n}^{v^\ell} \left(U_{\rm CS}^{v'_1} \otimes \cdots \otimes U_{\rm CS}^{v'_\ell}\right)^\dagger, \tag{117}$$

where $v^\ell + v'^\ell$ is modulo $|\mathcal{V}|$. We therefore conclude that (102) holds.

APPENDIX D
PROOF OF THEOREM 4

To prove Theorem 4, we need the following tools.

Theorem 5. ([19, Theorem 12.1.1]) *Let A and B be two quantum systems. Let ρ_A^0 and ρ_A^1 be in $\mathcal{D}(\mathcal{H}_A)$ and $\mathcal{N} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_B)$ be a quantum channel. There exists a quantum channel $\mathcal{R} : \mathcal{D}(\mathcal{H}_B) \to \mathcal{D}(\mathcal{H}_A)$ (depending only on $\mathcal{N}$ and ρ_A^0) such that*

$$\mathbb{D}\big(\rho_A^1 \| \rho_A^0\big) - \mathbb{D}\big(\mathcal{N}(\rho_A^1) \| \mathcal{N}(\rho_A^0)\big) \geqslant -\log F(\rho_A^1, (\mathcal{R} \circ \mathcal{N})(\rho_A^1)) \tag{118}$$

and

$$(\mathcal{R} \circ \mathcal{N})(\rho_A^0) = \rho_A^0. \tag{119}$$

Lemma 4. *Let A and B be two quantum systems such that A is a composition of two sub-systems A' and A''. Let ρ_A^0 and ρ_A^1 be in $\mathcal{D}(\mathcal{H}_A)$ such that for two pure states $|\phi^0\rangle_{A'}$ and $|\phi^1\rangle_{A'}$ in $\mathcal{H}_{A'}$ and a mixed state $\nu_{A''}$ in $\mathcal{D}(\mathcal{H}_{A''})$, we have $C(\phi_{A'}^x \otimes \nu_{A''}, \rho_A^x) \leqslant \delta_x$. Let $\mathcal{N} : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_A)$ be a quantum channels such that $F(\rho_A^x, \mathcal{N}(\rho_A^x)) \geqslant 1 - \epsilon_x$. We then have*

$$F(\mathcal{E}(\rho_A^1), \mathcal{E}(\rho_A^0)) \geqslant \aleph(\lambda, F(\phi_{A'}^1, \phi_{A'}^0)) - 2\sqrt{1 - F(\phi_{A'}^1, \phi_{A'}^0)}\delta - \delta^2, \tag{120}$$

where $\delta \triangleq \sum_x \delta_x$, $\lambda = \sum_x \sqrt{\epsilon_x + 4\sqrt{\epsilon_x}\delta_x + 4\delta_x^2}$, $\mathcal{E}$ is a complementary channel to $\mathcal{N}$.

Proof. See Appendix D-A. □

We are now ready to provide the proof of Theorem 4.

Proof. By Theorem 5, there exists a channel $\mathcal{R} : \mathcal{D}(E) \to \mathcal{D}(A)$ such that

$$\mathbb{D}\big(\rho_A^1 \| \rho_A^0\big) - \mathbb{D}\big(\mathcal{E}(\rho_A^1) \| \mathcal{E}(\rho_A^0)\big) \geqslant -\log F(\rho_A^1, (\mathcal{R} \circ \mathcal{E})(\rho_A^1)) \tag{121}$$

$$(\mathcal{R} \circ \mathcal{E})(\rho_A^0) = \rho_A^0. \tag{122}$$

Let $\mathcal{U}_{A\to BE}$ be an isometric extension of $\mathcal{N}$ compatible with $\mathcal{E}$. Let $\mathcal{W}_{E\to AF}$ be an isometric extension of $\mathcal{R}$. The isometry $(\mathbf{1}_B \otimes \mathcal{W}_{E\to AF})\mathcal{U}_{A\to BE}$ is an isometric extension of $\mathcal{R}\circ\mathcal{E}$. Hence, the mapping

$$\rho \mapsto \mathrm{tr}_A \left((\mathbf{1}_B \otimes \mathcal{W}_{E\to AF})\mathcal{U}_{A\to BE}\rho((\mathbf{1}_B \otimes \mathcal{W}_{E\to AF})\mathcal{U}_{A\to BE})^\dagger\right) \tag{123}$$

is a complementary channel of $\mathcal{R} \circ \mathcal{E}$ and

$$\mathrm{tr}_{AF} \left((\mathbf{1}_B \otimes \mathcal{W}_{E\to AF})\mathcal{U}_{A\to BE}\rho((\mathbf{1}_B \otimes \mathcal{W}_{E\to AF})\mathcal{U}_{A\to BE})^\dagger\right) = \mathrm{tr}_E \left(\mathcal{U}_{A\to BE}\rho\mathcal{U}_{A\to BE}\right) = \mathcal{N}(\rho) \tag{124}$$

Therefore, $\mathcal{N}$ is a degraded version of the complementary channel of $\mathcal{R}\circ\mathcal{E}$. Hence, by Lemma 4, we have

$$F(\mathcal{N}(\rho_A^1), \mathcal{N}(\rho_A^0)) \geqslant \aleph(\lambda', F(\phi_{A'}^1, \phi_{A'}^0)) - 2\sqrt{1 - F(\phi_{A'}^1, \phi_{A'}^0)}\delta - \delta^2 \tag{125}$$

where

$$\lambda' \triangleq \sum_x \left(1 - F(\rho_A^x, \mathcal{R}(\mathcal{E}(\rho_A^x))) + 4\sqrt{1 - F(\rho_A^x, \mathcal{R}(\mathcal{E}(\rho_A^x)))}\delta_x + 4\delta_x^2\right)^{\frac{1}{2}} \tag{126}$$

$$= 2\delta_0 + \left(1 - F(\rho_A^1, \mathcal{R}(\mathcal{E}(\rho_A^1)) + 4\sqrt{1 - F(\rho_A^1, \mathcal{R}(\mathcal{E}(\rho_A^1))}\delta_1 + 4\delta_1^2\right)^{\frac{1}{2}}. \tag{127}$$

By our assumption in (57), we have $\aleph(\lambda, F(\phi_A^1, \phi_A^0)) \geqslant \aleph(\lambda', F(\phi_A^1, \phi_A^0))$. Since $\aleph(x, y)$ is decreasing in x for positive x, we have

$$\lambda' \geqslant \lambda, \tag{128}$$

which yields that $1 - \eta \geqslant 1 - F(\rho_A^1, \mathcal{R}(\mathcal{E}(\rho_A^1))$. Substituting this inequality in (121) completes the proof of our claim. □

A. Proof of Lemma 4

We first prove a "triangle" inequality for fidelity measure, which follows from the triangle inequality for $C(\cdot,\cdot)$.

Lemma 5. *Let $\rho,\sigma,\rho',\sigma' \in \mathcal{D}(A)$ and let $\epsilon \triangleq C(\rho,\rho') + C(\sigma,\sigma')$. We then have*

$$F(\rho,\sigma) \geqslant F(\rho',\sigma') - 2\sqrt{1-F(\rho',\sigma')}\epsilon - \epsilon^2. \tag{129}$$

Proof. By the triangle inequality for $C(\cdot,\cdot)$, we have

$$C(\rho,\sigma) \leqslant C(\rho',\sigma') + C(\rho,\rho') + C(\sigma,\sigma') = C(\rho',\sigma') + \epsilon \tag{130}$$

This can be written as

$$\sqrt{1-F(\rho,\sigma)} \leqslant \sqrt{1-F(\rho',\sigma')} + \epsilon. \tag{131}$$

Therefore,

$$1 - F(\rho,\sigma) \leqslant 1 - F(\rho',\sigma') + 2\epsilon\sqrt{1-F(\rho',\sigma')} + \epsilon^2, \tag{132}$$

which yields the desired bound. □

We now prove a result similar to Lemma 4 when ρ_A^0 and ρ_A^1 are pure.

Lemma 6. *Let A and B be finite dimensional quantum systems such that A is a composition of two sub-systems A' and A''. Let $|\phi^0\rangle_{A'}$ and $|\phi^1\rangle_{A'}$ be pure states in $\mathcal{H}_{A'}$ and $\nu_{A''}$ be a mixed state in $\mathcal{D}(\mathcal{H}_{A''})$. Let us define $\rho_A^x \triangleq \phi_{A'}^x \otimes \nu_{A''}$. Let $V : \mathcal{H}_A \to \mathcal{H}_A \otimes \mathcal{H}_B$ be an isometry and define $\psi_{AB}^x \triangleq V\rho_A^x V^\dagger$. Let*

$$\epsilon \triangleq \sum_x C(\psi_A^x, \rho_A^x) \tag{133}$$

We then have

$$F(\psi_B^1, \psi_B^0) \geqslant \aleph(\epsilon, F(\phi_{A'}^1, \phi_{A'}^0)) \tag{134}$$

Proof. Let $|\nu\rangle_{RA''}$ be a purification of $\nu_{A''}$ and define $|\psi^x\rangle_{RAB} \triangleq \mathbf{1}_R \otimes V(|\phi^x\rangle_{A'} \otimes |\nu\rangle_{A''R})$, which is a purification of ψ_{AB}^x. By Uhlmann's theorem, there exist isometries U^0 and U^1 from $\mathcal{H}_R$ to $\mathcal{H}_R \otimes \mathcal{H}_B$ such that

$$C(\psi_A^x, \rho_A^x) = C(\psi_{ABR}^x, \phi_{A'}^x \otimes U^x \nu_{A''R}(U^x)^\dagger) \tag{135}$$

Furthermore, note that

$$F(\phi^1_{A'},\phi^0_{A'}) = F(\phi^1_{A'}\otimes\nu_{A''R},\phi^0_{A'}\otimes\nu_{A''R}) \tag{136}$$

$$\overset{(a)}{=} F(\psi^1_{ABR},\psi^0_{ABR}) \tag{137}$$

$$\overset{(b)}{\leqslant} F(\phi^1_{A'}\otimes U^1\nu_{A''R}(U^1)^\dagger,\phi^0_{A'}\otimes U^0\nu_{A''R}(U^0)^\dagger) + 2\sqrt{1-F(\psi^1_{ABR},\psi^0_{ABR})}\epsilon+\epsilon^2 \tag{138}$$

$$= F(\phi^1_{A'}\otimes U^1\nu_{A''R}(U^1)^\dagger,\phi^0_{A'}\otimes U^0\nu_{A''R}(U^0)^\dagger) + 2\sqrt{1-F(\phi^1_{A},\phi^0_{A})}\epsilon+\epsilon^2 \tag{139}$$

$$= F(\phi^1_{A'},\phi^0_{A'})F(U^1\nu_{A''R}(U^1)^\dagger,U^0\nu_{A''R}(U^0)^\dagger) + 2\sqrt{1-F(\phi^1_{A},\phi^0_{A})}\epsilon+\epsilon^2, \tag{140}$$

where (a) follows since $V_{A\to AB}$ is an isometry, and (b) follows from Lemma 5. Therefore, we have

$$F(U^1\nu_{A''R}(U^1)^\dagger,U^0\nu_{A''R}(U^0)^\dagger) \geqslant 1-\frac{2\sqrt{1-F(\phi^1_A,\phi^0_A)}\epsilon+\epsilon^2}{F(\phi^1_A,\phi^0_A)} \tag{141}$$

Using Lemma 5 again, we obtain

$$F(\psi^1_B,\psi^0_B) \geqslant F(U^1\nu_{A''R}(U^1)^\dagger,U^0\nu_{A''R}(U^0)^\dagger) - 2\sqrt{1-F(U^1\nu_{A''R}(U^1)^\dagger,U^0\nu_{A''R}(U^0)^\dagger)}\epsilon-\epsilon^2 \tag{142}$$

$$\geqslant 1-\frac{2\sqrt{1-F(\phi^1_A,\phi^0_A)}\epsilon+\epsilon^2}{F(\phi^1_A,\phi^0_A)} - 2\sqrt{\frac{2\sqrt{1-F(\phi^1_A,\phi^0_A)}\epsilon+\epsilon^2}{F(\phi^1_A,\phi^0_A)}}\epsilon-\epsilon^2 \tag{143}$$

$$= \aleph(\epsilon,F(\phi^1_A,\phi^0_A)). \tag{144}$$

□

We now prove Lemma 4. Note that for

$$\lambda \triangleq C(\phi^0,\mathcal{N}(\phi^0)) + C(\phi^1,\mathcal{N}(\phi^1)), \tag{145}$$

we have

$$F(\mathcal{E}(\rho^1_A),\mathcal{E}(\rho^0_A)) \overset{(a)}{\geqslant} F(\mathcal{E}(\phi^1_A),\mathcal{E}(\phi^0_A)) - 2\sqrt{1-F(\mathcal{E}(\phi^1_A),\mathcal{E}(\phi^0_A))}\delta-\delta^2 \tag{146}$$

$$\geqslant F(\mathcal{E}(\phi^1_A),\mathcal{E}(\phi^0_A)) - 2\sqrt{1-F(\phi^1_A,\phi^0_A)}\delta-\delta^2 \tag{147}$$

$$\overset{(b)}{\geqslant} \aleph(\lambda,F(\phi^1_A,\phi^0_A)),-2\sqrt{1-F(\phi^1_A,\phi^0_A)}\delta-\delta^2, \tag{148}$$

where (a) follows from Lemma 5, and (b) follows from Lemma 6 Additionally, we have

$$F(\phi^x, \mathcal{N}(\phi^x)) \geqslant F(\rho^x, \mathcal{N}(\rho^x)) - 4\sqrt{1 - F(\rho^x, \mathcal{N}(\rho^x))}\delta_x - 4\delta_x^2 \tag{149}$$

$$\geqslant 1 - \epsilon_x - 4\sqrt{\epsilon_x}\delta_x - 4\delta_x^2, \tag{150}$$

for $x = 0, 1$. This implies that $\lambda \leqslant \sum_x \sqrt{\epsilon_x + 4\sqrt{\epsilon_x}\delta_x + 4\delta_x^2}$.

APPENDIX E
ALGORITHMIC DESCRIPTION OF PPM-MLC-BASED PROTOCOL

Algorithm 1 PPM-MLC based covert QKD protocol

Physical specifications: $\mathcal{E}_{Q\to Q}$, $|0\rangle$, $|\phi\rangle$. See Table II.

Protocol specifications: m, ℓ, $\mathcal{X}$, $\mathcal{V}$, d, ℓ_1, ℓ_1, ϵ^1_{IR}, ϵ^2_{IR}, ϵ^3_{IR}, $\mathrm{leak}_{\mathsf{IR}}$, μ, δ, h. See Table III.

Sub-modules: IR, TG, $\mathcal{F}_t$, $\mathcal{G}$. See Table IV.

Shared key: R uniformly distributed in $[\![1, h]\!]$ and a string of random bits of size $O(\ell_1(\log \ell + \log m))$.

Quantum state distribution

Bob independently and uniformly samples Z and G^{-1} from $[\![1, |\mathcal{V}|^{\ell}/h]\!]$ and $\mathcal{G}^{-1}$, respectively.
Bob transmits Z and G^{-1} over the public channel.
Alice and Bob set $(V_1, \cdots, V_\ell) \leftarrow G(Z, R)$.
for $i = 1$ to ℓ **do**
  Alice uniformly samples X_i from $\mathcal{X}$.
  for $j = 1$ to m **do**
    if $\phi(X_i, V_i) = j$ **then**
      Alice transmits $|\phi\rangle$
    else
      Alice transmits $|0\rangle$.
    end if
    if $j \in \{d(x, V_i) : x \in \mathcal{X}\}$ **then**
      Bob keeps the quantum channel output.
    else
      Bob discards the quantum channel output.
    end if
  end for
end for

REFERENCES

[1] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *arXiv preprint arXiv:1906.01645*, 2019.

Parameter estimation

1: Alice selects $1 \leqslant i_1 < \cdots < i_{\ell_1} \leqslant \ell$ at random.
2: Alice sends $(i_1, \cdots, i_{\ell_1})$ and $(X_{i_1}, \cdots, X_{i_{\ell_1}})$ one-time-padded with a secret key over the public channel.
3: **for** x in $\mathcal{X}$ **do**
4: Alice and Bob set $k \leftarrow \left|\left\{j : X_{i_j} = x\right\}\right|$.
5: Alice transmits $|0\rangle$ over the quantum channel $k\,|\mathcal{X}|$ times (this adds $O(\ell_1)$ to the number of channel uses and does not change covertness or secrecy).
6: Bob applies TG to the received state for $i \in \left\{i_j : X_{i_j} = x\right\}$ and the state received in the previous step to estimate $F(\tau^x_{Q^{|\mathcal{X}|}}, \rho^0_{Q^{|\mathcal{X}|}})$.
7: **end for**
8: Bob sets $\widehat{H}^{\delta}_{\min}(X^{\ell}|E^n)_{\sigma}$ as the RHS of Eq. (20).
9: Bob sends $\left\lfloor \widehat{H}^{\delta}_{\min}(X^{\ell}|E^n)_{\sigma} \right\rfloor$ one-time padded with a shared key over the public channel.
10: Alice and Bob discard all information concerning PPM symbols $(i_1, \cdots, i_{\ell_1})$.

Information reconciliation

1: Alice and Bob perform IR so that Bob decodes X^{ℓ_2} as $\widehat{X}^{\ell_2}$.

Privacy amplification

1: Alice and Bob set $t \leftarrow \left\lfloor \widehat{H}^{\delta}_{\min}(X^{\ell}|E^n)_{\sigma} \right\rfloor - \mathsf{leak}_{\mathsf{IR}} - 2\log(1/\delta)$.
2: Alice samples F from $\mathcal{F}_t$ and sends F over the public channel.
3: Alice sets $S_A \leftarrow F(X^{\ell_2})$.
4: Bob sets $S_B \leftarrow F(\widehat{X}^{\ell_2})$.

TABLE II

PHYSICAL SPECIFICATION

$\mathcal{E}_{Q\to Q}$	the probe
$\mathcal{N}_{Q\to Q}$	the honest channel
$\|0\rangle$	the idle state
$\|\phi\rangle$	a non-idle state

TABLE III

PROTOCOL SPECIFICATION

m	length of PPM symbols
ℓ	number of PPM symbols
$\mathcal{X}$,$\mathcal{V}$	two sets with $\lvert\mathcal{X}\rvert \lvert\mathcal{V}\rvert = m$
d	one-to-one function from $\mathcal{X} \times \mathcal{V}$ to $[\![1, m]\!]$
ℓ_1, ℓ_2	two integers with $\ell = \ell_1 + \ell_2$
ϵ_{IR}^1, ϵ_{IR}^2, ϵ_{IR}^3, $\mathrm{leak}_{\mathsf{IR}}$	information reconciliation specifications (See Table V)
δ	positive real number controlling secrecy
μ	positive real number such that $\mu > \sqrt{\frac{\ell}{m}\chi_2(\mathcal{E}(\lvert\phi\rangle\langle\phi\rvert)\|\mathcal{E}(\lvert 0\rangle\langle 0\rvert))} + \epsilon_{\mathsf{IR}}^3$ controlling covertness
h	integer specifying the size of the shared key

TABLE IV

SUB-MODULES

IR	information reconciliation protocol with parameters ϵ_{IR}^1, ϵ_{IR}^2, ϵ_{IR}^3, $\mathrm{leak}_{\mathsf{IR}}$ (See Table V)
TG	quantum tomography protocol (See Table VI)
$\mathcal{F}_t$	efficient family of two-universal hash functions from $\mathcal{X}^{\ell_2}$ to $\{0,1\}^t$ for all $t \in [\![0, \lvert\mathcal{X}\rvert^{\ell_2}]\!]$
$\mathcal{G}$	efficiently invertible two-universal family of hash functions $\mathcal{G}$ from $\mathcal{V}^\ell$ to $[\![1, \lvert\mathcal{V}\rvert^\ell / h]\!]$

TABLE V

TWO-PARTY INFORMATION RECONCILIATION USING PUBLIC COMMUNICATION

Alice's input	X^{ℓ_2}
Bob's input	quantum state $\sigma_{Q^{\ell_2\lvert\mathcal{X}\rvert}}$
Public communication	C_{IR} belonging to $\mathcal{C}_{\mathsf{IR}}$
Bob's output	$\widehat{X}^{\ell_2}$
Information leakage	$\mathrm{leak}_{\mathsf{IR}} \triangleq \log \lvert\mathcal{C}_{\mathsf{IR}}\rvert - \inf_{x^{\ell_2}} H_{\min}(P_{C_{\mathsf{IR}}\lvert X^{\ell_2}=x^{\ell^2}})$
Reliability	$\epsilon_{\mathsf{IR}}^1 \leqslant \mathbb{P}\Big(X^{\ell_2} \neq \widehat{X}^{\ell_2}\Big)$ for all possible inputs
Robustness	$\mathbb{P}(\text{abort}) \leqslant \epsilon_{\mathsf{IR}}^2$ when the channel is honest
Covertness	$\frac{1}{2}\big\lVert\sigma_{C_{\mathsf{IR}}E^n} - \rho_{C_{\mathsf{IR}}}^{\mathrm{unif}} \otimes \sigma_{E^n}\big\rVert_1 \leqslant \epsilon_{\mathsf{IR}}^3$ for any Eve's attack

TABLE VI

ONE-PARTY QUANTUM TOMOGRAPHY PROTOCOL

Input	k, $\rho^{\otimes k}$, $\sigma^{\otimes k}$
Output	estimate of $F(\rho, \sigma)$

[2] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," *Quantum Information*, vol. 2, no. 1, nov 2016.

[3] H. Bennett Ch and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Prof. of Conf. on Computers, Systems and Signal Processing*, Bangalore, India, Dec. 1984, pp. 175–9.

[4] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, pp. 661–663, Aug. 1991.

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

[6] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, "Device-independent security of quantum cryptography against collective attacks," *Phys. Rev. Lett.*, vol. 98, p. 230501, Jun. 2007.

[7] B. Bash, D. Goeckel, and D. Towsley, "Limits of reliable communication with low probability of detection on AWGN channels," *IEEE Journal of Selected Areas in Communications*, vol. 31, no. 9, pp. 1921–1930, Sep. 2013.

[8] L. Wang, G. W. Wornell, and L. Zheng, "Fundamental limits of communication with low probability of detection," *IEEE Transactions on Information Theory*, vol. 62, no. 6, pp. 3493–3503, Jun. 2016.

[9] M. R. Bloch, "Covert communication over noisy channels: A resolvability perspective," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2334–2354, May 2016.

[10] A. Sheikholeslami, B. A. Bash, D. Towsley, D. Goeckel, and S. Guha, "Covert communication over classical-quantum channels," in *Proc. of IEEE International Symposium on Information Theory*, Barcelona, Spain, Jul. 2016, pp. 2064–2068.

[11] L. Wang, "Optimal throughput for covert communication over a classical-quantum channel," in *Proc. of IEEE Information Theory Workshop*, Cambridge, UK, Sep. 2016, pp. 364–368.

[12] J. M. Arrazola and V. Scarani, "Covert quantum communication," *Physical Review Letters*, vol. 117, p. 250503, Dec 2016.

[13] 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," *Nature Communications*, vol. 6, pp. –, Oct. 2015.

[14] 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.

[15] S. Watanabe and M. Hayashi, "Non-asymptotic analysis of privacy amplification via rényi entropy and inf-spectral entropy," in *Proc. of IEEE International Symposium on Information Theory*, Istanbul, Turkey, Jul. 2013, pp. 2715–2719.

[16] I. A. Kadampot, M. Tahmasbi, and M. R. Bloch, "Multilevel-coded pulse position modulation for covert communications," in *Proc. of IEEE International Symposium on Information Theory*, Vail, CO, Jun. 2018, pp. 1864–1868.

[17] J. M. Arrazola and R. Amiri, "Secret-key expansion from covert communication," *Phys. Rev. A*, vol. 97, p. 022325, Feb 2018.

[18] M. Tomamichel, *Quantum information processing with finite resources: mathematical foundations*, ser. Springer briefs in mathematical physics. Springer, 2016.

[19] M. M. Wilde, *Quantum information theory*. Cambridge University Press, 2013.

[20] M. R. Bloch and S. Guha, "Optimal covert communications using pulse-position modulation," in *Proc. of IEEE International Symposium on Information Theory*, Aachen, Germany, Jun. 2017, pp. 2825–2829.

[21] M. Hayashi, *Quantum information*. Springer, 2006.

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

[23] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep. 2009.

[24] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks," *Phys. Rev. Lett.*, vol. 109, p. 100502, Sep. 2012.

[25] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, "Security of continuous-variable quantum key distribution against general attacks," *Phys. Rev. Lett.*, vol. 110, p. 030502, Jan. 2013.

[26] R. Renner and J. I. Cirac, "de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Phys. Rev. Lett.*, vol. 102, p. 110504, Mar. 2009.

[27] M. R. Bloch and S. Guha, "Optimal covert communications using pulse-position modulation," in *Proc. of IEEE International Symposium on Information Theory*, Aachen, Germany, Jun. 2017, pp. 2835–2839.

[28] J. Martinez-Mateo, D. Elkouss, and V. Martin, "Key Reconciliation for High Performance Quantum Key Distribution," *Scientific Reports*, vol. 3, p. 1576, Apr. 2013.

[29] R. A. Chou and M. R. Bloch, "Polar coding for the broadcast channel with confidential messages: A random binning analogy," *IEEE Transactions on Information Theory*, vol. 62, no. 5, pp. 2410–2429, May 2016.

[30] M. Tahmasbi and M. R. Bloch, "A framework for covert and secret key expansion over quantum channels," *arXiv preprint arXiv:1811.05626*, 2018.

[31] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, "Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates," *Physical Review A*, vol. 94, no. 1, p. 012322, Jul. 2016.

[32] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, July 1993.

[33] I. Sason and S. Verdú, "f -divergence inequalities," *IEEE Transactions on Information Theory*, vol. 62, no. 11, p. 5973–6006, Nov. 2016.

[34] M. Hayashi, "Exponential decreasing rate of leaked information in universal random privacy amplification," *IEEE Transactions on Information Theory*, vol. 57, no. 6, p. 3989–4001, Jun. 2011.