Article:
Papanastasiou, Panagiotis, Ottaviani, Carlo orcid.org/0000-0002-0032-3999 and Pirandola, Stefano orcid.org/0000-0001-6165-5615 (2018) Gaussian one-way thermal quantum cryptography with finite-size effects. Physical Review A. 032314. pp. 1-9. ISSN 1094-1622

https://doi.org/10.1103/PhysRevA.98.032314

Gaussian one-way thermal quantum cryptography with finite-size effects

Panagiotis Papanastasiou, Carlo Ottaviani, and Stefano Pirandola
Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, United Kingdom

We study the impact of finite-size effects on the security of thermal one-way quantum cryptography. Our approach considers coherent/squeezed states at the preparation stage, on the top of which the sender adds trusted thermal noise. We compute the key rate incorporating finite-size effects, and we obtain the security threshold at different frequencies. As expected finite-size effects deteriorate the performance of thermal quantum cryptography. Our analysis is useful to quantify the impact of this degradation on relevant parameters like tolerable attenuation, transmission frequencies at which one can achieve security.

I. INTRODUCTION

Quantum key distribution (QKD) [1, 2] lets two authorized users (Alice and Bob) to establish unconditionally secure communication over an insecure quantum channel controlled by an eavesdropper (Eve). After having shared a secret key, the users can employ it in a one-time pad protocol. To implement the key distribution, the sender (Alice) sends non-orthogonal quantum states to the receiver (Bob) through the communication channel. In this way, the parties can detect Eve's intrusions to gain information. The absolute privacy of the communication is established post-processing the raw key by classical protocols of error correction and privacy amplification, which reduce Eve's information on the final key to a negligible amount.

Protocols using continuous variable (CV) systems [3, 4] have been proposed for point-to-point one-way communication, exploiting squeezed states [5, 6], finite alphabets [7–10], Gaussian [11] and non Gaussian post-selection [12]. Schemes based on Gaussian modulations of coherent states have been investigated in great detail [13–19], and we have now also experimental implementations over long distances [20–22]. Besides one-way protocols, it has been proposed to exploit two-way communication [23–25], quantum illumination [26], floodlight QKD [27–30], and measurement-device-independence (MDI) [31, 32], the latter very promising to establish end-to-end communications [33, 34]. In particular CV-MDI protocols are very promising for future implementation of high-rate metropolitan networks, or for multi-users quantum conferencing [35].

Thermal QKD has been investigated in both one-way [36, 37] and two-way [38] configuration, with the goal of exploring the possibility of implementing QKD at frequencies alternative to the optical one. Initially, the use of thermal states in the optical regime was proposed to describe imperfections in the preparation of coherent states due to the use of cheap thermal sources [40, 41]. In thermal protocols, the coherent-state based encoding is replaced by the Gaussian modulation of thermal states, prepared by adding trusted noise on top of coherent states. The analysis of the performance at various frequencies is carried out by expressing the trusted noise in terms of the thermal photon number of the background radiation.

The increasing attention received by CV-QKD in recent years is justified by the relative simplicity of the experimental setup, and the very high key-rate achievable, which can be close to the secret-key capacity of an optical communication channel, also known as PLOB bound [39, 42, 43]. Moreover, the possibility of implementing communications exploiting all the electromagnetic spectrum represents an additional appealing feature of CV systems. The progress achieved in recent years on the security proofs of Gaussian CV-QKD, has led to establish composable security proofs for coherent-state one-way protocols [44, 45] and MDI schemes [46]. An important scenario to consider, when we study the security of CV-QKD in practical conditions, is to quantify the security performances of a protocol when finite-size effects are incorporated in the analysis. The study of finite-size effects is a precursory step in the security analysis of both one-way [47] and MDI schemes [48].

Up to now, thermal protocols have been studied only considering ideal asymptotic conditions, where the parties exchange infinitely many signals over the quantum channel. This is a powerful assumption that simplifies the mathematical complexity of the security analysis: One can work within the Devetak-Winter security criterion [49] and use the Holevo quantity [50] to bound Eve's accessible information. The study of security under more practical conditions requires to assume that Alice and Bob can only make a finite use of the communication channel. This introduces finite-size effects that deteriorate the performance, reducing the tolerable excess of noise, lowering the key rate and shortening the achievable distances.

In this work, we study the impact of finite-size effects on the security of thermal one-way protocol, adapting the approach described in Ref. [51] for coherent state CV QKD. This allows us to quantify the performance of thermal QKD under more realistic assumptions than in previous studies. We focus on one-way schemes used in direct reconciliation (DR) because this represents the configuration providing the best performance for Gaussian-modulated thermal-state quantum cryptography. The performances are then limited, by construction, to 3 dB

of channel attenuation.

We systematically analyze the impact of finite-size effects on the performance of thermal one-way quantum cryptography in various decoding configurations (homodyne and heterodyne detections), which may be employed in short to mid-range communication, if one assumes to use optical fibers. Our analysis also shows that the parameter estimation procedure is negatively affected by the use of trusted thermal noise, which can further degrade the achievable distances. We also show that using thermal states, generated starting from moderately squeezed ones within state-of-the-art experimental equipment (e.g., 10 dB of squeezing), can provide an incremental improvement of the achievable distance which saturates for higher squeezing factors. Finally, we study the impact of the finite-size effects on the threshold of a protocol operating in the microwave regime.

The structure of the paper is the following. Section II describes the protocol, including the optimal attack. In Section III, we focus on the case where Bob's decoding is performed by randomly switching the homodyne detection between the two possible quadratures (switching protocol). The discussion of other cases (no-switching protocol and encoding based on squeezed-thermal states, rather than coherent-thermal ones) is given in the Appendices. In Section IV, we describe the steps to compute the secret key rate incorporating finite-size effects. In Section V, we give the results of our analysis, and discuss the performance of the switching protocol in terms of the achievable distance in the optical regime, and the security threshold at various frequencies. Finally, Section VI is left to our conclusions.

II. PROTOCOL AND EAVESDROPPING

We now describe the one-way thermal QKD protocol in the prepare and measure (PM) representation. Additional details on thermal QKD can be found in Ref. [36–38, 40, 52] and in the recent review of Ref. [41]. The general bosonic mode of the electromagnetic field can be described in terms of its quadratures, Q and P, defined as $Q := a^\dagger + a$ and $P := i\left(a^\dagger - a\right)$. We remark that we assume unit vacuum shot-noise units (SNU) and, from quadratures Q and P we define the vectorial operator

$$X := (Q, P)^T.$$

The one-way communication goes as follows (see Fig. 1): Alice prepares thermal states and modulates them by applying random displacement in the phase space, according to a bivariate Gaussian distribution. We notice that the sender can prepare thermal states starting from coherent or squeezed states. We then have that Alice's input mode, A, can be described by the following input quadrature X_A

$$X_A = X_s + X_{\rm th} + X_M, \tag{1}$$

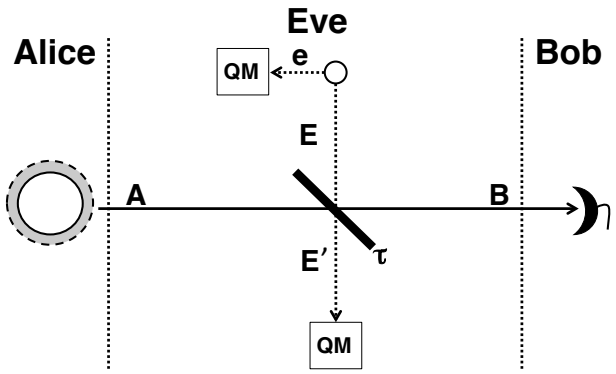

FIG. 1: The initial mode A is in a thermal state with variance $V_{\rm th} + V_s$ and modulate dwith variance V_M. After mode A is sent through the channel, Bob receives mode B and applies a homodyne detection on either q- or p-quadrature or a heterodyne detection measuring q and p-quadrature at the same time. The thermal-loss channel is modelled by a beam splitter with transmissivity τ. The Gaussian eavesdropping takes the form of an entangling cloner attack, where Eve's system is described by the modes e and E in an TMSV state with variance ω. According to this description, an optical fiber is simulated with transmissivity $\tau = 10^{-\frac{0.2d}{10}}$, where d (in km) is the length of the fiber, and excess noise variance $V_\varepsilon = \tau\varepsilon$, where $\varepsilon = \frac{(1-\tau)(\omega-1)}{\tau}$.

where X_s describes the quantum fluctuations of the initial coherent or squeezed state from which the sender starts, $X_{\rm th}$ is the contribution from trusted thermal noise, while X_M describes the Gaussian encoding. It is easy to see that the resulting input variance, describing the input mode, is given by the following simple relation

$$V_A = V_s + V_{\rm th} + V_M, \tag{2}$$

where $V_M > 0$ and $V_{\rm th} > 0$, and $V_s = 1$ if the sender starts from coherent states. In the next stage of the protocol, mode A is affected by a thermal-loss channel. The output mode B is then measured by Bob who can perform homodyne (switching protocol) or heterodyne detections (no-switching).

The optimal eavesdropping of CV one-way protocols after de Finetti reduction [45, 53] of general attacks, is a single-mode Gaussian collective attack [54–56], completely characterized in [57]. Thermal-loss channels, like free-space and optical fiber communications, can be dilated into entangling cloners, consisting of a beam splitter with transmissivity τ, placed between the parties. This device receives the incoming signal-mode A and Eve's ancillary mode E (see Fig. 1). Eve's modes E and e are in a two-mode squeezed vacuum state (TMSV) ρ_{eE} which is a zero-mean Gaussian state [3] described by the covariance matrix (CM)

$$\mathbf{V}_{eE} = \begin{pmatrix} \omega\mathbf{I} & \sqrt{\omega^2-1}\mathbf{Z} \\ \sqrt{\omega^2-1}\mathbf{Z} & \omega\mathbf{I} \end{pmatrix}, \tag{3}$$

with variance parameter $\omega \geq 1$. The output modes E' and e are then stored in a quantum memory that is op-

timally measured by the eavesdropper after the parties have concluded the communication stage.

In order to quantify Alice-Bob mutual information and Eve's accessible information, one needs to compute Bob's output mode B (see Fig. 1) which is described by the following vectorial operator

$$X_B = (Q_B, P_B)^T = \sqrt{\tau}(X_M + X_{\rm th}) + X_\varepsilon, \qquad (4)$$

where the term X_ε describes the excess of noise on the channel, conventionally defined as $\varepsilon := (1-\tau)(\omega-1)/\tau$ [13]. It is easy to check that the variance of X_B can be written as

$$V_B = \tau V_M + V_N, \qquad (5)$$

with variances $V_M \geq 0$, $V_{\rm th} \geq 0$, $V_s \leq 1$, where all noise contributions are grouped in the term

$$V_N = 1 + V_\varepsilon + \tau V_{\rm th}, \qquad (6)$$

and where we have defined the variances of the excess noise as $V_\varepsilon := \tau\varepsilon$ [51].

III. SWITCHING PROTOCOL WITH THERMAL STATES FROM MODULATED COHERENT STATES

We now consider a specific implementation: Alice starts preparing Gaussian-modulated coherent states, adds trusted thermal noise, and sends the resulting signals to Bob who, at random, switches his detection setup between homodyne measurements on Q or P (switching protocol). We discuss here only the direct reconciliation (DR), i.e., Bob infers Alice's encoded state from the outcomes of his detections.

With Alice starting from coherent states, one has the shot-noise variance $V_s = 1$, so that $V = V_{\rm th}$. In such a case, Eq. (6) reduces to the simpler expression

$$V_N^c = 1 + V_\varepsilon + \tau V_{\rm th}. \qquad (7)$$

We notice that, despite DR can only tolerate a maximum of 3 dB of channel's attenuation, in case of thermal one-way QKD, it does much better than the RR, which has been showed to tolerate only a small amount of thermal noise [38].

A. Mutual information

From the variances of Eq. (5) and Eq. (7), we compute Alice-Bob mutual information

$$I_{AB} := H_B - H_{B|\alpha}, \qquad (8)$$

with H_B ($H_{B|\alpha}$) being Bob's total (conditional) Shannon entropy [58]. In particular, we may write

$$I_{AB} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|\alpha}}, \qquad (9)$$

where V_B is the variance of Bob's output signal while $V_{B|\alpha} = V_N^c$ is Bob's variance conditioned to Alice's preparation. Therefore, using Eq. (5) and Eq. (7) we obtain the following general expression for Alice's Bob mutual information

$$I_{AB} = \frac{1}{2}\log_2\left(1 + \frac{\tau V_M}{1 + V_\varepsilon + \tau V_{\rm th}}\right). \qquad (10)$$

B. Key rate

Under ideal conditions of infinite number of channel uses, we can write the Devetak-Winter rate [49]

$$R := I_{AB} - I_E, \qquad (11)$$

where Eve's accessible information, I_E, is computed with the Holevo function [50]. In DR the quantity I_E is given by

$$I_E = S_{eE'} - S_{eE'|\alpha}, \qquad (12)$$

where $S_{eE'}$ and $S_{eE'|\alpha}$ describe the total and conditional von Neumann entropies of the output states $\rho_{eE'}$ and $\rho_{eE'|\alpha}$. For Gaussian states, the von Neumann entropies are completely determined by their CMs $\mathbf{V}_{eE'}$ and $\mathbf{V}_{eE'|\alpha}$ taking the following simple form [3]

$$S = \sum_i h(\nu_i), \qquad (13)$$

where the entropic function $h(.)$ is defined as

$$h(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}, \qquad (14)$$

and ν_i are the corresponding symplectic eigenvalues [3].

Moving from ideal conditions to realistic scenarios, the parties extract a usable key from a finite number of uses of the quantum channel. This generally deteriorates the performances because the efficiency of the classical protocols of error correction and privacy amplification is reduced, as well as the accuracy of the channel parameter estimation. A first adjustment to the key-rate of Eq. (11) incorporates the efficiency of classical protocols, and is given by the following key rate

$$R_\xi = \xi I_{AB} - I_E, \qquad (15)$$

with efficiency $\xi \leq 1$. We remark that the design of efficient classical error correction codes, such that $\xi \simeq 1$ is non-trivial, but recent progress [59, 60] showed that efficiencies as large as $\xi \simeq 0.98$, or more, are achievable today. For this reason this imperfection should not be considered as a major bottleneck for the development of CV quantum cryptography.

IV. FINITE-SIZE DESCRIPTION

The key rate R_ξ of Eq. (15) clearly fails to intercept all finite-size effects which play a role in quantifying the parameters of the attack which, accordingly to the discussion in Sec. II, is quantified by excess of noise V_ε and transmissivity τ. In this section, we quantify the impact of finite-size effects by adapting the approach described in Ref. [51], which is fairly simple to generalize to the thermal case. We can define two statistical variables M_i and B_i, for $i = 1, \ldots, m$, representing the realizations of the input X_M and of the output mode X_B of Eq. (4). The definition of the estimator of covariance $\hat{\sigma}_{MB}$, between modes X_M and X_B, is then easy to define as follows

$$\hat{\sigma}_{MB} = \frac{1}{m}\sum_{i=1}^{m} M_i B_i. \tag{16}$$

From Eq. (16) we can compute both expectation value and variance. Assuming M_i and B_i as independent and normally distributed Gaussian variables, we get the expectation value

$$\mathbb{E}\left[\hat{\sigma}_{MB}\right] = \sqrt{\tau} V_M = \sigma_{MB}, \tag{17}$$

and the variance

$$V_{\hat{\sigma}_{MB}} = \frac{\tau V_M^2}{m}\left(2 + \frac{V_N}{\tau V_M}\right). \tag{18}$$

Similarly, we can obtain expectation value and variance of the estimator, $\hat{\tau}$, of the transmissivity τ. From Eq. (17), one then writes

$$\hat{\tau} = \frac{\hat{\sigma}_{MB}^2}{V_M^2} = \frac{V_{\hat{\sigma}_{MB}}}{V_M^2}\left(\frac{\hat{\sigma}_{MB}}{\sqrt{V_{\hat{\sigma}_{MB}}}}\right)^2, \tag{19}$$

where $\left(\frac{\hat{\sigma}_{MB}}{\sqrt{V_{\hat{\sigma}_{MB}}}}\right)^2$ is chi-squared distributed.

From Eq. (19), we can compute the following expectation value

$$\mathbb{E}\left[\hat{\tau}\right] = \frac{V_{\hat{\sigma}_{MB}}}{V_M^2}\mathbb{E}\left[\left(\frac{\hat{\sigma}_{MB}}{\sqrt{V_{\hat{\sigma}_{MB}}}}\right)^2\right] = \tau + \mathcal{O}(1/m), \tag{20}$$

having confidence interval quantified by variance

$$\sigma_{\hat{\tau}}^2 = \frac{4\tau^2}{m}\left(2 + \frac{V_N}{\tau V_M}\right) + \mathcal{O}(1/m^2). \tag{21}$$

The same steps can be made to obtain the variance V_N starting from the statistical sampling B_i and M_i. Using Eq. (5) we can write the estimator $\hat{V}_N$ as follows

$$\hat{V}_N = \frac{1}{m}\sum_{i=1}^{m}\left(B_i - \sqrt{\hat{\tau}} M_i\right)^2. \tag{22}$$

It is clear from Eq. (20) and Eq. (21) that the standard deviation $\sigma_{\hat{\tau}}$ becomes rapidly negligible as $m \gg 1$. One can then safely replace the estimator $\hat{\tau}$ with its actual value τ in Eq. (22). Then, noticing that variable $B_i - \sqrt{\tau} M_i$ is normally distributed with variance V_N, we have that $\sum_{i=1}^{m}\left(\frac{B_i - \sqrt{\tau} M_i}{\sqrt{V_N}}\right)^2$ is also χ^2-distributed with expectation values m and variance $2m$. We then can write

$$\hat{V}_N = \frac{V_N}{m}\sum_{i=1}^{m}\left(\frac{B_i - \sqrt{\tau} M_i}{\sqrt{V_N}}\right)^2.$$

The estimator for the variance V_ε, can now be expressed using $\hat{V}_N$ and $\hat{\tau}$. It is easy to check that one obtains the following formula

$$\hat{V}_\varepsilon = \hat{V}_N - \hat{\tau} V - 1,$$

with expectation value

$$\mathbb{E}(\hat{V}_\varepsilon) = V_N - \tau V - 1, \tag{23}$$

and variance

$$\sigma_{\hat{V}_\varepsilon}^2 = \frac{2V_N^2}{m} + V^2 \sigma_{\hat{\tau}}^2. \tag{24}$$

We remark that these equations are formally identical to the case described in Ref. [51]. The only but crucial difference, in our case, is the presence of the contribution from thermal noise V_{th}, which appears in V.

Assuming an error probability for the parameter estimation of the order of $\varepsilon_{PE} = 10^{-10}$, we can associate confidence intervals of 6.5-sigmas which allow us to write the values of transmissivity and excess noise as

$$\tau^{\text{low}} := \hat{\tau} - 6.5\sigma_{\hat{\tau}}(\hat{\tau}, \hat{V}_\varepsilon),\ V_\varepsilon^{\text{up}} := \hat{V}_\varepsilon + 6.5\sigma_{\hat{V}_\varepsilon}(\hat{\tau}, \hat{V}_\varepsilon). \tag{25}$$

The quantities in Eq. (25) are then used to compute the finite-size key rate, which is given by the following expression

$$K = \frac{n}{\bar{N}}\left[R_\xi(\xi, V_s, V_M, V_{\text{th}}, V_\varepsilon^{\text{up}}, \tau^{\text{low}}) - \Delta\right], \tag{26}$$

where $\bar{N} = n + m$, is the total number of signals points, n is the number of signals used to build the key, and the correction term Δ accounts for the penalty for using the Holevo bound in the key rate of Eq. (26) using a finite number of signals. (Its description can be found in [47, 51]).

V. PERFORMANCES AND DISCUSSION

In this section, we discuss the performance of finite-size thermal one-way QKD DR. The results are obtained numerically, evaluating the key rate of Eq. (26), and quantifying relevant quantities like achievable distance, block-size dimensions needed to obtain a positive key or to recover the asymptotic key rate, and the finite-size performances of thermal QKD at different frequencies.

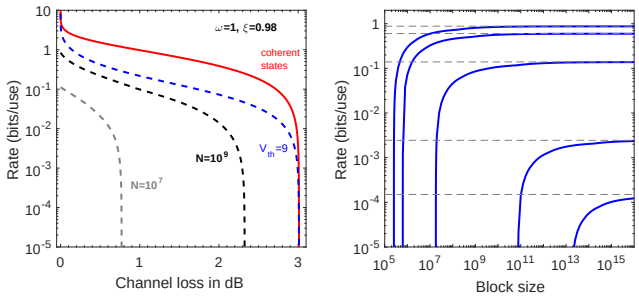

FIG. 2: (Color online) This figure focuses on the key-rate in the optical regime. The left panel describes the key rate versus channel attenuation given in dB. The red solid curve describes the ideal key-rate, using just coherent states. The blue-dashed curve describes the ideal key rate assuming a preparation noise with variance $V_{\rm th} = 9$ SNU. Then, we keep the same $V_{\rm th}$ and plot the finite-size rate for block size with $\bar{N} = 10^9$ (black dashed line) and $\bar{N} = 10^7$ (gray dashed) with $\xi = 0.98$ and $\omega = 1$. The key rate is optimized over the Gaussian modulation V_M. The right panel presents the key rate as a function of the block size ($\bar{N}$). We fix channel attenuation to 1 dB, and we assume pure loss attack $\omega = 1$ while $\xi = 0.98$. The plot shows the convergence of the key rates toward the asymptotic values (dashed curves) for different values of the preparation noise $V_{\rm th} = 0,\ 1,\ 10,\ 100,\ 150$ SNU, from top to bottom.

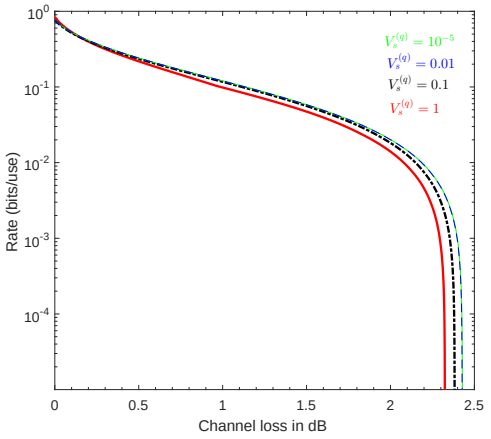

FIG. 3: (Color online) We consider the case for signal points block-size of $\bar{N} = 10^9$, reconciliation efficiency $\beta = 98\%$, trusted thermal noise of $V_{\rm th} = 9$ SNU and pure loss attack $\omega = 1$. We compare the finite-size key rate obtained when Alice starts from coherent states ($V_s^{(q)} = V_s^{(p)} = 1$) with the case when $V_s^{(q)} = 10^{-1}$, i.e., Alice's encoding is performed by adding thermal noise on moderate squeezed states. We notice that in such a case the achievable distance is only incrementally improved. Moreover the performance of the protocol saturates for stronger initial squeezing, i.e. for $V_s^{(q)} = 10^{-2}$ (blue-dashed), 10^{-5} (green line).

A. Secret key rate for different block sizes in the optical regime

Here we focus on the size of the signal blocks needed in order to achieve a positive key rate in the presence of increasing thermal noise. We use the average values $\langle \hat{\tau} \rangle \simeq \tau$ and $\langle \hat{V}_\varepsilon \rangle = V_\varepsilon$ for which one can write $V_\varepsilon = \tau\varepsilon$, with $\varepsilon = [(1-\tau)\omega - (1-\tau)]/\tau$. The parameter ω represents the variance of thermal noise of Eve's ancillary states used in the attack. We write the transmissivity τ in terms of dB of attenuation defining $\tau = 10^{-\frac{dB}{10}}$ and we express the key rate as follows

$$K = (1-r)\left[R_\xi(\xi, V_s, V_M, V_{\rm th}, \omega, dB, r, \bar{N}) - \Delta\right], \quad (27)$$

where $r := m/\bar{N}$. From Eq. (27) we can plot the key rate as a function of the channel attenuation, fixing the values of $V_{\rm th}$, efficiency ξ, thermal noise ω, and shot-noise variance V_s. Then we can optimize over the remaining parameters. The results for pure-loss attacks are shown in Fig. 2. In the left panel we plot the key rate for different values of the block-size and preparation noise. In particular, the red solid line describes the asymptotic key rate when Alice send coherent states, i.e., $V_{\rm th} = 0$, while the blue-dashed line is for $V_{\rm th} = 9$ SNU. Then, we compare the previous curves with the key rate of Eq. (27) for $\bar{N} = 10^9$ (black dashed line) and $\bar{N} = 10^7$ (gray dashed line).

In Fig. 2 (right panel), we quantify the block-size needed to achieve a positive key rate for increasing values of the preparation noise. We fix the attenuation to 1 dB and assume pure loss attack ($\omega = 1$ SNU). We then plot the key-rate as a function of the block-size, for preparation noise $V_{\rm th} = 0,\ 1,\ 10,\ 100,\ 150$ SNU from top to bottom and efficiency $\xi = 0.98$ [59]. Our results show that, by an increase in $V_{\rm th}$, the block-size need to be increased in order to match the asymptotic value of the key rate (dashed lines).

Finally Fig. 3 compares the key rate of the switching protocol when Alice start from coherent states (red solid line) with the case where she start from squeezed states. To distinguish between these two cases Eq. (6) splits as follows

$$V_N^{(q)} = 1 + V_\varepsilon + \tau\left(V_{th} + V_s^{(q)} - 1\right), \quad (28)$$

$$V_N^{(p)} = 1 + V_\varepsilon + \tau\left(V_{th} + V_s^{(p)} - 1\right), \quad (29)$$

where $V_s^{(p)} = 1/V_s^{(q)}$. For coherent states $V_s^{(q)} = V_s^{(p)} = 1$ and we recover Eq. (6). This case is described by the red line in Fig. 3, while the others lines describe the cases $V_s^{(q)} = 10^{-1}$ SNU (black dot-dashed), $V_s^{(q)} = 10^{-2}$ (blue-dashed) and $V_s^{(q)} = 10^{-5}$ (green). We see that using squeezed states can only incrementally increase the achievable distances, which saturates as the degree of squeezing increases.

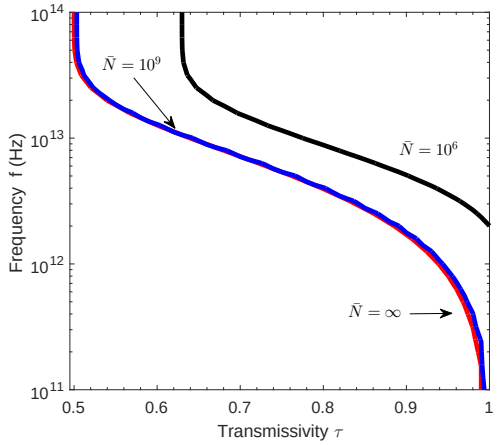

FIG. 4: (Color online) The red line shows the security threshold (frequencies vs channel's transmissivity) for a shot-noise level attack $\omega = V_{th} + 1$ without finite-size effects, and assuming infinite Gaussian modulation. Then we have the case for block size with $\bar{N} = 10^6$ signal points (black) and $\bar{N} = 10^9$ (blue).

B. Security thresholds with finite-size effects at different frequencies

In order to study the performance of the protocol at different frequencies, we follow the approach used in [36, 38]. We rewrite the preparation noise variance $V_{\rm th} \geq 0$, as

$$V_{\rm th} = 2\bar{n}, \tag{30}$$

where the average thermal photon number $\bar{n}$ is given by the Planck's formula

$$\bar{n} = \frac{1}{\exp\left(\frac{hf}{k_B T}\right) - 1},$$

at temperature T. The quantity h is Planck's constant, k_B is Boltzmann's constant, and f represents the frequency of the signals.

Therefore, the shot-noise level of Bob's detectors operating in the microwave regime will be different from the shot noise level in the optical regime, which is equal to 1 in vacuum shot-noise units. This shot noise will be given with respect to Alice's thermal mean photon number and will lead to an entangling cloner attack with $\omega = V_{\rm th} + 1$. Assuming room temperature of $T = 300$ Kelvin and replacing $\omega = V_{\rm th} + 1$, we can rewrite the key rate K as function of frequency f and transmissivity τ. The corresponding threshold of the rate for different block sizes is illustrated in Fig. 4 and shows that, in the microwave region, security is achieved only for transmissivities very close to $\tau = 1$ for a moderately high block size number of $N = 10^9$.

VI. CONCLUSION

In this work, we studied the security of thermal one-way quantum cryptography, including finite-size effects. These are evaluated adapting the estimation theory developed in Ref. [51] suitably extended to the case of thermal protocols. We focused on the protocol used in direct reconciliation because it is known that one-way protocols in reverse reconciliation cannot work at micro-wave frequencies.

Our analysis confirms that implementing CV-QKD with Gaussian modulated thermal states is challenging, and we cannot achieve long distance communications when we move away from a pure-loss attack scenario. When thermal noise increases (for instance $V_{\rm th} > 10$) both key rate and achievable distance rapidly deteriorate. This is caused by the role of the preparation noise variance $V_{\rm th}$ on the confidence interval. In fact, the use of large amount of trusted noise, spreads the confidence intervals reducing the transmissivity and increasing the noise to be considered. This determines a degradation of the performance, which can only be balanced by increasing the block-size. This degradation rapidly worsening when the protocol is operating in the microwave regime since in such a case the typical detector's shot-noise implies an entangling cloner attack with too high thermal noise.

Finally we remark that alternative approach, based on schemes exploiting post-selection and two-way communication might be more effective in the thermal regime. This will be investigated in future works.

VII. ACKNOWLEDGEMENTS

This work has been supported by the EPSRC via the 'UK Quantum Communications HUB' (Grant no. EP/M013472/1). Authors acknowledge V. Usenko for feedback.

Appendix A: No-switching protocol

In this appendix, we focus on the no-switching protocol studying both DR and RR. The description of the statistical estimators for the no-switching protocol is clearly analogous to that described in the main text for the switching protocol. For the no-switching scheme, we build two estimators, one for each quadrature q and p. The optimal estimators of transmissivity and excess of noise are then computed by combining them in the optimal linear combination.

Let B' describing Bob's output after the fifty-fifty beam splitter. The vectorial quadrature $X_{B'}$ =

$(q_{B'}, p_{B'})^T$ has entries given by

$$q_{B'} = \frac{q_B + q_{\rm vac}}{\sqrt{2}}, \tag{A1}$$

$$p_{B'} = -\frac{p_B - p_{\rm vac}}{\sqrt{2}}, \tag{A2}$$

where $q_{\rm vac}$ and $p_{\rm vac}$ describe the contributions from the vacuum mode mixed with mode B at the final beamsplitter.

From Eq. (5), one can write the variances of mode B as follows

$$V_B^q = \tau V_M + V_N^q, \tag{A3}$$

$$V_B^p = \tau V_M + V_N^p. \tag{A4}$$

In the general case, where Alice starts from squeezed states, the noise contributions are given by the expressions

$$V_N^q = 1 + V_\varepsilon + \tau(V_{\rm th} + V_s - 1), \tag{A5}$$

$$V_N^p = 1 + V_\varepsilon + \tau(V_{\rm th} + 1/V_s - 1). \tag{A6}$$

One can write the following output quadratures of mode B'

$$q_{B'} = \sqrt{\frac{\tau}{2}} q_M + q_{N'}, \tag{A7}$$

$$p_{B'} = -\left(\sqrt{\frac{\tau}{2}} p_M + p_{N'}\right), \tag{A8}$$

where $q_{N'}$ and $p_{N'}$ are given by

$$q_{N'} = \frac{1}{\sqrt{2}}\left(q_N + q_{\rm vac}\right) \tag{A9}$$

$$p_{N'} = \frac{1}{\sqrt{2}}\left(p_N - p_{\rm vac}\right). \tag{A10}$$

These have variances

$$V_{B'}^q = \frac{1}{2}\tau V_M + V_{N'}^q, \tag{A11}$$

$$V_{B'}^p = \frac{1}{2}\tau V_M + V_{N'}^p, \tag{A12}$$

and where

$$V_{N'}^q = \frac{V_N^q + 1}{2} = \frac{2 + V_\varepsilon + \tau(V_{\rm th} + V_s - 1)}{2} \tag{A13}$$

$$V_{N'}^p = \frac{V_N^p + 1}{2} = \frac{2 + V_\varepsilon + \tau(V_{\rm th} + 1/V_s - 1)}{2}. \tag{A14}$$

If Alice uses coherent states $V_s = 1$, the previous formulas simplify to the following expressions

$$V_{N'}^c = V_{N'}^q = V_{N'}^p = \frac{V_N^c + 1}{2} = \frac{2 + V_\varepsilon + \tau V_{\rm th}}{2}. \tag{A15}$$

The covariance between the input and output mode, for quadratures q_M and $q_{B'}$, is given by

$$\mathrm{Cov}(q_M, q_{B'}) = \sqrt{\frac{\tau}{2}} V_M. \tag{A16}$$

We can build the following statistical estimator

$$\hat{\sigma}_{MB'} = \frac{1}{m}\sum_{i=1}^{m} M_{q,i} B'_{q,i}, \tag{A17}$$

compute its expectation value, obtaining

$$\mathbb{E}\left[\hat{\sigma}_{MB'}\right] = \sqrt{\frac{\tau}{2}} V_M, \tag{A18}$$

and the variance

$$\begin{aligned} V_{\rm cov}^q &= \frac{1}{m^2}\sum_{i=1}^{m} \mathrm{Var}(M_{q,i} B'_{q,i}), \\ &= \frac{\tau V_M^2 + V_M V_{N'}^q}{m}, \\ &= \frac{\tau V_M^2}{2m}\left(2 + \frac{V_N^q + 1}{\tau V_M}\right). \end{aligned} \tag{A19}$$

Then, assuming that q_M and $q_{N'}$ are independent variables, with zero mean, we obtain the following expression for the estimator of the transmissivity

$$\hat{\tau} = \frac{2\hat{\sigma}_{MB'}^2}{V_M^2} = \frac{2V_{\rm cov}^q}{V_M^2}\left(\frac{\hat{\sigma}_{MB'}}{\sqrt{V_{\rm cov}^q}}\right)^2, \tag{A20}$$

where $\left(\frac{\hat{\sigma}_{MB'}}{\sqrt{V_{\rm cov}^q}}\right)^2$ is chi-squared distributed. Therefore, the expectation value is given by

$$\begin{aligned} \mathbb{E}(\hat{\tau}) &= \frac{2V_{\rm cov}^q}{V_M^2}\left(1 + \frac{\hat{\sigma}_{MB'}^2}{V_{\rm cov}^q}\right), \\ &= \frac{2\hat{\sigma}_{MB'}^2}{V_M^2} + \mathcal{O}(1/m), \\ &= \tau + \mathcal{O}(1/m) \end{aligned} \tag{A21}$$

and the variance

$$\begin{aligned} \mathrm{Var}(\hat{\tau}) &= \frac{8(V_{\rm cov}^q)^2}{V_M^4}\left(1 + 2\frac{\hat{\sigma}_{MB'}^2}{V_{\rm cov}^q}\right), \\ &= \frac{\frac{16\tau^2 V_M^4}{4m}\left(2 + \frac{V_N^q + 1}{\tau V_M}\right)}{V_M^4} + \mathcal{O}(1/m^2), \\ &= \frac{4\tau^2}{m}\left(2 + \frac{V_N^q + 1}{\tau V_M}\right) + \mathcal{O}(1/m^2). \end{aligned} \tag{A22}$$

For $m \gg 1$, we neglect terms proportional to $1/m^2$ and write the variance of $\hat{\tau}$ as follows

$$\sigma_q^2 := \frac{4\tau^2}{m}\left(2 + \frac{V_N^q + 1}{\tau V_M}\right). \tag{A23}$$

It is clear that repeating these steps for quadrature $\hat{p}_B$, we get

$$\sigma_p^2 := \frac{4\tau^2}{m}\left(2 + \frac{V_N^p + 1}{\tau V_M}\right), \tag{A24}$$

where the difference from σ_q^2 is the squeezing term of V_N^p.

From these, one can compute the optimal linear combination given by

$$\sigma^2_{\rm nsw} = \frac{1}{\sigma_q^{-2} + \sigma_p^{-2}}. \tag{A25}$$

Assuming that Alice starts the preparation from coherent states, we have that $V_s = 1$ and $\sigma^2_{\rm c,nsw}$ has the simpler form

$$\sigma^2_{\rm c,nsw} = \frac{2\tau^2}{m}\left(2 + \frac{V_N^c + 1}{\tau V_M}\right). \tag{A26}$$

By solving Eq. (A13) with respect to V_ε and using the estimators of $V^q_{N'}$ and τ, we obtain

$$\hat{V}_\varepsilon = 2\hat{V}^q_{N'} - \hat{\tau}(V_{\rm th} + V_s - 1) - 2. \tag{A27}$$

We can replace the expression for $\hat{V}^q_{N'}$ with

$$\hat{V}^q_{N'} = \frac{V^q_{N'}}{m}\sum_{i=1}^{m}\left(\frac{B_{q,i} - \sqrt{\frac{\tau}{2}}M_{q,i}}{\sqrt{V^q_{N'}}}\right)^2 \tag{A28}$$

which is chi-squared distributed, with mean m and variance $2m$, because $\left(B_i^q - \sqrt{\frac{\tau}{2}}M_i\right)/\sqrt{V^q_{N'}}$ is a linear combination of normally distributed variables, having unit variance and zero mean. Therefore, we obtain the following mean value for the excess noise

$$\mathbb{E}(\hat{V}_\varepsilon) = \mathbb{E}\left(2\hat{V}^q_{N'} - \hat{\tau}(V_{\rm th} + V_s - 1) - 2\right) := V_\varepsilon \tag{A29}$$

and its variance, which is given by

$$\begin{aligned} s_q^2 &:= {\rm Var}(\hat{V}_\varepsilon) = {\rm Var}\left(2\hat{V}^q_{N'} - \hat{\tau}(V_{\rm th} + V_s - 1) - 2\right) \\ &= \frac{4}{m^2}(V^q_{N'})^2 2m + (V_{\rm th} + V_s - 1)^2\sigma^2_{\rm nsw} \\ &= \frac{2}{m}(V_N^q + 1)^2 + (V_{\rm th} + V_s - 1)^2\sigma^2_{\rm nsw}. \end{aligned} \tag{A30}$$

The same steps provide the expression of the variance for quadrature p_B which is

$$s_p^2 = \frac{2}{m}(V_N^p + 1)^2 + (V_{\rm th} + 1/V_s - 1)^2\sigma^2_{\rm nsw}, \tag{A31}$$

and from Eq. (A30) and Eq. (A31), we obtain

$$s^2_{\rm nsw} = \frac{1}{s_q^{-2} + s_p^{-2}}, \tag{A32}$$

which for $V_s = 1$ simplifies to

$$s^2_{\rm c,nsw} = \frac{(V_N^c + 1)^2}{m} + \frac{V_{\rm th}^2\sigma^2_{\rm c,nsw}}{2}. \tag{A33}$$

Now, assuming the general case of moderately squeezed initial states, we can write the confidence intervals which are taken [51] as follows

$$\tau^{\rm low} = \hat{\tau} - 6.5\sigma_{\rm nsw}(\hat{\tau}, \hat{V}_\varepsilon), \tag{A34}$$

$$V_\varepsilon^{\rm up} = \hat{V}_\varepsilon + 6.5 s_{\rm nsw}(\hat{\tau}, \hat{V}_\varepsilon), \tag{A35}$$

assuming an error probability for the parameter estimation of the order of $\varepsilon_{PE} = 10^{-10}$.

Finally, proceeding as in Sec. V B, we can write a key rate of the form

$$\tilde{K} = (1 - r)\left[\tilde{R}_\xi(\xi, V_s, V_M, V_{\rm th}, V_\varepsilon^{\rm up}, \tau^{\rm low}) - \Delta\right], \tag{A36}$$

where the rate $\tilde{R}_\xi$ given by the following expression

$$\tilde{R}_\xi = \xi\tilde{I}_{AB} - \tilde{\chi}, \tag{A37}$$

where

$$\tilde{I}_{AB} = \log_2\left[1 + \frac{\tau V_M}{2 + V_\varepsilon + \tau V_{\rm th}}\right], \tag{A38}$$

and the expression of the Holevo function $\tilde{\chi}$ depends on the implementation of the no-switching protocol, i.e., if the parties use direct or reverse reconciliation.

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

[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81** 1301 (2008).

[3] 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).

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

[5] M. Hillery, Phys. Rev. A **61**, 022309 (2000).

[6] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).

[7] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[8] T. Symul, D. J. Alton, S. M. Assad, A. M. Lance, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. A **76**, 030303(R) (2007).

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

[10] K. Bradler and C. Weedbrook, Phys. Rev. A **97**, 022310

(2018).
[11] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, Phys. Rev. A **87**, 020303(R) (2013).
[12] Z Li, Y Zhang, X Wang, B Xu, X Peng, H Guo, Phys. Rev. A **93**, 012310 (2016).
[13] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[14] F. Grosshans and P. Grangier, Proceedings of the 6th International Conference on Quantum Communications, Measurement, and Computing, (2002).
[15] F. Grosshans, G. Van Ache, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[16] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[17] V. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).
[18] V. C. Usenko and F. Grosshans, Phys. Rev. A **92**, 062337 (2015).
[19] T. Gehring, C. S. Jacobsen, and U. L. Andersen, Quantum Inf. Comput. **16**, 1081 (2016).
[20] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
[21] D. Huang, P. Huang, D. Lin, and G. Zeng, Sci. Rep. **6**, 19201 (2016).
[22] Y. Zhang et al, arXiv:1709.04618, (2017).
[23] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nat. Phys. **4**, 726 (2008).
[24] C. Ottaviani and S. Pirandola, Sci. Rep. **6**, 22225 (2016).
[25] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A **92**, 062323, (2015).
[26] J. H. Shapiro, Phys. Rev. A **80**, 022320 (2009).
[27] Q. Zhuang, Z. Zhang, J. Dove, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **94**, 012322 (2016).
[28] Z. Zhang, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, Phys. Rev. A **95**, 012332 (2017).
[29] D. Bunandar, Z. Zhang, J. H. Shapiro, and D. R. Englund, Phys. Rev. A **91**, 022336 (2015).
[30] Z. Zhang, C. Chen, Q. Zhuang, F. N. C. Wong, and J. H. Shapiro, arXiv:1712.04973 (2017).
[31] S. L. Braunstein and S. Pirandola Phys. Rev. Lett. **108**, 130502 (2012).
[32] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[33] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Ghering, C.S. Jacobsen, and U. L. Andersen, Nat. Photonics **9**, 397 (2015).
[34] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Phys. Rev. A **91**, 022320 (2015).
[35] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, arXiv:1709.06988, (2017).
[36] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).
[37] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).
[38] C. Weedbrook, C. Ottaviani, S. Pirandola, Phys. Rev. A **89**, 012309 (2014).
[39] S. Pirandola, R. Garcia-Patrón, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).
[40] R. Filip, Phys. Rev. A **77**, 022310 (2008).
[41] V. Usenko and R. Filip, Entropy **18**, 20 (2016).
[42] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017); see also arXiv:1510.08863 and arXiv:1512.04945.
[43] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi, arXiv:1711.09909 (2017).
[44] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[45] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[46] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, arXiv:1704.07924 (2017).
[47] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
[48] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A **96**, 042332 (2017).
[49] I. Devetak and A. Winter, Proc. R. Soc. Lond. A **461**, 207 (2005).
[50] H. Holevo, Problems Inform. Transmission **9**, 177, (1973).
[51] L. Ruppert, V. C. Usenko, and R. Filip, Phys. Rev. A **90**, 062310 (2014).
[52] C. S. Jacobsen, T. Gehring, and U. L. Andersen, Entropy **17**, 4654 (2015).
[53] R. Renner and J.I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009)
[54] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[55] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[56] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A **95**, 052310 (2017).
[57] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101** 200504 (2008).
[58] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley & sons, (2006).
[59] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, arXiv:1702.07740 (2017).
[60] X. Wang, Y.-C. Zhang, Z. Li, B. Xu, S. Yu, and H. Guo, arXiv:1703.04916 (2017).