Continuous-variable quantum key distribution using thermal states

Christian Weedbrook,[1,*] Stefano Pirandola,[2] and Timothy C. Ralph[3]

[1]*Center for Quantum Information and Quantum Control, Department of Electrical and Computer Engineering and Department of Physics, University of Toronto, Toronto, M5S 3G4, Canada*

[2]*Department of Computer Science, University of York, Deramore Lane, York YO10 5GH, United Kingdom*

[3]*Centre for Quantum Computation and Communication, School of Mathematics and Physics, University of Queensland, St Lucia, Queensland 4072, Australia*

(Received 20 October 2011; revised manuscript received 15 May 2012; published 17 August 2012)

We consider the security of continuous-variable quantum key distribution using thermal (or noisy) Gaussian resource states. Specifically, we analyze this against collective Gaussian attacks using direct and reverse reconciliation where both protocols use either homodyne or heterodyne detection. We show that in the case of direct reconciliation with heterodyne detection, an improved robustness to channel noise is achieved when large amounts of preparation noise is added, as compared to the case when no preparation noise is added. We also consider the theoretical limit of infinite preparation noise and show a secure key can still be achieved in this limit provided the channel noise is less than the preparation noise. Finally, we consider the security of quantum key distribution at various electromagnetic wavelengths and derive an upper bound related to an entanglement-breaking eavesdropping attack and discuss the feasibility of microwave quantum key distribution.

DOI: 10.1103/PhysRevA.86.022318 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.−p

I. INTRODUCTION

Continuous-variable quantum key distribution (QKD) [1,2] is the ability to generate a secret key between two distant parties, Alice and Bob, which can be used to encrypt messages for secure communication. This is achieved by using Gaussian quantum resource states [2], where its theoretical security is guaranteed by the no-cloning theorem. A typical Gaussian modulated protocol [3–8] involves Alice randomly displacing a number of pure vacuum modes and sending them over an insecure quantum channel to Bob. These modes are then measured by Bob using either homodyne [3] or heterodyne detection [5]. The various stages of classical communication [1] follow next, including error correction, where either direct [3] or reverse reconciliation [4] can be used.

Generally, in Gaussian QKD protocols, it is assumed that Alice starts off with a large number of *pure* vacuum states. However, this is an idealization and is never quite true in practice with small amounts of unknown Gaussian preparation noise often being present. The idea of analyzing the security of continuous-variable QKD using such noisy or thermal states was considered in [9,10]. Here they showed, using reverse reconciliation, that the distance over which continuous-variable QKD was secure declined rapidly as the resource states became noisier, ultimately resulting in the inability to generate a secure key. However, in a subsequent work [11], it was shown using direct reconciliation that the distance with which the protocol is secure does not decline to zero as the states become noisier. In fact, even though the rate of generation of the secret key decreases for increasing noise, it remains bigger than zero for values of transmission $T > 0.5$. This means that the security threshold of the protocol remains at $T = 0.5$ for extremely high values of preparation noise. Thus, up to a requirement of a strong modulation of the input, thermal-state QKD is able to reach distances comparable to standard QKD. Furthermore, an application of the analysis of noisy coherent states using direct reconciliation was found by considering the security of QKD at various wavelengths of the electromagnetic spectrum, revealing regions of security from the optical all the way down into the microwave region [11].

In this paper, we build upon the work presented in [11] and outline our results here. We begin by using the previous analysis of reverse [10,11] and direct reconciliation [11] using homodyne detection and extending them both to study the case of heterodyne detection. For the case of direct reconciliation and heterodyne detection we show an improved robustness to channel noise when large amounts of preparation noise is added, as compared to the case with zero preparation noise. This effect of noise improving the performance of QKD was identified in discrete-variable QKD [12] and its manifestation in the context of continuous-variable QKD was found in [13,14]. In [11] it was shown that direct reconciliation could tolerate a thermal variance of 10^4 times that of the pure vacuum mode and still show no deterioration in the security threshold of the protocol (albeit with a reduced key rate). Here we extend this result and show that, provided the channel noise is less than the preparation noise, the same protocol can, in principle, tolerate any amount of preparation noise, again at a cost of decreasing key rate. Finally, we consider the security of QKD at various electromagnetic wavelengths and develop an improved security bound along with an upper bound related to an entanglement-breaking eavesdropping attack.

This paper is organized as follows. Section II introduces the main concepts of thermal-state QKD. In Secs. III and IV the secret key rates for direct and reverse reconciliation using both homodyne and heterodyne detection are given. Section V considers QKD in the so-called classical limit where an infinite amount of preparation noise is added for direct reconciliation using homodyne detection. Finally, before concluding in Sec. VIII, we look at the security of QKD at various wavelengths along with the feasibility of microwave QKD in Sec. VII.

*christian.weedbrook@gmail.com

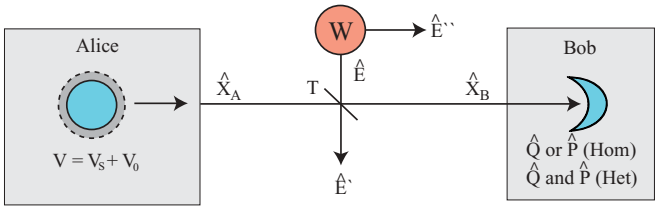


FIG. 1. (Color online) Schematic of a continuous-variable QKD protocol using thermal states. The loss in the quantum channel is modeled by a beam splitter with channel transmission T. The eavesdropping attack is a Gaussian collective attack in the form of an entangling cloner attack where the variance of the EPR state is W with the modes of the EPR beam described by the operators $\hat{E}''$ and $\hat{E}'$. The initial mode sent by Alice $\hat{X}_A$ is a thermal state, and once Bob receives the mode $\hat{X}_B$ he will perform either a homodyne (Hom) or heterodyne (Het) measurement on it.

II. THERMAL-STATE QUANTUM KEY DISTRIBUTION

The initial stages of a thermal-state QKD protocol consists in Alice preparing a number of randomly displaced thermal states and then sending them to Bob over an insecure quantum channel monitored by Eve (cf., Fig. 1). This initial mode prepared by Alice can be described in the Heisenberg picture as

$$\hat{X}_A = X_S + \hat{X}_0, \tag{1}$$

where X_S describes the classical signal encoding and $\hat{X}_0$ describes the quantum noise of the thermal mode. Here the quadrature variables are given by $\hat{X}_A \in \{\hat{Q}_A, \hat{P}_A\}$, $X_S \in \{Q_A, P_A\}$ and $\hat{X}_0 \in \{\hat{Q}_0, \hat{P}_0\}$. The overall variance $V := V(\hat{X}_A)$ of Alice's initially prepared modes is given by

$$V = V_S + V_0, \tag{2}$$

where V_S is a Gaussian distribution with zero mean. Here V_0 is the shot noise, which can be defined in terms of the conditional variance as

$$V(\hat{Q}_A|Q_A) = V(\hat{P}_A|P_A) = V_0 \geqslant 1, \tag{3}$$

where the conditional variance is defined as [15,16]

$$V(\hat{X}|Y) = V(\hat{X}) - \frac{|\langle \hat{X}Y\rangle|^2}{V(Y)}. \tag{4}$$

We can decompose the shot-noise variance as $V_0 = 1 + \beta$, where β is the variance of the preparation noise at Alice's station and 1 denotes the variance of the pure vacuum mode. It is common in most continuous-variable QKD protocols to theoretically let $V = V_S + 1$, i.e., zero preparation noise ($\beta = 0$) in Alice's mode preparation. However, in our analysis we consider the general case where β is different from zero. This means that the shot-noise V_0 (that we also call the "purity") can be greater than 1. Then we make the valid assumption that this preparation noise is restricted to Alice's station and is not accessible, or known, to Eve (or even to Alice for that matter).

The most important type of eavesdropping attack is the collective Gaussian attack [17–19]. It was shown that such an attack is the most powerful attack allowed by quantum physics, up to a suitable symmetrization of the protocols [20]. It consists in Eve interacting her independent ancilla modes with Alice's mode for each run of the protocol in such a way to generate a memoryless (or one-mode) Gaussian channel. The entangling cloner [21] is the most important and practical example of a collective Gaussian attack and is used in our analysis. This consists in Eve perfectly replacing the quantum channel between Alice and Bob with her own quantum channel where the loss is simulated by a beam splitter with transmission $T \in [0,1]$.

She then prepares ancilla modes $\hat{E}$ and $\hat{E}''$ in an Einstein-Podolsky-Rosen (EPR) entangled Gaussian state [22] with variance W (see Fig. 1). Eve keeps one mode $\hat{E}''$ and injects the other mode $\hat{E}$ into the unused port of the beam splitter, leading to the output mode $\hat{E}'$. This operation is repeated identically and independently for each signal mode sent by Alice. Eve's output modes are then stored in a quantum computer and detected collectively at the end of the protocol. Eve's final measurement is optimized based on Alice and Bob's classical communication. Note that this attack can be simply described by two parameters: the channel transmission T and the channel noise W. The latter parameter can be replaced by the equivalent noise of the channel,

$$\chi = \frac{(1-T)}{T} + \epsilon, \tag{5}$$

where the first term $(1-T)/T$ corresponds to the noise induced by the loss and ϵ is the excess channel noise, which can be written as $\epsilon = (W-1)(1-T)/T$. In the particular case where $W = 1$, or equivalently $\epsilon = 0$ (no excess noise), the attack corresponds to a pure loss channel.

III. REVERSE RECONCILIATION

We begin the analysis by considering reverse reconciliation [4] (denoted by the symbol ◀) using homodyne and heterodyne detection and then in the following section consider direct reconciliation. We note that there is also another postprocessing technique known as postselection [7]. However, such a technique is quite involved and thus lies outside the scope of this paper. Also note that reverse reconciliation using homodyne detection has been analyzed before [9,10]. For completeness, we give the derivation for reverse reconciliation for homodyne detection so as to help in the derivation for heterodyne detection. Before commencing we make a brief comment about notation. When we consider homodyne detection the relevant variable X_B is $Q_B \in \mathbb{R}$ (or $P_B \in \mathbb{R}$, equivalently). On the other hand, when considering heterodyne detection, the relevant variable X_B is the pair $\{Q_B, P_B\} \in \mathbb{R}^2$. Also, a variable with a hat is an operator, while the same variable without a hat is the corresponding classical variable after measurement.

A. Homodyne detection

The secret key rate $R^{\blacktriangleleft[\mathrm{Hom}]}$ for reverse reconciliation where Bob uses homodyne detection is given by

$$R^{\blacktriangleleft[\mathrm{Hom}]} := I(X_A : X_B) - I(X_B : E), \tag{6}$$

where the mutual information between Alice and Bob is given by

$$I(X_A : X_B) := H(X_B) - H(X_B|X_A), \tag{7}$$

where

$$H(X_B) = \tfrac{1}{2}\log_2 V(\hat{X}_B) \tag{8}$$

is the Shannon (or classical) entropy and

$$H(X_B|X_A) = \tfrac{1}{2}\log_2 V(\hat{X}_B|X_A) \tag{9}$$

is the conditional Shannon entropy [23]. The mutual information between Eve and Bob is given by the Holevo bound [24], defined as

$$I(X_B : E) := S(E) - S(E|X_B), \tag{10}$$

where $S(\cdot)$ is the von Neumann (or quantum) entropy. The von Neumann entropy of a Gaussian state ρ containing n modes can be written in terms of its symplectic eigenvalues [25]

$$S(\rho) = \sum_{k=1}^{n} g(\nu_k), \tag{11}$$

where

$$g(\nu) = \left(\frac{\nu+1}{2}\right)\log_2\left(\frac{\nu+1}{2}\right) - \left(\frac{\nu-1}{2}\right)\log_2\left(\frac{\nu-1}{2}\right). \tag{12}$$

We will show how to explicitly calculate the symplectic spectrum $\boldsymbol{\nu} = \{\nu_1, \ldots, \nu_n\}$ soon.

To begin with, though, we calculate Alice and Bob's mutual information. To achieve this the first step is to consider the output modes at Bob's (and Eve's) station. These are given, respectively, by

$$V(\hat{Q}_B) = V(\hat{P}_B) = (1-T)W + TV := b_V, \tag{13}$$

$$V(\hat{Q}_{E'}) = V(\hat{P}_{E'}) = (1-T)V + TW := e_V, \tag{14}$$

with the following conditional variances:

$$V(\hat{Q}_B|Q_A) = V(\hat{P}_B|P_A) = (1-T)W + TV_0 := b_1, \tag{15}$$

$$V(\hat{Q}_{E'}|Q_A) = V(\hat{P}_{E'}|P_A) = (1-T)V_0 + TW := e_1, \tag{16}$$

derived using the definition given in Eq. (4). Using Eq. (7) with Eqs. (13) and (15) we can calculate Alice and Bob's mutual information to be

$$I(X_A : X_B) = \frac{1}{2}\log_2\left[\frac{(1-T)W + TV_S + TV_0}{(1-T)W + TV_0}\right]. \tag{17}$$

Note that, ultimately in the above equation it is V_0 that will be varied in our calculations. Next up is the calculation of Eve and Bob's mutual information, i.e., Eq. (10). First, though, we need to introduce the covariance matrix. The covariance matrix $\mathbf{V}$ can be constructed using the following definitions of its matrix elements:

$$V_{lm} := \tfrac{1}{2}\langle \hat{Y}_l\hat{Y}_m + \hat{Y}_m\hat{Y}_l\rangle - \langle\hat{Y}_l\rangle\langle\hat{Y}_m\rangle, \tag{18}$$

$$V_{ll} = \left\langle \hat{Y}_l^2\right\rangle - \langle\hat{Y}_l\rangle^2 := V(\hat{Y}_l), \tag{19}$$

where $\hat{Y}_l$ is the lth element of the quadrature row vector $\hat{\mathbf{Y}} = (\hat{Q}_1, \hat{P}_1, \ldots, \hat{Q}_n, \hat{P}_n)$, which describes the bosonic system of n modes. As mentioned previously, to calculate Eq. (10), we need to calculate the symplectic spectrum of the appropriate covariance matrices. The symplectic spectrum $\boldsymbol{\nu} = \{\nu_1, \ldots, \nu_n\}$ of an arbitrary covariance matrix $\mathbf{V}$ can be calculated by finding the (standard) eigenvalues of the matrix $|i\boldsymbol{\Omega}\mathbf{V}|$, where $\boldsymbol{\Omega}$ defines the symplectic form and is given by

$$\boldsymbol{\Omega} := \bigoplus_{k=1}^{n}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{20}$$

Here $\bigoplus$ is the direct sum indicating adding matrices on the block diagonal.

Eve's covariance matrix is made up from the two modes $\hat{E}'$ and $\hat{E}''$:

$$\mathbf{V}_E(V,V) = \begin{pmatrix} \mathrm{diag}[e_V, e_V] & \varphi\mathbf{Z} \\ \varphi\mathbf{Z} & W\mathbf{I} \end{pmatrix}, \tag{21}$$

where $\varphi = [T(W^2-1)]^{1/2}$ and the notation "diag" simply means a matrix with the arguments on the diagonal elements of a matrix and zeros everywhere else. Here $\mathbf{Z}$ and $\mathbf{I}$ are the Pauli matrices

$$\mathbf{Z} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{22}$$

To calculate Eve's symplectic spectrum, we note that a particular covariance matrix of the form

$$\mathbf{V} = \begin{pmatrix} a\mathbf{I} & \sqrt{T}c\mathbf{Z} \\ \sqrt{T}c\mathbf{Z} & b\mathbf{I} \end{pmatrix} := \mathbf{V}(a,b,c,T), \tag{23}$$

where $c \geqslant 0$ and $T \in [0,1]$ has a symplectic spectrum with a simple expression given by

$$\nu_\pm := \tfrac{1}{2}[\sqrt{y} \pm (a-b)], \tag{24}$$

where $y = (a+b)^2 - 4c^2T \geqslant 4$ [2]. Therefore, using the above, Eve's symplectic spectrum can be expressed in a more compact form as

$$\nu_E^\pm = \tfrac{1}{2}[\sqrt{(e_V+W)^2 - 4T(W^2-1)} \pm (e_V - W)]. \tag{25}$$

Next we need to calculate the symplectic spectrum of the covariance matrix $\mathbf{V}_{E|X_B}$. This represents the covariance matrix of a system where one of the modes has been measured using homodyne detection (in this case Bob) and is given by [2,26,27]

$$\mathbf{V}_{E|X_B} = \mathbf{V}_E - (b_V)^{-1}\mathbf{D}\boldsymbol{\Pi}\mathbf{D}^T, \tag{26}$$

where

$$\boldsymbol{\Pi} := \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}. \tag{27}$$

Here $\mathbf{D}$ is a 4×2 matrix describing the (quantum) correlations between Eve's modes $\{\hat{E}', \hat{E}''\}$ and Bob's output mode $\hat{X}_B$. It is given by

$$\mathbf{D} := \begin{pmatrix} \langle\hat{E}'\hat{X}_B\rangle\mathbf{I} \\ \langle\hat{E}''\hat{X}_B\rangle\mathbf{Z} \end{pmatrix} = \begin{pmatrix} \xi\mathbf{I} \\ \phi\mathbf{Z} \end{pmatrix}, \tag{28}$$

where

$$\xi = \sqrt{T(1-T)}(V_S + V_0 - W), \tag{29}$$

$$\phi = \sqrt{1-T}\sqrt{W^2-1}, \tag{30}$$

and we have used $\hat{X}_B = \sqrt{T}\hat{X}_A + \sqrt{1-T}\hat{E}$ and $\hat{E}' = \sqrt{1-T}\hat{X}_A - \sqrt{T}\hat{E}$. Using Eq. (26) we find that Eve's conditional covariance matrix is given by

$$\mathbf{V}_{E|X_B} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}, \tag{31}$$

where

$$\mathbf{A} = \begin{pmatrix} \frac{VW}{T(V-W)+W} & 0 \\ 0 & (1-T)V + TW \end{pmatrix},$$

$$\mathbf{B} = \begin{pmatrix} \frac{1-T+TWV}{TV+W-TW} & 0 \\ 0 & W \end{pmatrix},$$

$$\mathbf{C} = \begin{pmatrix} \sqrt{T(W^2-1)}\left(2 - \frac{V}{TV+W-TW}\right) & 0 \\ 0 & -\sqrt{T(W^2-1)} \end{pmatrix}.$$

The symplectic spectrum of the above conditional covariance matrix is composed by the two eigenvalues [28]

$$\nu_{\pm} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\det\mathbf{V}}}{2}}, \tag{32}$$

where $\det\mathbf{V}$ (the determinant of the covariance matrix) and $\Delta := \det\mathbf{A} + \det\mathbf{B} + 2\det\mathbf{C}$ are global symplectic invariants. Note that these quantities can also be simply expressed in terms of the symplectic spectrum as

$$\det\mathbf{V} = \nu_+^2\nu_-^2, \quad \Delta = \nu_+^2 + \nu_-^2. \tag{33}$$

Using Eq. (32), the corresponding symplectic spectrum $\boldsymbol{\nu}_{E|X_B}$ of $\mathbf{V}_{E|X_B}$ can be calculated but is not written down explicitly here due to its length. Finally, using Eq. (11) and Eq. (12) with the just-computed symplectic spectra, we can determine Bob and Eve's mutual information. The final secret key rate $R^{\blacktriangleleft[\mathrm{Hom}]}$ is calculated and plotted in Fig. 2(a) using various values of V_0 for a lossy channel (i.e., a quantum channel with only loss and no added noise, i.e., $W = 1$). We find that, for only moderate values of V_0, the security of the protocol reduces rapidly.

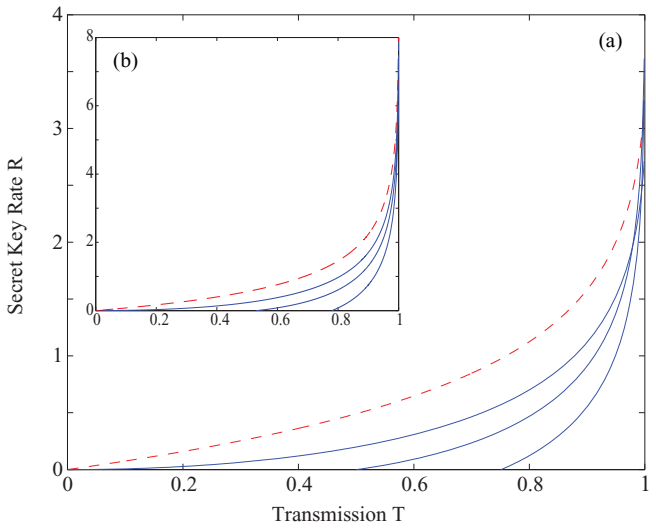


FIG. 2. (Color online) Secret key rates for reverse reconciliation using (a) homodyne detection and (b) heterodyne detection for various values of V_0. The top dashed (red) line is a pure encoded state sent by Alice with the solid (blue) lines giving different values of impurity, i.e., $V_0 = 2,3,5$ from top to bottom. Here $V_S = 10^3$ and $W = 1$ (i.e., only loss on the quantum channel).

B. Heterodyne detection

The secret key rate for reverse reconciliation where Bob now employs heterodyne detection is given by

$$R^{\blacktriangleleft[\mathrm{Het}]} := I(X_A : X_B) - I(X_B : E), \tag{34}$$

where, as mentioned previously, X_B is $\{Q_B, P_B\} \in \mathbb{R}^2$ for heterodyne detection and not $Q_B \in \mathbb{R}$ (or equivalently, $P_B \in \mathbb{R}$), as it was previously for homodyne detection. The mutual information between Alice and Bob is again defined as

$$I(X_A : X_B) := H(X_B) - H(X_B|X_A), \tag{35}$$

except now the Shannon entropies are

$$H(X_B) = \log_2 V(\hat{X}_B) \tag{36}$$

and

$$H(X_B|X_A) = \log_2 V(\hat{X}_B|X_A). \tag{37}$$

Note that the above two formulas do not have the usual factor of $1/2$ out the front. This indicates that twice the amount of information is obtained using heterodyne detection, but at a cost of the extra unit of vacuum noise introduced at the beam splitter. The mutual information between Eve and Bob is again given by the Holevo information,

$$I(X_B : E) := S(E) - S(E|Q_B, P_B), \tag{38}$$

but now $S(E|Q_B, P_B)$ is calculated from the symplectic spectrum $\boldsymbol{\nu}_{E|Q_B,P_B}$ of the conditional covariance matrix $\mathbf{V}_{E|Q_B,P_B}$. The variances of the quadratures of the output modes after Bob's heterodyne measurement are given by

$$V(\hat{Q}_B) = V(\hat{P}_B) = \tfrac{1}{2}(b_V + 1) := b'_V, \tag{39}$$

where b_V is defined in Eq. (13). The following conditional variances now apply:

$$V(\hat{Q}_B|Q_A) = V(\hat{P}_B|P_A) = \tfrac{1}{2}(b_1 + 1). \tag{40}$$

Using Eq. (35) we calculate Alice and Bob's mutual information to be

$$I(X_A : X_B) = \log_2\left[\frac{(1-T)W + TV_S + TV_0 + 1}{(1-T)W + TV_0 + 1}\right]. \tag{41}$$

The covariance matrix of Eve conditioned on Bob's heterodyne measurement results $\{Q_B, P_B\}$ is given by [2]

$$\mathbf{V}_{E|Q_B,P_B} = \mathbf{V}_E - \theta^{-1}\mathbf{D}(\boldsymbol{\Omega}\mathbf{V}_B\boldsymbol{\Omega}^T + \mathbf{I})\mathbf{D}^T, \tag{42}$$

where $\mathbf{V}_E$ is given by Eq. (21) and $\mathbf{V}_B = b_V\mathbf{I}$. Here $\theta := \det\mathbf{V}_B + \mathrm{Tr}\mathbf{V}_B + 1$ and $\mathbf{D}$ is defined previously in Eq. (28). We find that $\theta = b_V^2 + 2b_V + 1$ and $\boldsymbol{\Omega}\mathbf{V}_B\boldsymbol{\Omega}^T + \mathbf{I} = \mathbf{V}_B + \mathbf{I}$. We find that

$$\mathbf{V}_{E|Q_B,P_B} = \begin{pmatrix} a\mathbf{I} & \sqrt{T}c\mathbf{Z} \\ \sqrt{T}c\mathbf{Z} & b\mathbf{I} \end{pmatrix}, \tag{43}$$

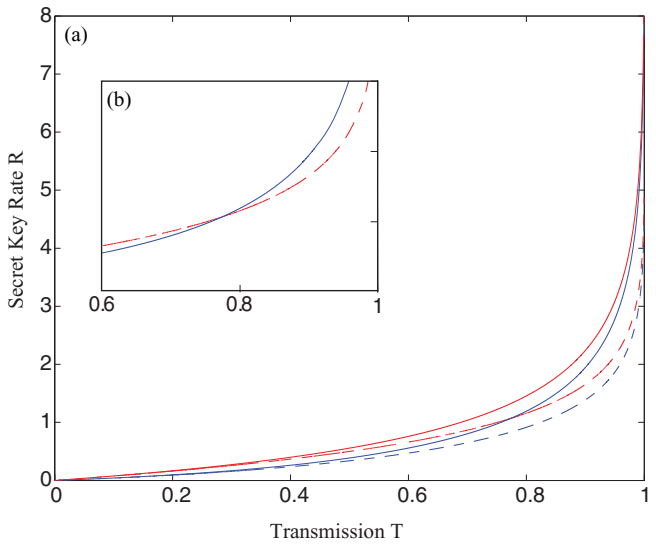


FIG. 3. (Color online) (a) Comparison of reverse reconciliation using homodyne detection (dashed lines) against heterodyne detection (solid lines) for $V_0 = 1$ (red lines) and $V_0 = 1.5$ (blue lines) and with only loss on the quantum channel, i.e., $W = 1$ with $V_S = 10^3$. (b) Close-up view of (a), where $V_0 = 1.5$ for heterodyne detection [solid (blue) line] crosses over with the pure state [dotted (red) line] for homodyne detection.

where

$$a = \frac{(1-T)V + (T+V)W}{1 + TV + (1-T)W},$$
$$b = \frac{1 - T + (1+TV)W}{1 + TV + (1-T)W},$$
$$c = \sqrt{W^2 - 1}\left(2 - \frac{1+V}{1 + TV + (1-T)W}\right).$$

The above covariance matrix has the corresponding symplectic spectrum

$$\nu^{\pm}_{E|Q_B,P_B} = \tfrac{1}{2}[\sqrt{y} \pm (a-b)], \tag{44}$$

where $y = (a+b)^2 - 4c^2T$ as given by Eq. (24). Using this, the final secret key rate $R^{\blacktriangleleft[\mathrm{Het}]}$ can be calculated and is plotted in Fig. 2(b) for different values of V_0.

We can now compare homodyne detection to heterodyne detection using reverse reconciliation with, for example, an impurity of $V_0 = 1.5$. This is plotted in Fig. 3(a). We note that after a certain value of line transmission ($\approx T > 0.79$) it is better, in terms of information rates, to use heterodyne detection with a noisy input state than homodyne detection with a pure input state, cf., Fig. 3(b).

IV. DIRECT RECONCILIATION

We now look at direct reconciliation [3] ($\blacktriangleright$), which is known to be better suited to short-range QKD with noisy channels [4], where Bob uses both homodyne and heterodyne detection. First, though, we begin with our analysis using homodyne detection, as first presented in [11].

A. Homodyne detection

The secret key rate for direct reconciliation using homodyne detection is given by

$$R^{\blacktriangleright[\mathrm{Hom}]} := I(X_A : X_B) - I(X_A : E), \tag{45}$$

where $I(X_A : X_B)$ has already been calculated in Eq. (17). (Note that the mutual information between Alice and Bob is symmetric with respect to the two reconciliation protocols). For Eve we have

$$I(X_A : E) := S(E) - S(E|X_A), \tag{46}$$

where $S(E|X_A)$ is calculated from the spectrum $\boldsymbol{\nu}_{E|X_A}$ of the conditional covariance matrix $\mathbf{V}_{E|X_A}$. Eve's conditional covariance matrix for homodyne detection using direct reconciliation is equal to

$$\mathbf{V}_{E|Q_A} = \mathbf{V}_E(V_0, V), \tag{47}$$

where $\mathbf{V}_E$ is defined in Eq. (21). The resulting symplectic spectrum calculated using Eq. (32) is again too complicated to be written here. However, in Fig. 4(a) we have plotted the resulting secret key rates for various values of V_0. Here we see the feature of direct reconciliation, as first noticed in [11], where adding preparation noise onto the initial states does not reduce the transmission range of the protocol (despite the fact that the secret key rate is reduced). More on this effect soon.

B. Heterodyne detection

In our final analysis of this section, we consider heterodyne detection using direct reconciliation. The secret key rate for direct reconciliation using homodyne detection is given by

$$R^{\blacktriangleright[\mathrm{Het}]} := I(X_A : X_B) - I(X_A : E), \tag{48}$$

where $I(X_A : X_B)$ is the same as Eq. (41). For Eve, her mutual information with Alice is defined as

$$I(X_A : E) := S(E) - S(E|Q_A, P_A), \tag{49}$$

where $S(E|Q_A, P_A)$ is calculated from the spectrum $\boldsymbol{\nu}_{E|Q_A,P_A}$ of the conditional covariance matrix $\mathbf{V}_{E|Q_A,P_A}$. This conditional covariance matrix is given by

$$\mathbf{V}_{E|Q_A,P_A} = \mathbf{V}_E(V_0, V_0), \tag{50}$$

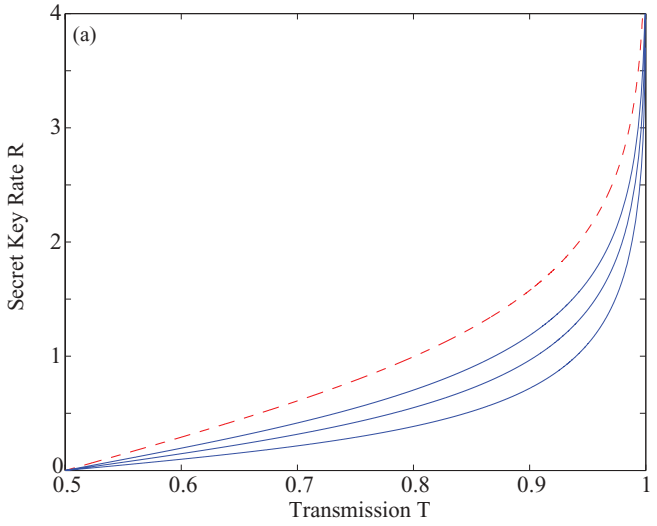
where again $\mathbf{V}_E$ is defined in Eq. (21). Using Eq. (24) we can write the symplectic spectrum as

$$\boldsymbol{\nu}^{\pm}_{E|Q_A,P_A} = \tfrac{1}{2}\left[\sqrt{(e_1+W)^2 - 4T(W^2-1)} \pm (e_1 - W)\right]. \tag{51}$$

The resulting secret key rates are plotted in Fig. 4(b) for different values of initial mode impurity. As with homodyne detection, when the impurity is increased, there is no reduction in the security threshold of the protocol, only the secret key rates. Note, however, that the security threshold for heterodyne detection ($T \approx 0.73$) is higher than that of homodyne detection ($T = 0.5$).

C. Improved performance using noise

We also notice that by adding more and more uncertainty to the initial modes, the security threshold slightly improves for heterodyne detection, meaning that the protocol can, at



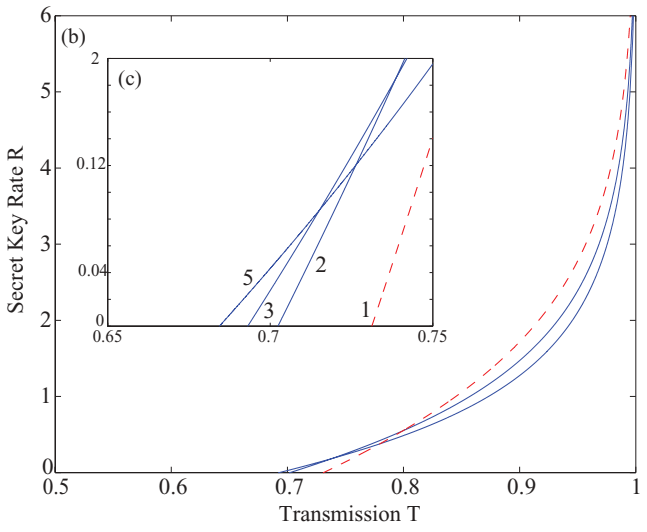


FIG. 4. (Color online) Secret key rates for direct reconciliation using (a) homodyne detection and (b) heterodyne detection. Here the dashed (red) line is the pure mode case $V_0 = 1$ where the solid (blue) lines are for impurity values $V_0 = 2,3,5$, from top to bottom, again using the parameters $W = 1$ and $V_S = 10^3$. (c) Close-up view of (b) showing that as Alice's input state becomes more and more thermal, even though the information rates are reduced, the protocol becomes more secure in terms of where the lines cross the transmission axis. The values of V_0 are indicated next to the respective lines.

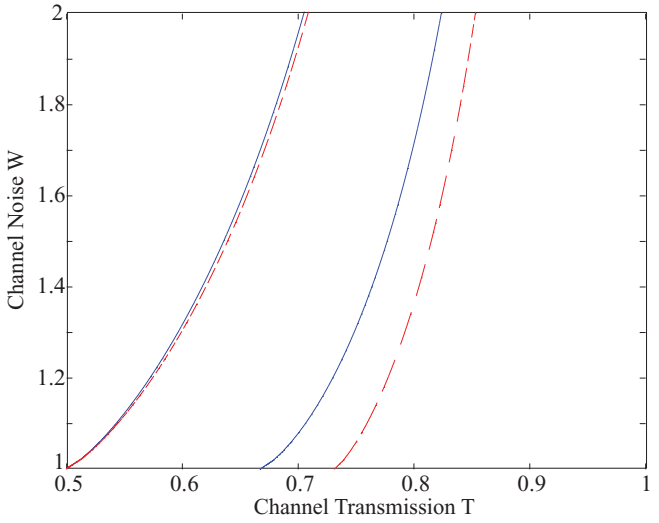


FIG. 5. (Color online) Security threshold plots for direct reconciliation where the (red) dashed lines indicate a pure vacuum mode at Alice's preparation side and the (blue) solid lines indicate a noisy coherent state ($V_0 \gg 1$) as input. The two lines converging to $T = 0.5$ are for homodyne detection while the other two lines indicate heterodyne detection. Adding preparation noise to the heterodyne detection protocol illustrates the largest improvement in security of the pair of two protocols.

least for a small window of channel transmissions, tolerate slightly higher levels of loss [cf., Fig. 4(c)]. For example, for a pure vacuum as input, a secure key can be generated from a transmission of $T >\approx 0.73$. However, when the initial mode is set to $V_0 = 5$ we have $T >\approx 0.68$. Numerically, we find that for large values of impurity ($V_0 \gg 1$), the security asymptotes to $T \to 0.67$. Out of the four families of protocols studied in this paper, this is the only protocol that exhibits such behavior. Figure 5 contains plots of the security thresholds (i.e., where $R = 0$) for both homodyne and heterodyne detection using direct reconciliation and shows the improvement in security when (unknown) preparation noise is added, with heterodyne detection offering the largest improvement. This situation of noise improving the performance of QKD was seen in discrete-variable protocols [12] and has also been seen in the context of direct reconciliation, where (pure) coherent states and homodyne detection are more robust than squeezed states and homodyne detection [29]. Furthermore, reverse reconciliation, where Bob measures squeezed states using heterodyne detection rather than homodyne detection, also shows an enhanced robustness [13,14]. Achieving such security robustness only works when additional noise is added to the reference point (either Alice or Bob) of the reconciliation protocol. This means Alice in direct reconciliation and Bob in reverse reconciliation.

A simple physical way of understanding this effect and why it sometimes helps in direct reconciliation but not in reverse reconciliation, and vice versa, can be understood by considering the following: the noise added on the side that is used to make the key is not very harmful (and may even be good sometimes) because it deteriorates both Eve's information and that of the authorized party trying to infer the key. The exact balance between these two effects is subtle, so that the difference (the secret key rate) may only be weakly affected. In contrast, adding noise on the other side (i.e., on the authorized party trying to infer the key) is only detrimental to Alice and Bob, while it does not affect Eve's information. In the present case, preparation noise at Alice's side obviously hurts in reverse reconciliation, since it only penalizes Alice and not Eve, while it does not hurt so much in direct reconciliation. As an explicit example, consider the results in [14]. Here it was explained that the improved performance of coherent-state versus squeezed-state protocols in direct reconciliation originates from the effect of adding noise at Alice's side (this effect is actually observable but not explained in [29]). This

is easy to understand in the entanglement-based picture of the protocol, where Alice's estimate of a quadrature via a heterodyne measurement can be seen as a noisy homodyne measurement of the same quadrature. In this sense, the coherent-state protocol is a noisy version of the squeezed-state protocol, hence its improved performance [14]. This same feature explains the comparison in Fig. 3 between homodyne and heterodyne detection in reverse reconciliation. Since Bob is having the key, heterodyning (viewed as noisy homodyning) at Bob's side does not hurt much and may even be beneficial, as it appears to be the case here.

Finally, as we did with the reverse reconciliation protocols, we compare homodyne detection to heterodyne detection but this time for direct reconciliation. This comparison is plotted in Fig. 6(a), where we have compared the two pure vacuum modes against $V_0 = 3$ for both homodyne and heterodyne detection. We have also plotted a comparison between direct and reverse reconciliation for both homodyne and heterodyne detection using impurity values of $V_0 = 3$ and 5. In the case of homodyne detection, as given in Fig. 6(b), we find that direct reconciliation offers stronger security and higher information rates than reverse reconciliation for the same values of impurity. This is somewhat mirrored in the heterodyne detection scenario given in Fig. 6(c), although it only becomes more apparent for values of impurity higher than $V_0 = 5$.

D. Effect of channel noise

Here we consider the effect of channel noise ($W > 1$) on the protocol that uses direct reconciliation with homodyne detection for larger values of preparation noise. In particular, we consider preparation noises with a variance up to 10^4. In Fig. 7 we plot the two cases of channel noises of $W = 1.01$ and $W = 3$ [Figs. 7(a) and 7(b), respectively]. As expected, both plots show a reduction in both the channel transmission and secret key rate for both channel noises. However, the characteristic where the various values of V_0 converge to the same channel transmission value still remains.

V. QKD IN THE CLASSICAL LIMIT

So far we have considered what happens to the four protocols (direct/reverse reconciliation using homodyne/heterodyne detection) when modest amounts (at most $V_0 = 5$) of preparation noise is added onto Alice's input states. In this section we consider the theoretically interesting "classical limit," where an infinite amount of preparation noise is added, i.e., $V_0 \to \infty$, and hence, the quantum vacuum mode contribution to QKD becomes (almost) negligible. Here we consider the case of direct reconciliation (using homodyne detection), because as we have seen, reverse reconciliation (using either homodyne or heterodyne detection) does not handle preparation noise very well as the security (channel transmission) and the secret key rate deteriorate quickly for modest increases in noise. It was shown in [11] that for a pure loss channel ($W = 1$), a secret key could still be established even if Alice's preparation noise was as large as $V_0 = 10^4$. Adding preparation noise from $V_0 = 1$ to $V_0 = 10^4$ reduced the key rate but kept the maximum transmission threshold fixed at $T = 0.5$.

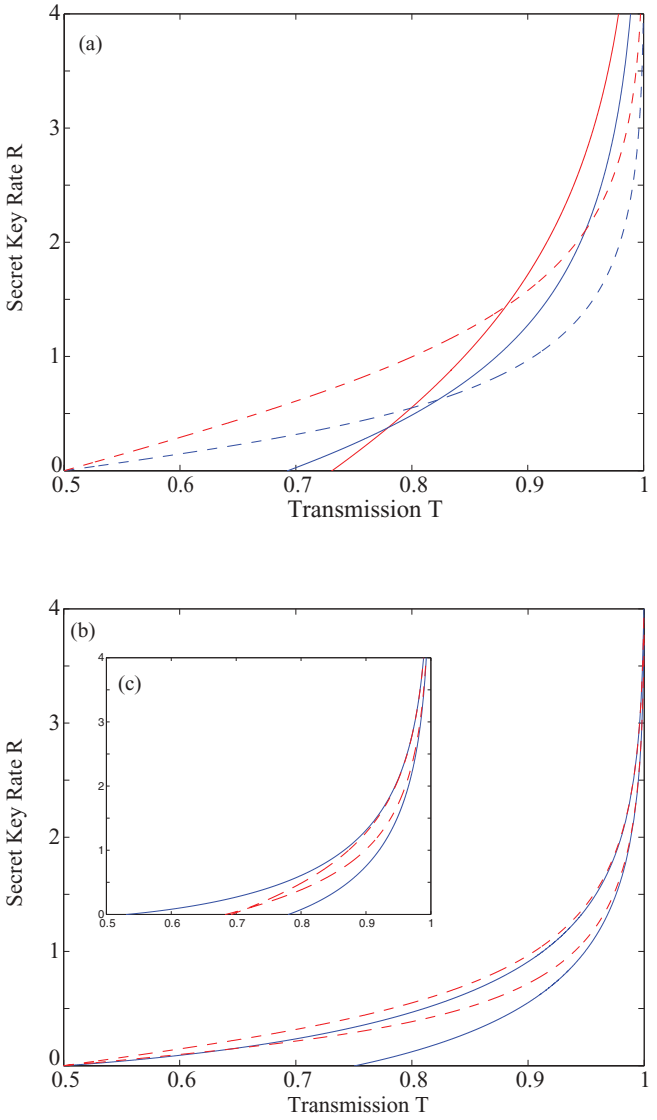


FIG. 6. (Color online) (a) Comparison of secret key rates between direct reconciliation using homodyne detection (dashed lines) and heterodyne detection (solid lines) for $V_0 = 1$ (red lines) and $V_0 = 3$ (blue lines) and with only loss on the quantum channel, i.e., $W = 1$, with $V_S = 10^3$. Comparison of direct and reverse reconciliation for (b) homodyne detection and (c) heterodyne detection for a lossy channel. Here the dashed (red) lines indicate direct reconciliation, while the solid (blue) lines indicate reverse reconciliation. In each of the cases we have plotted the impurity values of $V_0 = 3$ and 5.

We now consider what happens to the secret key rate $R^{\blacktriangleright[\mathrm{Hom}]}$ in the asymptotic limit where the preparation noise goes to infinity $V_0 \to \infty$ and the channel noise is much smaller, i.e., $W \ll V_0$. To do this we consider the fixed ratio

$$\phi := \frac{V_S}{V_0} > 0. \tag{52}$$

We note that keeping ϕ fixed results in keeping the signal-to-noise ratio constant while increasing both the signal V_S and the noise V_0. In our calculations we make the substitution $V_S = \phi V_0$ and take the limit $V_0 \to \infty$. We begin by first considering the mutual information between Alice and Bob as defined in

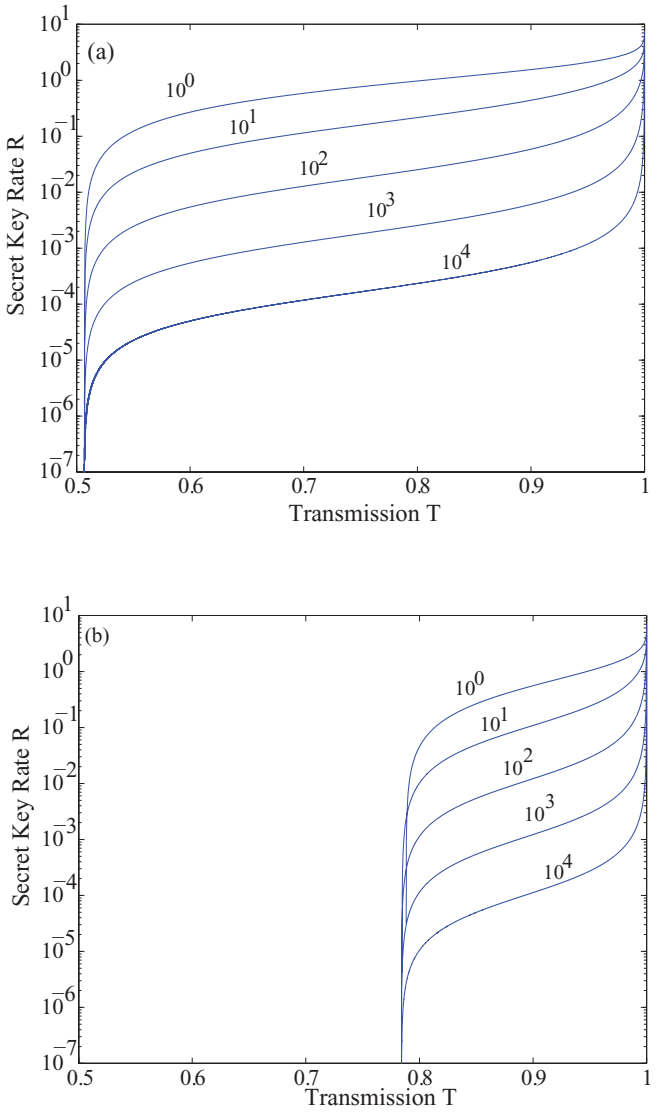


FIG. 7. (Color online) The effect of channel noise W on the secret key rates for direct reconciliation using homodyne detection for a quantum channel with noise of (a) $W = 1.01$ and (b) $W = 3$ for various values of V_0 where $V_S = 10^5$. The effect of increasing the channel noise only shifts the security threshold of both plots while maintaining the same characteristic of the lossy channel [11] where all values of V_0 converge to the same channel transmission. Such a preparation noise effect is not seen in reverse reconciliation.

Eq. (17). Following the recipe given above, we obtain

$$I(X_A : X_B) = \tfrac{1}{2}\log_2(1+\phi). \tag{53}$$

The above equation is simply Shannon's formula for the classical capacity of a single-mode communication channel with additive Gaussian noise of variance V_0 and input Gaussian signal V_S [23]. We now calculate the mutual information between Eve and Alice $I(X_A : E)$ in this so-called classical limit. To do this we follow the techniques given in Sec. IV A. Note that Eve and Alice's mutual information is defined in Eq. (46) and uses Eq. (11) with Eq. (12). However, in this asymptotic limit the symplectic eigenvalues are also very large, i.e., $\nu \gg 1$, in which case Eq. (12) is simplified to

$$g(\nu) \to g'(\nu) = \log_2\left(\frac{e\nu}{2}\right) + O(\nu^{-1}). \tag{54}$$

Again, in this asymptotic limit, the first symplectic spectrum value of Eve using Eq. (25) is given by

$$\nu_E^+ = (1-T)V, \tag{55}$$

while the other symplectic eigenvalue can be calculated in the same manner to give

$$\nu_E^- = W. \tag{56}$$

To calculate the conditional symplectic spectrum $\boldsymbol{\nu}_{E|X_A}$ we use Eq. (32), where

$$\begin{aligned}\Delta = {} & W^2 + (V - TV + TW)(V_0 - TV_0 + TW) \\ & - 2T(W^2 - 1)\end{aligned} \tag{57}$$

and

$$\begin{aligned}\left(\Delta^2 - 4\det\mathbf{V}_{E|X_A}\right) = {} & (T-1)^2[T^2(V-W)^2(V_0-W)^2 \\ & + (W^2 - VV_0)^2 + 2T(V-W) \\ & \times (W - V_0)(W^2 + VV_0 - 2)].\end{aligned} \tag{58}$$

Taking the limit as before gives, for the first symplectic eigenvalue, the following:

$$\nu_{E|X_A}^+ = \sqrt{1+\phi}(1-T)V_0 + O\left(V_0^{-1}\right). \tag{59}$$

Now in order to get a nonzero value for the other symplectic eigenvalue we use Eq. (33) to give

$$\begin{aligned}&\nu_{E|X_A}^- \\ &= (1-T)^{-1}\sqrt{\frac{(T + VW - TVW)(T + V_0W - TV_0W)}{VV_0}}.\end{aligned} \tag{60}$$

Using the above asymptotic formulas with Eq. (45), we find that a positive secret key rate exists only when

$$R^{\blacktriangleright[\mathrm{Hom}]} = \log_2\left[\frac{(\sqrt{1+\phi})\nu_{E|X_A}^+\nu_{E|X_A}^-}{\nu_E^+\nu_E^-}\right] > 0. \tag{61}$$

The above expression can be simplified to

$$\log_2\left[\frac{[T + VW(1-T)][T + V_0W(1-T)]}{VV_0W^2(1-T)^2}\right] > 0. \tag{62}$$

For a finite information rate we therefore require the following inequality to be true:

$$\frac{[T + VW(1-T)][T + V_0W(1-T)]}{VV_0W^2(1-T)^2} > 1. \tag{63}$$

Algebraically, we find that the above inequality is always satisfied for our required conditions of $1/2 < T < 1$, $V_0 > 1$, $V_S > 1$, and $W > 1$. Therefore we have shown that in the asymptotic limit where $V_0 \to \infty$, $V_S = \phi V_0$, and $W \ll V_0$, any value of preparation noise can be added onto the initial quantum states used by Alice and a secret key can still be achieved, albeit with a very small, but still finite, key rate. This happens as long as the transmission of the channel is greater than a half.

VI. QUANTUM CRYPTOGRAPHY AT VARIOUS ELECTROMAGNETIC WAVELENGTHS

It is interesting to consider that one possible application of the results from the previous two sections is continuous-variable QKD over different wavelengths of the electromagnetic spectrum. Such regimes would be interesting to explore due to various technologies using wavelengths other than optical. For example, Wi-Fi and Bluetooth technologies operate at the microwave frequency, and the security of such devices is extremely important, as well as the security of free space optical communication using infrared lasers. The reason why the previous analyses would be useful for such an application is that the average photon number is dependent on the wavelength of the signals sent. Typically, QKD experiments [1] are performed at telecom wavelengths of 1550 nm, where the average photon number at room temperature is very low ($\bar{n} \sim 10^{-14}$). However, when one moves away from this wavelength and down into the infrared, the modes become more thermal. In Sec. IV we determined that direct reconciliation is significantly more robust against preparation noise than reverse reconciliation and is therefore better suited to our analysis of QKD at various wavelengths.

We consider a simple model where Alice sends Bob thermal states at a particular wavelength and Bob uses a (perfect efficiency) homodyne detector that is unaffected by the thermal radiation. Note that if Bob employed heterodyne detection, the additional unit of shot noise vacuum from the heterodyne detector would also be thermal and would need to be taken into account. For Eve's attack, as with the previous sections, we assume she performs a collective Gaussian attack, but this time with a difference. Eve's ancilla modes, which she interacts with Alice's incoming modes (where the interaction is typically modeled using a Gaussian beam splitter), are also thermal (for the same reason Alice's are). In order to combat this Eve performs her entire attack inside a cryostat (see Fig. 8). In preparation for her attack, Eve's first step (1) is to cool her thermal ancilla modes so as to approximate pure vacuum modes. In the second step (2) she performs a collective Gaussian attack via the entangling cloner attack with variance W. The variance of this thermal state is chosen to be equal to the variance of the environmental noise, so that Eve essentially covers her tracks.

To begin the analysis we need to calculate the variance of a mode at a specific wavelength. To do this we note that we can write the average photon number $\bar{n}$ in terms of the quadrature variance V as

$$\bar{n} = \langle \hat{a}^\dagger \hat{a} \rangle = \tfrac{1}{2}(V-1) \Longrightarrow V = 2\bar{n} + 1, \tag{64}$$

where $\hat{a} = (\hat{Q} + i\hat{P})/2$ and $\hat{a}^\dagger$ are the annihilation and creations operators, respectively, and we have also symmetrized both quadratures, i.e., $V := V(\hat{Q}) = V(\hat{P})$. Now the average photon number for a single mode is equal to [30]

$$\bar{n} = \frac{1}{\exp(hf/k_B\tau) - 1}, \tag{65}$$

where τ is the temperature, f is the frequency of the mode, h is Planck's constant, and k_B is Boltzmann's constant. Using the techniques from Sec. IV A we can calculate the regions where continuous-variable QKD is secure as a function of the frequency (wavelength) and channel transmission. This is plotted in Fig. 9, where areas of security correspond to $R > 0$ where again R is the secret key rate. We see that regions of security exist over various wavelength values from optical (1550 nm) into the infrared and down into the microwave region. We note that in the original paper [11], where continuous-variable QKD at various frequencies was first investigated, a bound was derived that underestimated the security threshold. The new, tighter bound given in Fig. 9

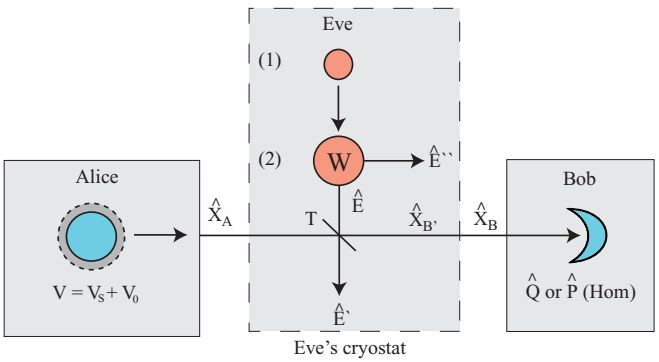


FIG. 8. (Color online) Schematic of a continuous-variable QKD protocol performed at different wavelengths of the electromagnetic spectrum. Alice sends modes at a particular fixed wavelength to Bob who measures the incoming modes using homodyne (Hom) detection. Eve's attack consists of using a cryostat which is used to cool her thermal modes to produce pure vacuum modes (1). The second step (2) involves implementing the entangling cloner attack with variance W. This variance is chosen to match the level of the variance of the radiation of the environment, effectively covering her tracks.

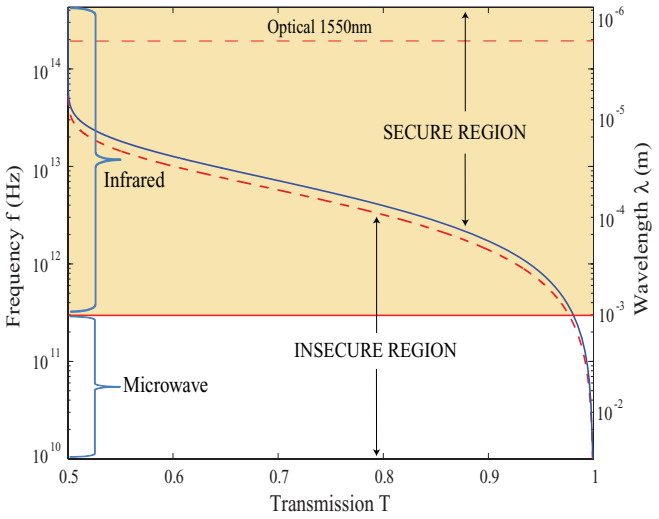


FIG. 9. (Color online) Security of continuous-variable QKD as a function of channel transmission T at various wavelengths of the electromagnetic spectrum at room temperature $\tau = 300$ K. Beginning at the infrared spectrum (430 THz) and down into the microwave spectrum (starting from 300 GHz) where $V_S = 10^8$. The solid (blue) line is the secure region derived against a collective Gaussian attack. The dotted (red) line corresponds to an entanglement-breaking channel, where Eve performs an intercept-resend attack. In such a situation no secure key can be synthesized.

improves upon the previous bound by having higher levels of security.

It is instructive to consider a loss limit (or transmission threshold) for QKD at various wavelengths. It is known [31] that a loss limit exists when considering channel noise for continuous-variable QKD. This bound corresponds to Eve performing an intercept-resend attack, which destroys any quantum correlations between Alice and Bob and thus the possibility of generating a secure key [32]. In order to avoid an entanglement-breaking channel, we demand that the equivalent noise of the quantum channel χ cannot exceed one unit of shot noise, i.e., $\chi < 1$ [3]. Since $\chi = W(1-T)/T$, the security condition becomes

$$W < \frac{T}{1-T}. \tag{66}$$

We can rewrite the above equation in terms of a secure bound on the required frequency as a function of channel transmission. Using the fact that $W = 2\bar{n} + 1$ with Eqs. (65) and (66), we can show that we require

$$f > -\alpha \ln(2T - 1), \tag{67}$$

where $\alpha = k_B \tau / h$. This curve is plotted as the dotted (red) line in Fig. 9 and gives a lower bound in security.

A. Discussion: Feasibility of microwave QKD

Here we consider the possibility of using QKD at the microwave frequency. The microwave frequency is ubiquitous as a communication wavelength in today's technologies, ranging from cell phones to short-range devices such as Wi-Fi and Bluetooth. The fact that small regions of security exist in the microwave regime is initially quite surprising due to the presence of large amounts of background noise. We consider the microwave frequency from 300 GHz (1 mm) to 1 GHz (30 cm). Using Eq. (65) for Alice's initial modes, we find that this corresponds to a range of variances from $V_0 = 41.66$ to $V_0 = 1.25 \times 10^4$, respectively. In Fig. 10 we plot the case where $V_0 = 41.66$ (i.e., 300 GHz) and where the noise on Eve's mode is also $W = 41.66$. We see that a secure key can only be generated when the transmission is higher than $T \approx 0.981$. Here the straight vertical line distinguishing the insecure and secure regions is the entanglement-breaking region as given by Eq. (66), i.e., $T > W/(1+W) = 0.9\,766$. For the 1-GHz frequency, numerically we only start getting positive key rates when the channel reflection (i.e., loss) is on the order of $1 - T \approx 10^{-5}$, giving a key rate on the order of $R \approx 10^{-6}$. Although the secure region is very small, the practical required distances are also very small. Such a short-range QKD scheme, unlike the typical long-range QKD protocols, could potentially be ideal for such devices as Bluetooth (maximum distance of ~10 m) and Wi-Fi (~75 m). Also, a secure quantum version of near-field communication (NFC) [33] would be an ideal application, as the range with which these microwave devices operate over is ~10 cm. However, in such a situation what actually constitutes Alice's and Bob's stations becomes blurred. We point out that the dominant factor in terms of the limited range in security is the channel noise W and, as we have seen from the results of the previous section, not the preparation noise. The effect of channel noise on the security

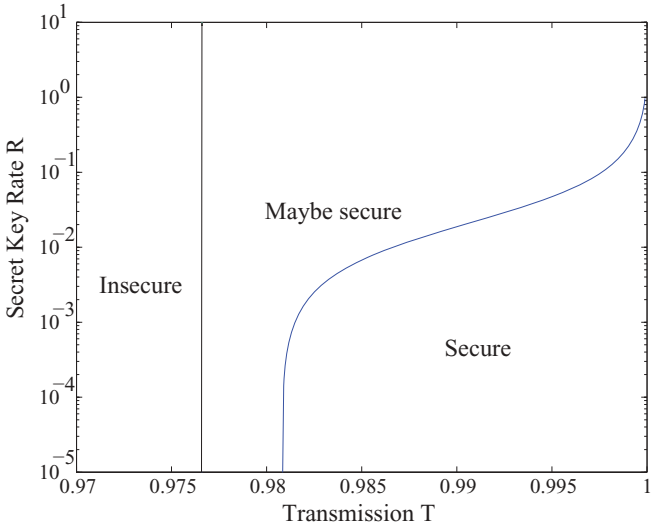


FIG. 10. (Color online) Security of microwave quantum cryptography. Here we consider the upper end of the microwave spectrum, i.e., $V_0 = 41.66$ (300 GHz), using the direct reconciliation protocol and homodyne detection, where $W = 41.66$ and $V_S = 10^8$. The insecure region corresponds to the entanglement-breaking channel where no secure key can be created, while a region between the secure and insecure region exists where it might be secure but as yet no known protocol exists. For example, secure protocols could be developed which are based on more complex strategies in terms of classical communications and postprocessing.

of thermal-state QKD is plotted in Fig. 11. Here we assume $V_0 = 41.66$ and see that after only a small increase in channel noise (i.e., $W = 5$) one can only generate a secure key after $T \approx 0.86$. Therefore a continuous-variable QKD protocol that is able to tolerate large amounts of preparation *and* channel noise is required in order to make microwave QKD feasible. Other important effects such as efficiency of the reconciliation

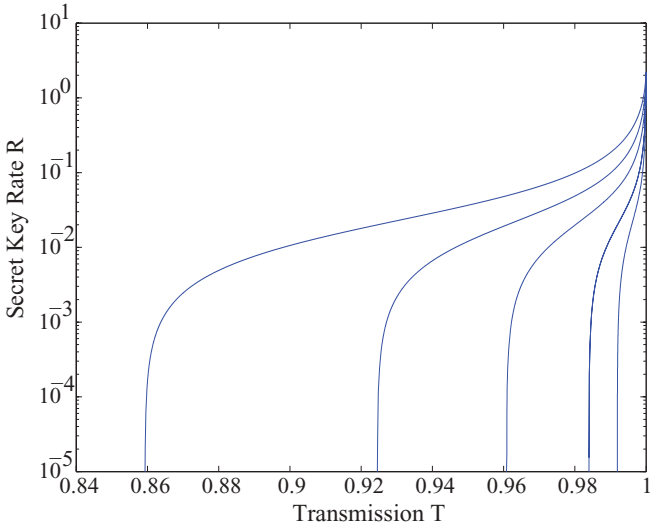


FIG. 11. (Color online) How channel noise W affects the security of thermal state QKD. Here we have $V_0 = 41.66$ using direct reconciliation and homodyne detection with $V_S = 10^3$. From left to right: $W = 5, 10, 20, 50$, and 100. After only modest increases in channel noise the security of the protocol reduces rapidly.

protocol and finite-size key effects need to be considered and will also reduce the secure region.

Another possible platform for microwave QKD is using discrete variables, e.g., the BB84 protocol [34]. The preparation and detection of photons at the microwave frequency is an active field of experimental research in cavity quantum electrodynamics [35–38]. However, such experiments do not involve the propagation of microwave photons over free space. Although, even if the technology allowed the efficient generation and detection of single microwave photons over free space, the fundamental problem exists where Bob would not be able to distinguish the photons that originated from Alice to those which came from the surrounding environment—both are indistinguishable.

VII. CONCLUSION

In conclusion, we have considered continuous-variable quantum key distribution from the perspective of Alice using thermal Gaussian states as her initial cryptographic resource, instead of the usual pure Gaussian states. The case of direct reconciliation and homodyne detection was analyzed in [11], and we have extended those results here to include both direct and reverse reconciliation for the case of heterodyne detection. We showed that an improved robustness to channel noise can be achieved when preparation noise is added in the case of direct reconciliation using heterodyne detection. In [11] it was shown that direct reconciliation does not suffer any loss in security when preparation noise is added (although the secret key rate does decrease as a function of preparation noise), even when the variance of the initial thermal states was as large as 10^4 times that of the pure vacuum. We significantly improved upon this result by showing that direct reconciliation can tolerate any amount of preparation noise, provided the channel noise is much less than the preparation noise. Finally, we derived an upper bound related to an entanglement-breaking eavesdropping attack for quantum key distribution at various electromagnetic wavelengths and ended with a discussion on the feasibility of microwave quantum key distribution.

ACKNOWLEDGMENTS

C.W. would like to thank Bing Qi, Hoi-Kwong Lo, Li Qian, Travis Humble, and Nathan Walk for discussions and acknowledges the helpful comments and suggestions made by the referees. C.W. acknowledges support from the Ontario postdoctoral fellowship program, the CQIQC postdoctoral fellowship program, CIFAR, Canada Research Chair program, NSERC, and QuantumWorks. S.P. acknowledges support from EPSRC under Grant No. EP/J00796X/1 (HIPERCOM) and the European Union under Grant Agreement No. MOIF-CT-2006-039703. T.C.R. acknowledges support from the Australian Research Council.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[3] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[4] F. Grosshans, G. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[5] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[6] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nat. Phys. **4**, 726 (2008).
[7] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[8] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
[9] R. Filip, Phys. Rev. A **77**, 022310 (2008).
[10] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).
[11] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).
[12] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[13] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).
[14] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).
[15] J.-P. Poizat, J. F. Roch, and P. Grangier, Ann. Phys. (Paris) **19**, 265 (1994).
[16] P. Grangier, J. A. Levenson, and J.-P. Poizat, Nature (London) **396**, 537 (1998).
[17] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[18] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[19] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).
[20] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[21] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and Ph. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[22] P. Kok and B. Lovett, *Introduction to Optical Quantum Information Processing* (Cambridge University Press, Cambridge, 2010).
[23] C. E. Shannon, Bell Syst. Tech. J. **27**, 623 (1948).
[24] A. S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).
[25] A. S. Holevo, M. Sohma, and O. Hirota, Phys. Rev. A **59**, 1820 (1999).
[26] J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. **89**, 137903 (2002).
[27] J. Fiurášek, Phys. Rev. Lett. **89**, 137904 (2002).
[28] A. Serafini, F. Illuminati, and S. De Siena, J. Phys. B **37**, L21 (2004); G. Adesso, A. Serafini, and F. Illuminati, Phys. Rev. A **70**, 022318 (2004).
[29] M. Navascués and A. Acín, Phys. Rev. Lett. **94**, 020505 (2005).
[30] C. C. Gerry and P. L. Knight, *Introductory Quantum Optics* (Cambridge University Press, Cambridge, England, 2005).
[31] R. Namiki and T. Hirano, Phys. Rev. Lett. **92**, 117901 (2004).

[32] M. Curty, M. Lewenstein, and N. Lütkenhaus, Phys. Rev. Lett. **92**, 217903 (2004).
[33] [www.nfc-forum.org/home].
[34] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Proceedings (Bangalore)* (IEEE, New York, 1984), pp. 175–179.
[35] A. A. Houck *et al*., Nature (London) **449**, 328 (2007).
[36] B. T. H. Varcoe, S. Brattke, M. Weidinger, and H. Walther, Nature (London) **403**, 743 (2000).
[37] J. M. Raimond, M. Brune, and S. Haroche, Rev. Mod. Phys. **73**, 565 (2001).
[38] D. I. Schuster *et al*., Nature (London) **445**, 515 (2007).