Continuous-variable quantum key distribution with discretized modulations in the strong noise regime

Mikhail Erementchouk* and Pinaki Mazumder†
Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, Michigan 48109, USA

(Received 17 September 2019; revised manuscript received 2 February 2020; accepted 11 May 2020; published 5 June 2020)

We consider a general family of quantum key distribution (QKD) protocols utilizing displaced thermal states with discretized modulations. Separating the effects of the Gaussian channel and the non-Gaussian distribution, we study the dependence of the secret key generation rate on the magnitude of modulations (the strength of the modulated signal). We show that in the limit of a strong signal, QKD is impossible. In this case, from the perspective of an efficient eavesdropper, the ensemble of transmitted states is effectively classical and the amount of leaked information is limited only by the entropy of the distribution of transmitted states, while the mutual information between the legitimate parties is also subject to such limiting factors as detection and reconciliation efficiencies. We demonstrate that two regimes must be distinguished: weak and strong thermal noise. In the case of strong noise, the security boundary is mostly determined by the weak-signal limit, for which we obtain an explicit form of the condition where the secret key can be generated in the asymptotic limit. When the noise is weak, however, QKD may become possible only when the signal strength exceeds some critical value.

DOI: 10.1103/PhysRevA.101.062313

I. INTRODUCTION

The inherent asymmetry of three-way quantum communications is one of the drastic differences between classical and quantum communications. A quantum state sent by one party cannot be freely shared between the remaining two. This circumstance is formalized by the famous no-cloning theorem: an unknown quantum state cannot be cloned [1,2]. Indeed, if such a cloner existed, it would have to commute with all operators acting on the cloned state, and hence, its action would be independent of the cloned state. This demonstrates that the no-cloning property has fundamental roots similar to those of the Heisenberg uncertainty relation. Consequently, gaining information about an unknown state necessarily perturbs the state, as in the noise-disturbance uncertainty relation [3]. Thus, roughly, sharing an unknown quantum state between two parties is a "zero-sum game": one party can gain information about the state only at the expense of another party.

This feature of quantum communications constitutes a foundation for the quantum key distribution (QKD) [4–8], aiming at the production by two parties of probabilistically noninterceptable shared keys over authenticated channels. As hinted at by the proof of the no-cloning theorem above, in order to avoid direct cloning, states associated with noncommuting operators must be employed. QKD protocols leverage this property by sending nonorthogonal noncoinciding states. Subsequently, a shared key is recovered from apparently a random preparation and observation data. Since, at this stage, the data held by communicating parties are classical, they fall under the classical Shannon's information framework, and hence, the shared key can be recovered using an adaptation of an error-correcting algorithm.

Initially, QKD was developed for discrete variables, such as electron spin and photon polarization, but later the class of physical systems enabling QKD was extended by incorporating continuous variables (CV-QKD), for instance, quadratures of the electromagnetic field. Moreover, it was shown in Ref. [9] that displaced thermal states can be used for generating the secret key, thus dissociating QKD from the sole nature of utilized states. Since displaced states can be regarded as a result of quasiclassical driving of a cavity at thermal equilibrium, this significantly relaxes the requirements for state sources.

Bringing QKD to the realm of conventional sources boosted the development of practical QKD infrastructures, which potentially may significantly impact the field of secure communications. The main success in realizing CV-QKD is achieved in the optical and near-infrared spectral domains, owing to the ready availability of highly coherent sources of the electromagnetic field and the low magnitude of thermal noise at room temperature [8].

To propagate QKD technologies farther down the electromagnetic spectrum one has to deal with several obstacles. The main challenge appears to stem from thermal noise. With a decreasing base frequency, ω, the noise magnitude increases rapidly, $\sim \exp(\omega_T/\omega)$ with $\omega_T = k_B T/\hbar$, once $\omega < \omega_T$. Here, $\hbar$ is the Planck constant, k_B is the Boltzmann constant, and T is the channel temperature. In Refs. [10] and [11], however, it was shown that strong thermal noise does not prohibit QKD but, rather, determines the family of protocols (in this case, it is the direct reconciliation since it is more resistant to noise).

*merement@gmail.com
†pinakimazum@gmail.com

Thus, further studies of QKD in the far-infrared and below spectral regions are warranted, motivated, on the one hand, by fundamental questions of the quantum-classical interface and the physical origin of information [12] and, on the other hand, by the demand to have matching technologies for emerging small-size high-bandwidth wireless networks.

In the present paper, we address a question that naturally arises in the context of low-frequency implementations of QKD. The main results concerning the frequency dependence of QKD were obtained within the framework of Gaussian states, that is, when the Wigner function of quantum states is a Gaussian function of field quadratures. Overall, this assumption is not too restrictive since the Gaussian property is preserved in dynamics governed by the Hamiltonian's quadratic in the field creation and annihilation operators. Such dynamics envelop a wide range of physical situations including linear and squeezing systems. However, for a train of transmitted states to submit to the formalism of Gaussian states, the variations of the transmitted states must follow a Gaussian distribution, in which case they essentially mimic thermal noise. In practical implementations, however, various deviations from a Gaussian distribution are unavoidable, which calls into question the applicability of the results obtained within the framework of Gaussian states.

We consider the situation where the actual distribution of displacements of displaced thermal states is discretized [13], which clearly demonstrates deviations from the Gaussian framework. It should be noted that QKD protocols with discretized modulations of the displacement parameter had previously attracted researchers' attention [14–23]. The main focus, however, was on protocols based on coherent states encoding finite alphabets. This imposes strict requirements on the quantum state source, which may be challenging to meet at lower frequencies. In the present work, we consider discretized modulations with an unrestricted distribution function and without assuming synchronized phases between the source and the receiver. To describe the effect of thermal noise, we revisit the standard theory of CV-QKD for Gaussian states in such a way that distinguishes effects inherent to Gaussian channels and those caused by the specific form of the distribution of the displacements. To this end, we have to abandon the convenient formalism of covariance matrices and to keep the explicit operator form of relevant density matrices.

The strongest manifestations of the departure of discretized distributions from Gaussian is a nonmonotonous dependence of the key generation rate on the intensity of the transmitted state. Moreover, the rate vanishes in the limit of strong excitations, making QKD impossible. Physically, this can be understood as follows. Different states obtained by sufficiently strong displacement of thermal states are essentially orthogonal to each other and, thus, can be associated with (practically) commuting operators in the proof of the no-cloning theorem above. As a result, large values of the quantization parameter destroy the no-cloning character of the transmitted quantum states, stripping the QKD of its fundamental background. This suggests that, in the QKD context, the transition to the classical regime emerges as an *ensemble property* rather than one of individual states.

II. CV-QKD NETWORK WITH DISCRETIZED MODULATIONS

QKD protocols and networks have been reviewed in a number of publications [4–8,24]. Therefore, we limit ourselves to setting up the problem of networks with discretized modulations and defining the main notation without going into detail.

A. Key generation rate

In one-way QKD networks, the key is recovered from two strings of data held by the sender, A, and the receiver, B. On the A side, the string $\Sigma_A = \{\zeta_1, \ldots\}$ comprises the values of the control parameters, while on the B side, $\Sigma_B = \{\kappa_1, \ldots\}$ is populated by the results of observations. Assuming that there are no quantum correlations *within* Σ_A and Σ_B, these strings can be regarded as classical, resulting from a communication with abundant information over a noisy channel. According to Shannon's theory, the length of a perfectly correlated substring recoverable from Σ_A and Σ_B in the asymptotic limit is proportional to mutual information,

$$I(A:B) = \int d\zeta d\kappa\, \Pi(\zeta,\kappa) \ln\left[\frac{\Pi(\zeta,\kappa)}{\Pi_0(\zeta)\Pi(\kappa)}\right], \qquad (1)$$

where $\Pi(\zeta,\kappa)$ is the joint distribution function of the controlling parameters and the results of observations, and $\Pi_0(\zeta)$ and $\Pi(\kappa)$ are the respective marginal distributions. The base of the logarithm in Eq. (1) determines the units for measuring information. We adopt natural units (nat), which slightly simplifies the derived formulas.

In one-way protocols, the distribution of outcomes of the receiver's measurements deterministically depends on the transmitted state, so that the joint distribution has the form

$$\Pi(\zeta,\kappa) = \Pi_{\mathcal{K}}(\kappa|\zeta)\Pi_0(\zeta), \qquad (2)$$

where $\Pi_{\mathcal{K}}(\kappa|\zeta)$ is the conditional probability of obtaining κ while observing $\mathcal{K}$ for a system in a state obtained with the controlling parameters set to ζ. In physical terms, the conditional probability can be presented as $\Pi_{\mathcal{K}}(\kappa|\zeta) = \mathrm{Tr}[\mathcal{E}_{\mathcal{K}}(\kappa)\rho(\zeta)]$, where $\mathcal{E}_{\mathcal{K}}(\kappa)$ is the respective spectral projector, and $\rho(\zeta)$ is the density matrix of the full channel-environment state at the final stage of a QKD transaction starting from a state prepared with ζ. Since only the reduced density matrix on the receiving side is relevant, we have $\Pi_{\mathcal{K}}(\kappa|\zeta) = \mathrm{Tr}[\mathcal{E}_{\mathcal{K}}(\kappa)\rho_B(\zeta)]$, where

$$\rho_B(\zeta) = \mathrm{Tr}_E[\rho(\zeta)], \qquad (3)$$

with traced-out environmental degrees of freedom.

Using Eq. (2) in Eq. (1), we obtain

$$I(A:B) = S(\overline{\Pi_{\mathcal{K}}(\kappa|\zeta)}) - \overline{S(\Pi_{\mathcal{K}}(\kappa|\zeta))}, \qquad (4)$$

where $S[f(\kappa)] = -\int d\kappa f(\kappa)\ln[f(\kappa)]$ is Shannon's entropy of distribution $f(x)$. An overline, as in Eq. (4), denotes averaging with respect to the controlling parameter $\overline{F(\zeta)} = \int d\zeta F(\zeta)\Pi_0(\zeta)$. For such averaging, we also use the standard expectation symbol: $\mathbb{E}F(\zeta) = \overline{F(\zeta)}$.

Applying an error correction kind of algorithm to Σ_A and Σ_B, the communicating parties can "recover the original message" or, more formally, construct a common shared string

Σ_K. When there is no noise of uncontrolled origin (untrusted noise), Σ_K will constitute a secret key. Thus, in this case, the rate of generation of the secret key is simply $R = I(A : B)$. In the presence of untrusted noise, however, the actual key must be constructed assuming that this noise is due to eavesdropping. In this case, the key rate must be adjusted to account for information intercepted by the eavesdropper, which yields

$$R = I(A : B) - \chi_E. \tag{5}$$

Here, χ_E quantifies the amount of information accessible to the third party for a given magnitude of untrusted noise. Since Σ_K is *reconstructed* from Σ_A and Σ_B rather than transmitted, say, from A to B, either A or B can be regarded as the holder of the "original message" and, respectively, either A or B can initiate error correction. These scenarios are called *direct* and *reverse reconciliation*, respectively [25,26]. In the present paper, we limit ourselves to the case of direct reconciliation, as it demonstrates stronger resilience to thermal noise. In this case, the maximum information is limited from above by the mutual quantum information between A and E (Holevo bound), $\chi_E = \chi(A : E)$ with

$$\chi(A : E) = H(\overline{\rho_E(\zeta)}) - \overline{H(\rho_E(\zeta))}, \tag{6}$$

where $H(\rho) = -\mathrm{Tr}[\rho \ln(\rho)]$ is the von Neumann entropy of the density matrix ρ and $\rho_E(\zeta) = \mathrm{Tr}_B[\rho(\zeta)]$ is the density matrix of the environment obtained by tracing out the receiver degree of freedom.

It must be noted that the fraction of recoverable message in a noisy string reaches Shannon's limit, $I(A : B)$, only asymptotically, when the length of the transmitted messages, N, is infinite, and the error correction algorithm is perfect. For finite N and realistic algorithms, one needs to take into account that the recoverable message is shorter than prescribed by Shannon's limit. In the analysis of QKD protocols, this circumstance is accounted for by introducing the reconciliation efficiency λ, which renormalizes the mutual information, so that the actual secret key generation rate is given instead by $R = \lambda I(A : B) - \chi_E$. In turn, the reconciliation efficiency is regarded as being determined by classical parameters and postprocessing (see, e.g., [27–29]). We show below that there are corrections of essentially quantum origin that modify the key generation rate, so that the finite-N effect cannot be accounted for by the reconciliation efficiency alone. Because of this circumstance, we presume that the main limitations arise due to the discrete character of the displacement parameter and take $\lambda = 1$.

B. Transmitted states

In the present paper, we limit ourselves to the single-mode approximation, which assumes that only one mode contributes to QKD transactions. First, we describe a general model of transmitted displaced single-mode states and establish general relations between these states and the mutual information that they can carry.

Displaced states are a particular case of Perelomov's coherent states [30]. Let the sender's source cavity subjected to a semiclassical excitation be initially in the thermal state

$$\widetilde{\rho}(0;\widetilde{n}) = \frac{e^{-\beta a_0^\dagger a_0}}{1+\widetilde{n}}, \tag{7}$$

where $\beta = \ln(1+\widetilde{n}^{-1})$, $\widetilde{n}$ is the average population of the cavity mode, and $a_0^\dagger$ and a_0 are the cavity mode creating and annihilating operators, respectively. The dynamics of the driven cavity is described by $\mathcal{H}_{\mathrm{int}} = a_0^\dagger E + a_0 E^*$, where E is the complex amplitude of the external classical field. The evolution operator describing the action of the semiclassical excitation is Glauber's displacement operator $\mathcal{D}_A$, and thus, we assume that the states leaving the cavity have the form

$$\widetilde{\rho}_A(\widetilde{\zeta};\widetilde{n}) = \mathcal{D}_A(\widetilde{\zeta})\widetilde{\rho}_A(0;\widetilde{n})\mathcal{D}_A^\dagger(\widetilde{\zeta}), \tag{8}$$

with

$$\mathcal{D}_A(\widetilde{\zeta}) = \exp(a_0^\dagger\widetilde{\zeta} - a_0\widetilde{\zeta}^*). \tag{9}$$

Here, $\widetilde{\zeta}$ depends on the magnitude and duration of the classical driving field. Its relation with the displacement of transmitted states is described below in the model of discretized modulations.

The linear coupling between the channel mode and the environment is described by the Hamiltonian $\mathcal{H}_e = f(t)(a_e^\dagger a_0 + a_0^\dagger a_e)$, where a_e and $a_e^\dagger$ are the operators corresponding to the external field. Let the initial states of the channel and the external field be $\widetilde{\rho}_c$ and ρ_e, respectively. Then the result of such coupling is given by $\rho = \mathcal{S}\widetilde{\rho}_c \otimes \rho_e \mathcal{S}^\dagger$, where $\mathcal{S}$ is the evolution operator describing the action of $\mathcal{H}_e$. It is convenient to consider the external and the channel modes on an equal footing and to introduce vector notations $\mathbf{a}^\dagger \cdot \mathbf{v} \equiv v_0 a_0^\dagger + v_e a_e^\dagger$ with complex v_0 and v_e. Then the action of $\mathcal{S}$ can be represented as

$$\mathcal{S} f(\mathbf{a}^\dagger \cdot \mathbf{v})\mathcal{S}^\dagger = f[\mathbf{a}^\dagger \cdot (\widehat{S}\mathbf{v})], \tag{10}$$

where $\widehat{S}$ is the scattering matrix relating the initial and final operators

$$\begin{pmatrix} a_0(\mathrm{out}) \\ a_e(\mathrm{out}) \end{pmatrix} = \widehat{S}\begin{pmatrix} a_0(\mathrm{in}) \\ a_e(\mathrm{in}) \end{pmatrix}, \tag{11}$$

with

$$\widehat{S} = \begin{pmatrix} t & r^* \\ -r & t^* \end{pmatrix}. \tag{12}$$

Thus, the linear coupling can be represented as mixing the external and channel modes on a beam splitter characterized by complex reflection and transmission coefficients, r and t, constrained by the unitarity condition $|t|^2 + |r|^2 = 1$.

Measurements of the channel field after such an interaction are described by the effective channel density matrix obtained by tracing the external degrees of freedom $\rho_c = \mathrm{Tr}_e[\rho]$. If the channel is initially in the displaced thermal state $\widetilde{\rho}_c = \mathcal{D}(\widetilde{\zeta})\widetilde{\rho}_A(0;\widetilde{n})\mathcal{D}^\dagger(\widetilde{\zeta})$, then ρ_c is also a displaced thermal state,

$$\rho_c = \mathcal{D}(\zeta)\rho_A(0)\mathcal{D}^\dagger(\zeta), \tag{13}$$

where $\zeta = \mathbf{e}_0^\dagger \cdot (\widehat{S}\boldsymbol{\zeta})$ with $\mathbf{e}_0^\dagger = (1, 0)$ and $\boldsymbol{\zeta} = (\widetilde{\zeta}, 0)^T$, so that $\zeta = t\widetilde{\zeta}$, and

$$\rho_A(0) = \mathrm{Tr}_e[\mathcal{S}\widetilde{\rho}_A(0) \otimes \rho_e \mathcal{S}^\dagger]. \tag{14}$$

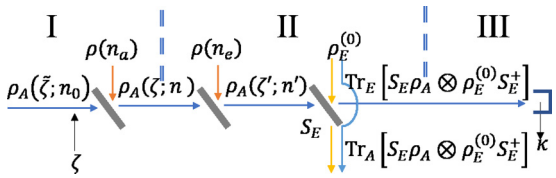

FIG. 1. Propagation of a quantum state in a QKD transaction. Stage I: preparation of the quantum state. Stage II: effect of the environment and model of information losses. Stage III: detection.

Let the ambient electromagnetic field be in a thermal state characterized by the average population n_a. The beam splitter turns the incoming state into the channel state (see Stage I in Fig. 1)

$$\rho_A(\zeta;n)=\mathrm{Tr}_a[\mathcal{S}(r,t)\rho_A(\widetilde{\zeta};n_0)\otimes\rho_{th}(n_a)\mathcal{S}^\dagger(r,t)], \tag{15}$$

where $\mathcal{S}(r,t)$ is an operator describing the transformation induced by the beam splitter.

Using the P representation for the density matrices, we can rewrite this equation as

$$\rho_A(\zeta;n)=\frac{1}{\pi^2 n_0 n_a}\int d^2z_0 d^2z_a e^{-|z_0|^2/n_0-|z_a|^2/n_a} \times \mathrm{Tr}_a[\mathcal{S}\mathcal{D}(\mathbf{v})|0\rangle\langle 0|\mathcal{D}^\dagger(\mathbf{v})\mathcal{S}^\dagger], \tag{16}$$

where $\mathcal{D}(\mathbf{v})=\exp(\mathbf{v}\cdot\mathbf{a}^\dagger-\mathbf{v}^*\cdot\mathbf{a})$ and $\mathbf{v}\cdot\mathbf{a}^\dagger=v_0a_0^\dagger+v_aa_a^\dagger$ with $v_0=z_0+\zeta$ and $v_a=z_a$. Taking into account that $\mathcal{S}\mathcal{D}(\mathbf{v})|0\rangle=\mathcal{D}(\mathbf{u})|0\rangle$ with $\mathbf{u}=\widehat{S}\mathbf{v}$, we obtain

$$\rho_A(\zeta;n)=\frac{1}{\pi^2 n_0 n_a}\int d^2z_0 d^2z_a e^{-|z_0|^2/n_0-|z_a|^2/n_a} \times \mathcal{D}(u_0)|0\rangle\langle 0|\mathcal{D}^\dagger(u_0). \tag{17}$$

By changing the integration variables, Eq. (17) can be turned into the canonical form, yielding

$$\zeta=t\widetilde{\zeta},\quad n=|t|^2n_0+|r|^2n_a. \tag{18}$$

Thus, the modulation of the transmitted state for a given outcome of the source of displaced thermal states can be achieved by varying the complex transmission coefficient of the beam splitter. The modulation of postsource states is commonly used in experimental implementations of QKD.

If controls determining the value of t admit a finite number of states, t takes values at a finite number of points inside the unit circle on the complex plane. Multiplication by $\widetilde{\zeta}$ maps these points into the complex ζ plane, resulting in discretized modulations. In the present paper, we consider the effect of the magnitude of $\widetilde{\zeta}$ or, more physically, of the strength of the quasiclassical excitation, on the key generation rate. To this end, we represent the modulation value as $s\zeta$, where s is a scaling parameter. Figure 2 shows an example where the discretized nature of the distribution becomes apparent with increasing value of the scaling parameter. The figure shows the case where the points are arranged on a lattice, which makes the notion of a characteristic separation Δ_ζ apparent. This scale plays an important role in determining the security boundary as discussed in Sec. IV A below.

Some results obtained below can be formulated for a general observable $\mathcal{K}$ measured at the receiving end. Such a generalization may be of interest in the context of low-frequency spectral domains, where a wide variety of methods to control the electromagnetic field is available. In the present paper, however, we limit ourselves to the case where quadratures are measured. In this case, the conditional probability of obtaining value κ is given by

$$\Pi_{\mathcal{K}}(\kappa|\zeta)=Q(\kappa|\zeta)\equiv\frac{1}{\sqrt{2\pi\sigma^2}}\exp\left\{-\frac{1}{\sigma^2}[\kappa-\langle\kappa_\zeta\rangle]^2\right\}, \tag{19}$$

where $\sigma^2=2n+1$ and

$$\langle\kappa_\zeta\rangle=\sqrt{2}\,\mathrm{Re}(t\zeta e^{i\theta}). \tag{20}$$

The family of quadratures is parameterized by the phase parameter θ and the argument of the channel transmission coefficient. A variety of protocols is based on the precise control

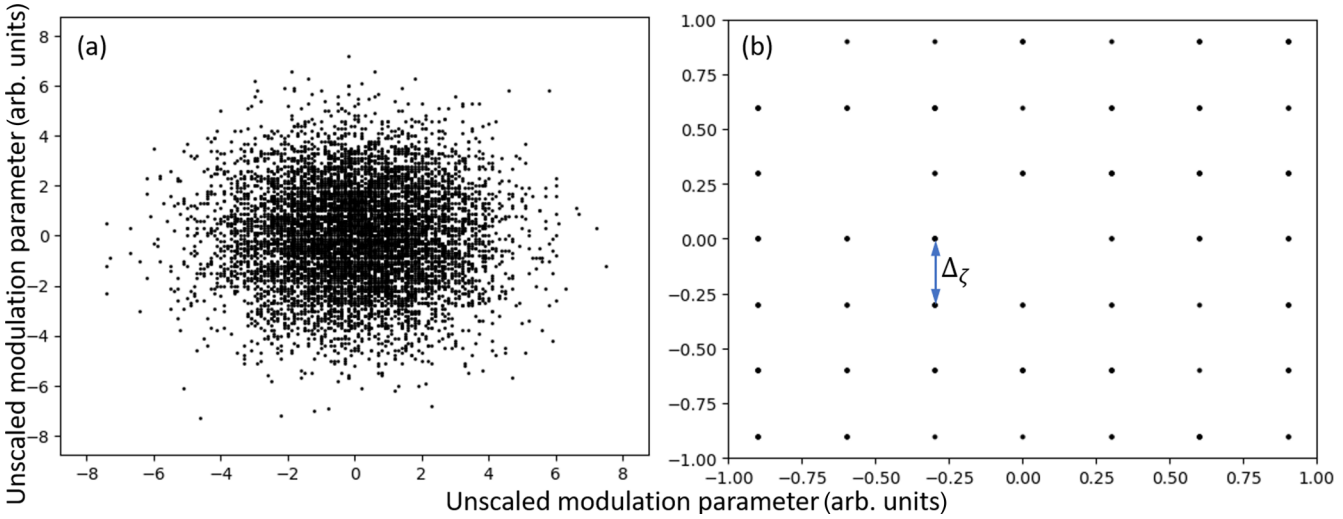

FIG. 2. (a) The unscaled (say, $s=s_0=1$) distribution may appear as a sample of the Gaussian distribution. (b) With increasing scale (the case corresponding to $s=8s_0$ is shown), the distribution reveals that it has an inherently discretized structure with the characteristic separation Δ_ζ (see analysis in Sec. IV A).

over the quadrature phase provided by synchronizing the local oscillator in the homodyne detection of the quadrature. Here, we do not put any restrictions on the phase, thus allowing for an unsynchronized local oscillator.

C. Physical model of the information loss

We model the information loss into the environment using the model of Gaussian collective attacks. These attacks are proven to be optimal for Gaussian protocols and are conjectured to be optimal in general [31–33]. Within this model, eavesdropping masks itself as thermal noise, so that the external coupled state purifies the thermal state. More specifically, the external field is initially prepared in a two-mode squeezed vacuum state,

$$\rho_E^{(0)} = \mathcal{F}(\mu)|0\rangle\langle 0|\mathcal{F}^\dagger(\mu), \tag{21}$$

where $\mathcal{F}(\mu)$ is the two-mode squeezing operator. Denoting the operators of the environment modes a_2 and a_3, we have

$$\mathcal{F}(\mu) = \exp[\mu(a_2^\dagger a_3^\dagger - a_2 a_3)]. \tag{22}$$

Generally, the squeezing parameter can be complex. Its argument, however, can be absorbed into $a_{2,3}$ without changing the final results. Therefore, Eq. (22) presumes that the squeezing parameter is a real number, which simplifies intermediate formulas.

One of the squeezed modes is mixed with the channel mode on a beam splitter, while the second mode is collected together with the mode transmitted through the beam splitter (see Stage II in Fig. 1), which constitutes $\rho_E(\zeta)$ in Eq. (6). The strength of the channel-environment coupling is quantified by the reflection coefficient of the beam splitter, r_E, which also can be assumed real without loss of generality.

III. UNTRUSTED NOISE AND INFORMATION LEAKED INTO THE ENVIRONMENT

One of the main objectives of a theory of QKD is to establish the amount of leaked information for a given (measured during the communication session) amount of untrusted noise. Based on this knowledge, the communicating parties decide whether the secret key can be extracted (if mutual information exceeds losses) or the results of the communication session must be abandoned.

A. Emergence of untrusted noise

Coupling channel modes with the environment in a purified thermal state affects the channel mode in the same way as coupling with a thermal state. Indeed, when evaluating the partial trace over the eavesdropper's modes in Eq. (3), one needs to take into account that the displacement direction of the channel state is orthogonal to the plane of squeezing. Thus, tracing out the mode, which is not mixed with the state in the channel, yields

$$\rho_B(\zeta) = \sum_{m_2}\langle m_2|\mathcal{S}(\theta)\rho_A(\zeta;n)\otimes\widetilde{\rho}_{\rm th}\mathcal{S}^\dagger(\theta)|m_2\rangle, \tag{23}$$

where $\widetilde{\rho}_{\rm th}$ is an effective thermal state,

$$\widetilde{\rho}_{\rm th} = \frac{1}{\cosh^2(\mu)}\sum_{m_3}\tanh^{2m_3}(\mu)|m_3\rangle\langle m_3|. \tag{24}$$

Thus, from the channel perspective, efficient eavesdropping is indistinguishable from coupling with a thermal state $\rho_{\rm th}(\sinh^2(\mu))$. If all environment states are of uncontrolled origin, then on the receiving side we have $\rho_B(\zeta) = \rho_{\rm th}(t_E\zeta, nt_E^2 + n_E)$, where

$$n_E = r_E^2\sinh^2(\mu) \tag{25}$$

is the magnitude of untrusted noise and we have taken into account that the parameters describing the strength of coupling with the environment, t_E and r_E, can be chosen real.

Importantly, this implies the reverse: any untrusted noise must be regarded as stemming from the information loss to an efficient eavesdropper.

B. Information loss

When A announces its data, the amount of leaked information is limited by the Holevo bound $\chi(A:E)$. Since we do not assume the Gaussian form of $\Pi_0(\zeta)$, it is convenient to rewrite the environment density matrix in a form distinguishing non-Gaussian modulations and propagation in the Gaussian channel,

$$\rho_E(\zeta) = \mathcal{D}_2(-r\zeta)\widetilde{\rho}_E\mathcal{D}_2^\dagger(-r\zeta), \tag{26}$$

where

$$\widetilde{\rho}_E = {\rm Tr}_A[\mathcal{S}(\theta)\rho_{\rm th}(n)\otimes\rho_{\mathcal{F}}(\mu)\mathcal{S}^\dagger(\theta)] \tag{27}$$

is the density matrix of a two-mode squeezed vacuum mixed with a thermal state. This density matrix is independent of the modulation parameter, and due to invariance of the von Neumann entropy with respect to unitary transformations of the density matrix, we immediately obtain

$$\overline{H(\rho_E(\zeta))} = H(\widetilde{\rho}_E). \tag{28}$$

While $\widetilde{\rho}_E$ is a Gaussian state and, therefore, is completely characterized by its covariance matrix, in order to find $\overline{\rho_E(\zeta)}$, it is convenient to have an explicit form of $\widetilde{\rho}_E$ in an operator form. It can be recovered from the covariance matrix. We find it constructive, however, to perform the calculation using the representation in terms of creation and annihilation operators and to demonstrate the emergence of the phase-space representation. It can be done, for example, as follows. Using the P representation for $\rho_{\rm th}$ in Eq. (27), it can be rewritten as $\widetilde{\rho}_E = \mathcal{F}(\mu_t)\widehat{\rho}_E\mathcal{F}^\dagger(\mu_t)$, where μ_t is defined by $\tau_t \equiv \tanh(\mu_t) = t\tanh(\mu)$ and

$$\begin{aligned}\widehat{\rho}_E =& \frac{1}{\pi\bar{n}}\int d\alpha e^{-|\alpha|^2/\bar{n}}\mathcal{D}_2(\alpha_c)\mathcal{D}_3(\alpha_s)\\ &\times|0\rangle\langle 0|\otimes\rho_{\rm th}^{(3)}(\bar{n}_E)\mathcal{D}_3^\dagger(\alpha_s)\mathcal{D}_2^\dagger(\alpha_c),\end{aligned} \tag{29}$$

with $\alpha_c = r\alpha\cosh(\mu_t)$ and $\alpha_s = -r\alpha^*\sinh(\mu_t)$. In this expression, $\rho_{\rm th}^{(3)}(n_E) = Z_E^{-1}\exp(-\beta_E a_3^\dagger a_3)$ is a thermal state characterized by the same average number of particles $n_E = r^2\sinh^2(\mu)$ as the magnitude of untrusted noise. Using the P

representation again turns Eq. (29) into

$$\widehat{\rho}_E = \frac{1}{\pi^2 n_r n_E}\int d\mathbf{z}\, e^{-|z_2|^2/n_r - |z_3+\tau_t z_2^*|^2/n_E} \times \mathcal{D}(\mathbf{z})|0\rangle\langle 0|\mathcal{D}^\dagger(\mathbf{z}), \tag{30}$$

where we have introduced $n_r = r^2 n\cosh^2(\mu_t) = r^2 n/(1-\tau_t^2)$, $d\mathbf{z} = dz_2 dz_3$, and

$$\mathcal{D}(\mathbf{z}) = \exp(z_2 a_2^\dagger + z_3 a_3^\dagger - \text{H.c.}). \tag{31}$$

A connection with the phase-space formalism is then established through Williamson's theorem [34], which guarantees that any Gaussian state can be presented as a transformation of a direct product of thermal states. In terms of the representation of the density matrix given by Eq. (30), this means that the form $-|z_2|^2/n_r - |z_3+\tau_t z_2^*|^2/n_E$ can be diagonalized by proper transformations. To this end, it is convenient to rewrite the argument in Eq. (31) as

$$\mathbf{z}\cdot\mathbf{a}^\dagger - \mathbf{z}^*\cdot\mathbf{a} = (\mathbf{z}\quad \mathbf{z}^*)\widehat{J}\begin{pmatrix}\mathbf{a}\\ \mathbf{a}^\dagger\end{pmatrix}, \tag{32}$$

where $\widehat{J} = \left(\begin{smallmatrix}0 & \widehat{1}\\ -\widehat{1} & 0\end{smallmatrix}\right)$, with $\widehat{1}$ being the 2×2 identity matrix, is a symplectic form consistent with the commutation relations $\mathcal{C} - \mathcal{C}^T = \widehat{J}$, where $\mathcal{C} = \left(\begin{smallmatrix}\mathbf{a}\\ \mathbf{a}^\dagger\end{smallmatrix}\right)\otimes\left(\begin{smallmatrix}\mathbf{a}\\ \mathbf{a}^\dagger\end{smallmatrix}\right)$. It can be seen that transformations of the creation and annihilation operators preserving the commutation relations induce "symplectic orthogonal" transformations of $z_{1,2}$. Indeed, the transformation of operators $\mathbf{a}\to\mathbf{b}$ according to

$$\widehat{R}\begin{pmatrix}\mathbf{a}\\ \mathbf{a}^\dagger\end{pmatrix} = \begin{pmatrix}\mathbf{b}\\ \mathbf{b}^\dagger\end{pmatrix} \tag{33}$$

induces the transformation $\mathbf{z}\to\mathbf{w}$:

$$-(\mathbf{z}\quad \mathbf{z}^*)\widehat{J}\widehat{R}\widehat{J} = (\mathbf{w}\quad \mathbf{w}^*). \tag{34}$$

For example, two-mode squeezing described by the operator $\mathcal{F}(\gamma)$ yields

$$\begin{aligned} w_2 &= z_2\cosh(\gamma) - z_3^*\sinh(\gamma),\\ w_3 &= z_3\cosh(\gamma) - z_2^*\sinh(\gamma). \end{aligned} \tag{35}$$

It turns out that two-mode squeezing is the only transformation needed for diagonalization of the form in the exponential term in Eq. (30), so that

$$\widehat{\rho}_E = \mathcal{F}(\gamma)\rho_{\text{th}}^{(2)}(n_2)\otimes\rho_{\text{th}}^{(3)}(n_3)\mathcal{F}^\dagger(\gamma), \tag{36}$$

where

$$\tanh(2\gamma) = \frac{2\tau_t}{Y+2}, \tag{37}$$

with $Y = X + \tau_t^2 - 1$, $X = n_r/n_E$, and

$$n_{2,3} = \frac{2n_E}{\sqrt{Y^2+4X}\pm Y}. \tag{38}$$

Collecting these results, we obtain the averaged environment density matrix (up to a ζ-independent unitary transformation) $\overline{\rho_E} = \int d\zeta\,\Pi_0(\zeta)\rho_E(\zeta)$, where

$$\rho_E(\zeta) = \mathcal{D}(\mathbf{z}(\zeta))\rho_{\text{th}}^{(2)}(n_2)\otimes\rho_{\text{th}}^{(3)}(n_3)\mathcal{D}^\dagger(\mathbf{z}(\zeta)), \tag{39}$$

with $z_2(\zeta) = -s\zeta r_E\cosh(\mu+\gamma)$ and $z_3(\zeta) = s\zeta^* r_E\sinh(\mu+\gamma)$.

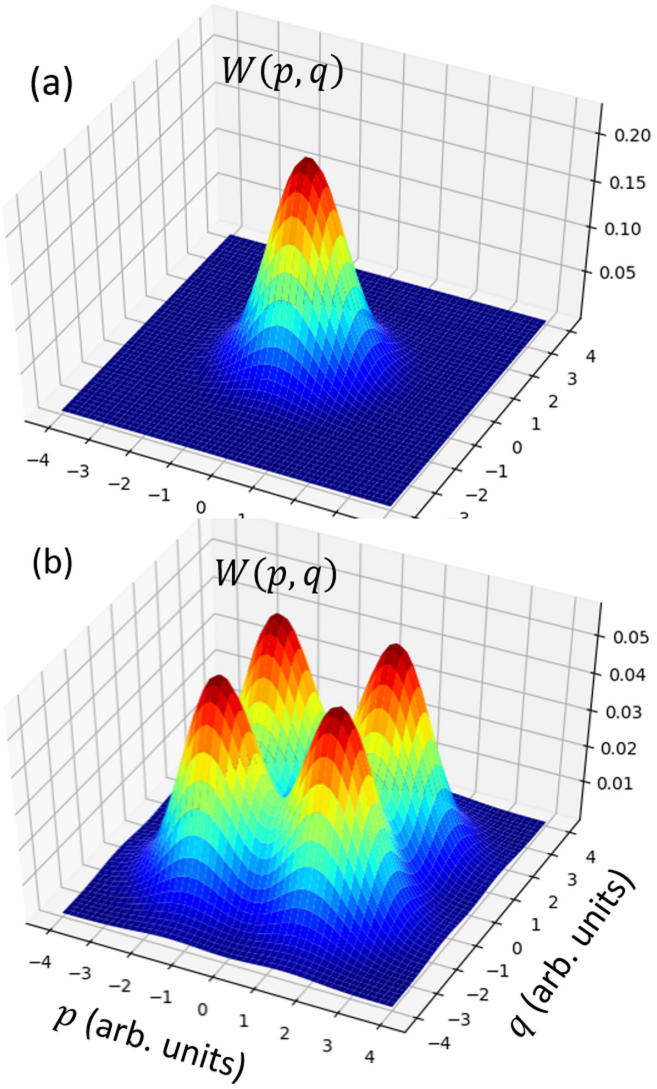

FIG. 3. Example of the Wigner distribution of the environment density matrix traced over one of the degrees of freedom, $\rho_E^{(\text{red})} = \text{Tr}_2[\widehat{\rho}_E]$, in the case of (a) weak and (b) strong modulations. For the sake of illustration, the distribution of ζ's is assumed to be uniform over points $\pm 1 \pm i$ of the complex plane.

IV. KEY GENERATION RATE

A. Strong modulation limit

The limit of strong modulations, when the magnitude of ζ exceeds characteristic scales describing the channel and environment modes, is the simplest since, in this limit, quantum correlations in the environment between individual transactions become negligible. Figure 3(a) shows the partial Wigner distribution of the environment density matrix in the case where the modulation parameter is strong, $s\gg 1$, so that the fluctuations of the displacement parameter exceed the width of the Gaussian states $s\Delta_\zeta \gg \max(n_2, n_3)$, where $n_{2,3}$ are given by Eq. (38) and Δ_ζ is the magnitude of a "typical" separation between points in the ζ plane. The multimodal character of the Wigner distribution in Fig. 3(b) is the principal feature of the environment density matrix when the magnitude of discretized modulations becomes too strong.

A formal manifestation of this observation is vanishing commutators of individual terms with $\zeta \neq \zeta'$ in $\overline{\rho_E}$,

$$[\rho_E(\zeta), \rho_E(\zeta')] \propto e^{-(\mathbf{z}(\zeta)-\mathbf{z}(\zeta'))^* \cdot \widehat{n}^{-1} \cdot (\mathbf{z}(\zeta)-\mathbf{z}(\zeta'))}, \tag{40}$$

where $\widehat{n} = \mathrm{diag}(n_2, n_3)$. Based on this, the perturbation theory can be used for an analysis of the spectrum of $\overline{\rho_E}$ with the characteristic decay of small terms $\propto e^{-s^2/s_0^2}$ with $s_0^{-2} \propto \Delta_\zeta r_E^2 (n_2^{-1} \cosh^2(\mu+\gamma) + n_3^{-1} \sinh^2(\mu+\gamma))$ as $s \to \infty$. The precise form of s_0 depends on the mutual arrangement of eigenvalues of individual terms in $\overline{\rho_E}$. For example, when $\Pi_0(\zeta) = 1/M$, where M is the total number of values of modulations, all eigenvalues of $\Pi_0(\zeta)\rho_E(\zeta)$ are M-fold degenerate and s_0^2 may acquire a factor depending on the details of how ζ is distributed in the complex plane. As will be apparent from the following, however, the exact asymptotic form of the Holevo bound may be of rather minor importance. Therefore, in the present paper, we limit ourselves to the zeroth order of the perturbation theory, when the overlap between the eigenstates of $\rho_E(\zeta)$ and $\rho_E(\zeta')$ for $\zeta \neq \zeta'$ is completely neglected.

In this case, the commutator above vanishes and the environment density matrix reduces to the direct sum of individual $\rho_E(\zeta)$'s. Taking into account that $H(\bigoplus_n \rho_n) = \sum_n H(\rho_n)$ for any set of commuting operators ρ_n, and $H(a\rho) = -a\ln(a) + aH(\rho)$ for a real number a and normalized ρ, we obtain

$$H(\overline{\rho_E}) = S(\Pi_0(\zeta)) + \overline{H(\rho_E(\zeta))}. \tag{41}$$

Thus, in the limit of strong modulations, the Holevo bound saturates at the entropy of the distribution of the modulation parameter. Since this entropy limits the amount of transmitted information, we conclude that in the limit of strong modulations the rate of generation of the secure key is vanishing and the QKD is impossible.

At practically the same time, the limit reached by $I(A:B)$ is strictly smaller than $S(\Pi_0(\zeta))$. On the one hand, it is limited by the reduced reconciliation efficiency of finite-size messages and the reduced detection efficiency. On the other hand, it depends on the details of how the modulation parameter enters the propagator $Q(\kappa|\zeta)$. For example, as shown in Eq. (19), the homodyne detection of quadratures depends on the value of modulation through $\langle\kappa_\zeta\rangle = \sqrt{2}\,\mathrm{Re}(t\zeta e^{i\theta})$. Then, in the limit of strong modulations, the mutual information asymptotically tends to the entropy of distribution of this parameter, $I(A:B) = S(\Pi_0(\langle\kappa_\zeta\rangle))$. Up to scaling, the distribution of $\langle\kappa_\zeta\rangle$ has the same form as that of the projection of the distribution of ζ onto the line passing through the origin of the complex plane at the angle determined by the angular parameter of the quadrature and the phase of the effective transmission coefficient t. If the distribution of ζ has a cluster form, after such projection the clusters may overlap, yielding a distribution with a smaller entropy.

From the QKD perspective, the consequence of mismatched asymptotics of $I(A:B)$ and $\chi(A:E)$ is that in the limit of strong modulations there is a sharp security boundary: there is a maximal magnitude, beyond which QKD is impossible.

It should be noted that, in the consideration above, the quadrature phase parameter θ is not presumed to be controlled by communicating parties. Such control can be achieved by synchronizing the local oscillator in the homogeneous detection of quadratures. On the one hand, this provides a means to ensure the certain orientation of the distribution $\Pi_0(\zeta)$ in the complex plane, thus minimizing the loss of information due to its projection on the real axis. On the other hand, due to the effect of the phase acquired during propagation, accounted for by the argument of the effective transmission coefficient t, such synchronization is a nontrivial task and poses a challenge for practical implementations of CV-QKD. Therefore, it is noteworthy that the analysis above confirms that such synchronization, while beneficial, is not strictly required [35]. Random variations of θ can be taken into consideration while optimizing particular implementations and accounted for in the estimate of the mutual information between the communicating parties.

We take this circumstance into account by limiting ourselves in the following numerical evaluations to distributions $t\zeta e^{i\theta}$ confined to the real axis. This does not significantly impact the generality, while it simplifies the discussion.

Because the physical origin of the vanishing key generation rate is the effective emergence of the classical ensemble of states due to the weak overlap of individual density matrices in the limit of strong variation, it affects all protocols based on displaced coherent states, including those with a Gaussian distribution of the displacing parameter. Because of the finite length of the sequence of transmitted quantum states, a signal of sufficiently strong amplitude will "separate" individual states, leading to a collapsing key generation rate. It must be noted that this kind of finite-length effect cannot be accounted for by reconciliation efficiency, which quantifies the error correction algorithm and renormalizes the mutual information. Moreover, a high efficiency (yielding $\lambda > 0.95$) is reached in the limit of a high signal-to-noise ratio [27–29], thus making the estimate of the protocol performance vulnerable with respect to the effect of emergence of classical ensembles when the length of the sequence of transmitted quantum states is relatively small.

B. Weak modulation limit

In the opposite limit of weak modulations (small s), both the mutual information and the Holevo bound vanish in a thresholdless manner and their Taylor expansions start with terms quadratic in s. Thus, in this limit,

$$R = s^2 C, \tag{42}$$

where

$$C = \frac{d^2}{ds^2}[I(A:B) - \chi(A:E)]. \tag{43}$$

The key can be generated if $C > 0$.

It follows straightforwardly from Eq. (19) that

$$\frac{d^2}{ds^2} I(A:B) = \frac{2}{\sigma^2}\mathbb{E}[\langle\kappa(\zeta)\rangle - \overline{\langle\kappa(\zeta)\rangle}]^2. \tag{44}$$

It should be noted that, in this limit, the nonideal reconciliation efficiency leads to the simple renormalization $\langle\kappa(\zeta)\rangle \to \sqrt{\lambda}\langle\kappa(\zeta)\rangle$, which can be considered rescaling of the displacement parameter or the phase mismatch [see Eq. (20)].

The Holevo bound is determined by the eigenvalues of ρ_E. When $s = 0$, they are given by the product of eigenvalues of $\rho_{\rm th}^{(2,3)}$ in Eq. (39). Since $\rho_{\rm th}^{(2,3)}$ are diagonal in the product of Fock bases, it is convenient to introduce a "vector" notation for the basis states $|\mathbf{l}\rangle \equiv |l_2, l_3\rangle$, so that $\rho_E^{(\mathbf{l})}(0)$, the eigenvalues at $s = 0$, can be expressed in terms of the average number of thermal photons $n_{2,3}$ as

$$\rho_E^{(\mathbf{l})}(0) = \frac{e^{-\beta_2 l_2 - \beta_3 l_3}}{(1+n_2)(1+n_3)}, \tag{45}$$

where $\beta_{2,3} = \ln(1 + 1/n_{2,3})$.

Since we are interested only in the variation of the eigenvalues, we can use the same approach as for the Feynman-Hellmann theorem. The first order is given by $\partial \rho_E^{(\mathbf{l})}/\partial s|_{s=0} = \langle \mathbf{l}|\partial \rho_E(0)/\partial s|\mathbf{l}\rangle$, while at second order we have

$$\left.\frac{\partial^2 \rho_E^{(\mathbf{l})}}{\partial s^2}\right|_{s=0} = \langle \mathbf{l}|\partial^2 \rho_E(0)/\partial s^2|\mathbf{l}\rangle + 2\sum_{\mathbf{m}\neq\mathbf{l}} \frac{\langle \mathbf{l}|\partial \rho_E(0)/\partial s|\mathbf{m}\rangle\langle \mathbf{m}|\partial \rho_E(0)/\partial s|\mathbf{l}\rangle}{\rho_{2,3}^{(\mathbf{l})}(0) - \rho_{2,3}^{(\mathbf{m})}(0)}, \tag{46}$$

where $\mathbf{l} = (l_2, l_3)$ and $\mathbf{m} = (m_2, m_3)$.

Introducing $s\mathcal{V}(\zeta) = \mathbf{z}(\zeta)\cdot\mathbf{a}^\dagger - \mathbf{z}^*(\zeta)\cdot\mathbf{a}$, these expressions can be rewritten in a more explicit form:

$$\begin{aligned}
\left.\frac{\partial}{\partial s}\rho_E^{(\mathbf{l})}\right|_{s=0} &= \langle \mathbf{l}|\left[\overline{\mathcal{V}(\zeta)}, \rho_E(0)\right]|\mathbf{l}\rangle, \\
\left.\frac{\partial^2}{\partial s^2}\rho_E^{(\mathbf{l})}\right|_{s=0} &= \langle \mathbf{l}|(\overline{\mathcal{V}^2(\zeta)}\rho_E(0) + \rho_E(0)\overline{\mathcal{V}^2(\zeta)})|\mathbf{l}\rangle \\
&\quad - 2\langle \mathbf{l}|\overline{\mathcal{V}(\zeta)\rho_E(0)\mathcal{V}(\zeta)}|\mathbf{l}\rangle.
\end{aligned} \tag{47}$$

Because of invariance of the von Neumann entropy with respect to unitary transformations of the density matrix, we can set $\overline{\zeta} = 0$ without any loss of generality, which yields

$$\left.\frac{\partial^2}{\partial s^2}\chi(A:E)\right|_{s=0} = \sum_{\mathbf{l}} \frac{\partial^2}{\partial s^2}\rho_E^{(\mathbf{l})}(0)\ln\left[\rho_E^{(\mathbf{l})}(0)\right]. \tag{48}$$

Using Eq. (47) in this expression, we obtain

$$\left.\frac{\partial^2}{\partial s^2}\chi(A:E)\right|_{s=0} = 2\overline{|\zeta|^2}r_E^2[\beta_2\cosh^2(\mu+\gamma) + \beta_3\sinh^2(\mu+\gamma)]. \tag{49}$$

Together with Eq. (44), this expression gives an explicit condition whether the QKD is possible in the limit of weak modulations.

We conclude our consideration of the limiting cases by noting that they imply that the key generation rate is a nonmonotonous function of the signal strength. Thus, the implementation of a QKD protocol based on discretized modulations must include a solution of the respective optimization problem which takes into account the characteristics of the communication channel and the magnitude of untrusted noise.

V. WEAK AND STRONG NOISE REGIMES

To investigate the dependence of the security boundary given by $C = 0$ on the parameters of the environment and coupling with it, we assume that the effective temperature of the environment is fixed. In Fig. 4, we plot $C(r_E, \mu, \omega) = 0$, the phase diagram separating secure and insecure regimes, with the imposed constraint $r_E^2\sinh^2(\mu) = \text{const}$, as a function of the coupling with the environment and the carrier frequency (energy) of the quantum states. It demonstrates that at low frequencies, the security boundary obtained in the weak modulation limit correctly distinguishes secure and insecure regimes even when the modulation is not necessarily weak. The signal dependencies of the key generation rate presented in Fig. 5(a) show that the sign of R does not change with the magnitude of displacement.

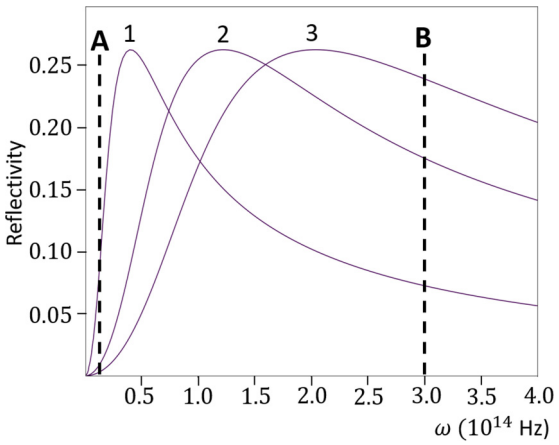

FIG. 4. The security boundary $C(r_E, \omega) = 0$ [see Eq. (43)] up to the midinfrared region (the shortest wavelength is 4.7 μm) for a fixed effective temperature of the environment: (1) $T = 100$ K; (2) $T = 300$ K; (3) $T = 500$ K. The regions above and below the curve correspond to insecure and secure regimes, respectively. Dashed vertical lines A and B mark the frequencies, for which the magnitude dependence of the key generation rate is plotted in Figs. 5(a) and 5(b), respectively.

The security boundary defined as $C = 0$ predicts that with increasing frequency the maximal coupling with the environment permitting generation of the key eventually starts to decrease, signifying that the condition $C = 0$ is no longer applicable when the number of thermal photons at the energy of transmitted states becomes *smaller* than 1. This observation is confirmed by comparing the security boundary found as $C = 0$ with the numerically obtained security boundary presented in Fig. 6.

It should be noted, however, that the condition $C = 0$ correctly predicts the security of protocols utilizing weak states even in this case. To illustrate this circumstance, we show in Fig. 5(b) the signal dependence of the key generation rate in the case where the thermal noise is small. It shows that for systems that are in different regions according to the weak signal and a precise condition, there is a critical magnitude of the signal below which QKD is impossible. Taking into account the effect of the nonideal reconciliation efficiency and nonoptimal distribution of the displacement parameter discussed in the previous section, this means that, in the weak noise regime, protocols based on discretized modulations may permit the key generation only when the signal magnitude is within a certain range. A detailed investigation of the

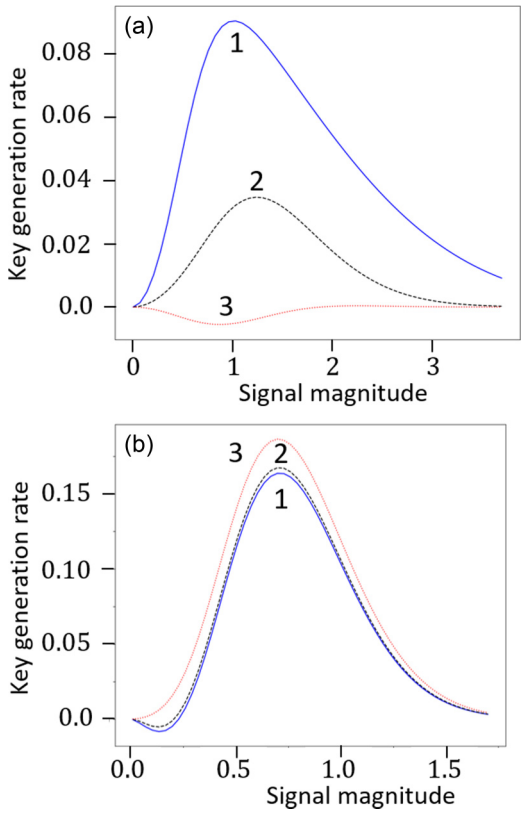

FIG. 5. Numerical evaluation of the signal dependence of the key generation rate at the frequencies marked in Fig. 4: (A) $\omega = 2 \times 10^{13}$ Hz and $r_E^2 = 0.01$ and (B) $\omega = 3 \times 10^{14}$ Hz and $r_E^2 = 0.22$.

critical strength requires a more refined approach and will be presented elsewhere.

On the contrary, in the strong noise regime, which is of the most interest from the perspective of low-frequency implementations of QKD, the emergence of the lower threshold

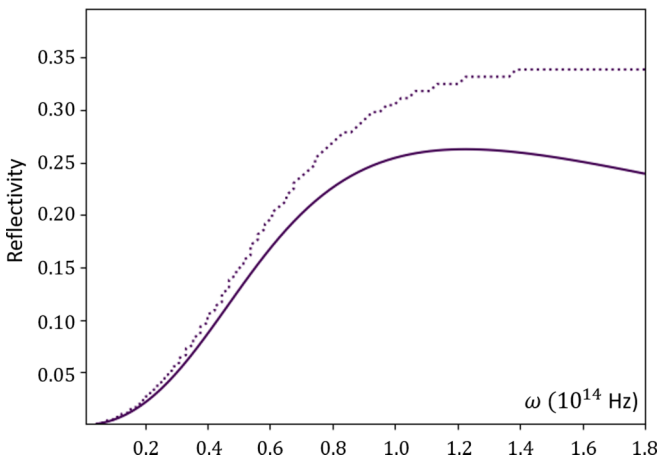

FIG. 6. Security boundary on the (r_E, ω) plane for $T = 300$ K. The solid line represents the security boundary based on the weak signal approximation and the dotted line shows the security boundary obtained by a numerical simulation of QKD transactions with discretized modulations.

appears to be a rather marginal effect and the security of QKD can be investigated using the weak-signal approximation.

VI. CONCLUSION

In anticipation of the appearance of implementations of QKD protocols in the spectral domain below the midinfrared, we have considered a general problem of QKD protocols based on displaced thermal states with a discretized distribution of the displacement parameter. We have investigated specific features of such protocols distinguishing them from well-studied protocols utilizing Gaussian states. We developed a basic formalism separating the effects of the Gaussian channel and non-Gaussian modulations. With the help of this formalism, we have studied the effect of the magnitude of the quasiclassical driving field on the source of displaced quantum states.

The main important feature, specific for protocols with discretized modulations, is the impossibility of generating a secret key, in the limit of the strong quasiclassical field. The physical origin of such a collapse of QKD is the weak overlap of the density matrices of individual states, which makes the transmitted sequence of quantum states essentially classical. In this limit, information available to the eavesdropper is limited only by the entropy of the distribution of the displacement parameter, which, in turn, limits from above the mutual information between legitimate communicating parties.

Since the emergence of the classical ensemble is due to lacunae in the factual filling of the complex plane by the values of the displacement parameter used for preparation of transmitted states, it becomes a limiting factor whenever the number of transmitted states is too small, even if they are sampled from the Gaussian distribution. This is a manifestation of possible quantum correlations between the transmitted states and the environment (eavesdropper). This indicates that accounting for the finite-length effect by the reconciliation efficiency may not be enough to estimate correctly the key generation rate.

The numerical investigation of the signal strength dependence of the key generation rate revealed that two operating regimes must be distinguished: strong and weak noise. The strong noise regime is relevant when the number of thermal photons is large and is of the most importance for low-frequency QKD implementations. In this case, the security boundary is determined by the weak signal limit and we have found its explicit form.

The weak noise regime corresponds to a small number of thermal photons. Numerical simulations showed that in this regime a low-signal threshold may appear, so that the secret key can be generated only when the signal is sufficiently strong (but not too strong because of the transition to the classical ensemble discussed above).

ACKNOWLEDGMENT

The work was supported by Air Force Office of Scientific Research (AFOSR) Grant No. FA9550-16-1-0363.

[1] V. Scarani, S. Iblisdir, N. Gisin, and A. Acin, Rev. Mod. Phys. **77**, 1225 (2005).

[2] N. J. Cerf and J. Fiurasek, in *Progress in Optics*, Vol. 49 (Elsevier, Amsterdam, 2006), pp. 455–545.

[3] M. Ozawa, Phys. Rev. A **67**, 042105 (2003).

[4] G. V. Assche, *Quantum Cryptography and Secret-Key Distillation* (Cambridge University Press, Cambridge, UK, 2006).

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

[6] C. Weedbrook, S. Pirandola, R. Garcia-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[7] E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).

[8] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Adv. Quant. Technol. **1**, 1800011 (2018).

[9] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).

[10] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).

[11] C. Weedbrook, C. Ottaviani, and S. Pirandola, Phys. Rev. A **89**, 012309 (2014).

[12] L. Brillouin, *Science and Information* (Academic Press, New York, 1962).

[13] Within the fields of conventional communications and signal processing, such signals are called quantized [36], but for obvious reasons we use less confusing terminology and call them discretized.

[14] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma, New J. Phys. **17**, 053014 (2015).

[15] A. Becir, F. a. A. El-Orany, and M. R. B. Wahiddin, Int. J. Quantum. Info. **10**, 1250004 (2012).

[16] A. Leverrier and P. Grangier, Phys. Rev. A **83**, 042312 (2011).

[17] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).

[18] K. Bradler and C. Weedbrook, Phys. Rev. A **97**, 022310 (2018).

[19] N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, Sci. Adv. **3**, e1701491 (2017).

[20] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, Phys. Rev. X **9**, 021059 (2019).

[21] J. Lin, T. Upadhyaya, and N. Lutkenhaus, Phys. Rev. X **9**, 041064 (2019).

[22] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lutkenhaus, Phys. Rev. A **79**, 012307 (2009).

[23] P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, Phys. Rev. A **98**, 012340 (2018).

[24] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, arXiv:1906.01645.

[25] F. Grosshans and P. Grangier, arXiv:quant-ph/0204127.

[26] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Info. Comput. **3**, 532 (2003).

[27] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[28] L. Ruppert, V. C. Usenko, and R. Filip, Phys. Rev. A **90**, 062310 (2014).

[29] P. Jouguet, D. Elkouss, and S. Kunz-Jacques, Phys. Rev. A **90**, 042329 (2014).

[30] A. Perelomov, *Generalized Coherent States and Their Applications* (Springer-Verlag, Berlin, 1986).

[31] M. Navascues, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).

[32] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[33] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).

[34] J. Williamson, Am. J. Math. **58**, 141 (1936).

[35] D. B. S. Soh, C. Brif, P. J. Coles, N. Lutkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041010 (2015).

[36] R. G. Gallager, *Principles of Digital Communication* (Cambridge University Press, New York, 2008).