# Perspectives of microwave quantum key distribution in the open air

F. Fesquet,[1,2,*] F. Kronowetter,[1,2,3] M. Renger,[1,2] Q. Chen,[1,2] K. Honasoge,[1,2] O. Gargiulo,[1,2] Y. Nojiri,[1,2] A. Marx,[1] F. Deppe,[1,2,4,†] R. Gross,[1,2,4] and K. G. Fedorov[1,2,‡]

[1]*Walther-Meißner-Institut, Bayerische Akademie der Wissenschaften, 85748 Garching, Germany*
[2]*School of Natural Sciences, Technische Universität München, 85748 Garching, Germany*
[3]*Rohde and Schwarz GmbH and Co. KG, Mühldorfstraße 15, 81671 Munich, Germany*
[4]*Munich Center for Quantum Science and Technology, Schellingstrasse 4, 80799 Munich, Germany*

(Received 14 April 2022; accepted 17 August 2023; published 14 September 2023)

One of the cornerstones of quantum communication is the unconditionally secure distribution of classical keys between remote parties. This key feature of quantum technology is based on the quantum properties of propagating electromagnetic waves, such as entanglement, or the no-cloning theorem. However, these quantum resources are known to be susceptible to noise and losses, which are omnipresent in open-air communication scenarios. In this paper, we theoretically investigate the perspectives of continuous-variable open-air quantum key distribution at microwave frequencies. In particular, we present a model describing the coupling of propagating microwaves with a noisy environment. Using a protocol based on displaced squeezed states, we demonstrate that continuous-variable quantum key distribution with propagating microwaves can be unconditionally secure with communication at room temperature up to distances of around 200 m, limited by the total coupled noise photon number. Moreover, we show that microwaves can potentially outperform conventional quantum key distribution at telecom wavelengths and imperfect weather conditions.

DOI: 10.1103/PhysRevA.108.032607

## I. INTRODUCTION

Quantum key distribution (QKD) is a method to securely exchange a common key between two parties, conventionally referred to as Alice and Bob. QKD has attracted increasing interest over the last decades due to the promise of unconditionally secure communication while maintaining high secret key rates [1,2]. The security of commonly used classical encryption schemes is based on asymmetric mathematical problems which cannot be easily inverted by classical methods. Prominent examples are the Diffie-Hellman algorithm and the RSA code [3,4]. In contrast, QKD relies on the fact that unconditional security is provided by the fundamental laws of quantum mechanics, taking advantage of unique quantum resources, such as entanglement [5], or notably, the no-cloning theorem [6]. In QKD based on continuous-variable quantum states (CV-QKD), one encodes information in conjugate electromagnetic field quadratures, according to various specific protocols [7]. In particular, CV-QKD protocols provide a powerful alternative to QKD based on discrete-variable quantum states (DV-QKD), due to potentially higher secret key rates and being compatible with the existing communication infrastructure [8,9].

First successful realizations of QKD protocols have been implemented at the near-infrared regime at so-called telecom wavelengths (780–850- and 1520–1600-nm wavelength) [10], where a significant progress has been achieved with the recent realization of ground-to-satellite QKD networks [11]. A particular reason for this choice of frequencies is the low atmospheric absorption on the order of less than $1.0 \times 10^{-2}$ dB/km [12]. However, in the light of recent impressive achievements with superconducting quantum circuits operating in the microwave regime [13–16] and due to the lack of efficient microwave-to-optical frequency transducers [17], a natural choice is to consider quantum communication and QKD in the associated microwave regime. Here, superconducting Josephson parametric amplifiers (JPAs) represent a robust source of quantum states in the form of squeezed microwaves. Flux-driven JPAs routinely generate microwave squeezed states with squeezing levels up to 10 dB below the vacuum limit [18–20].

In this paper, we focus on a theoretical analysis of a particular one-way communication prepare-and-measure CV-QKD protocol with Gaussian modulation [21] for the microwave wavelength range of 30–300 mm, corresponding to the frequency range of 1–10 GHz. We analyze the potential of this protocol for open-air microwave quantum communication (MQC), considering realistic atmospheric conditions. We compare its performance to a traditional implementation at the telecom wavelength of 1550 nm (193.55 THz). We model the signal readout with a homodyne detection, since the information is encoded only in one of the two electromagnetic field quadratures. In the last step, signal detection is followed by a one-way classical reconciliation, or error correction, protocol. There, an important distinction must be made between either direct reconciliation (DR) or reverse reconciliation (RR) [9]. In DR, the one-way communication is performed from Alice to Bob. As a result, Alice's key is used as a reference which

*florian.fesquet@wmi.badw.de
†Present address: IQM Germany GmbH, Nymphenburger Straße 86, 80335 München, Germany.
‡kirill.fedorov@wmi.badw.de

 

Bob tries to estimate from the data he obtained via the communication. In contrast, in RR the one-way communication goes from Bob to Alice, where Bob's measured key is estimated by Alice.

The paper is organized as follows: in Secs. II and III, we introduce all relevant elements for a practical implementation of the CV-QKD protocol in the microwave regime. We perform a quantitative analysis of the secret key rate and secure distance, assuming either DR or RR with an ideal reconciliation efficiency in the asymptotic case, i.e., in the case of Alice and Bob exchanging an infinitely long key. We additionally present a model based on beam splitter transformations to describe the coupling of propagating microwaves with a bright microwave thermal background. Our results show that microwave CV-QKD can be well suited for short-distance open-air communication scenarios. In particular, in Sec. IV we find that the microwave CV-QKD protocol may produce higher secure key rates than its telecom counterpart. We conclude our discussion in Sec. V with a detailed study of weather effects for the particular common cases of rain and haze. We find that MQC secure communication distances are almost unchanged as compared to ideal dry weather conditions. This is in striking contrast to the protocols in the telecom wavelength regime.

## II. QUANTUM KEY DISTRIBUTION PROTOCOL WITH CONTINUOUS VARIABLES

First, we consider a prepare-and-measure CV-QKD protocol, independent of a particular hardware platform and frequency range, as described in [21]. A corresponding scheme is shown in Fig. 1. Here, Alice transmits to Bob a Gaussian-modulated random key $\mathcal{K} = \{k_1, \ldots, k_i, \ldots, k_N\}$. This key is a string of real numbers $k_i$, randomly chosen from a Gaussian distribution with variance $\sigma_A^2$. To this end, Alice prepares a $q$-squeezed or $p$-squeezed state [15], with both states having an equal chance of being selected. Each symbol, $k_i$, is then encoded as a displacement amplitude, $\alpha_i$, of each squeezed state such that $|\alpha_i| = |k_i|$. Averaging over various states of Alice results in a thermal state, preventing Eve from extracting any information on the encoding basis and encoded symbols. This imposes an additional constraint $\sigma_s^2 + \sigma_A^2 = \sigma_{as}^2$, where we denote the squeezed and antisqueezed quadrature variance as $\sigma_s^2$ and $\sigma_{as}^2$, respectively. The resulting displaced squeezed state propagates through a lossy and noisy quantum channel $\mathcal{N}$ before being received and measured by Bob with a local homodyne measurement. After repeating this process for each of Alice's symbols, Bob obtains a measured key $\mathcal{K}' = \{k'_1, \ldots, k'_i, \ldots, k'_N\}$, representing an estimation of Alice's key $\mathcal{K}$.

In order to obtain a common secret key, Alice and Bob perform a one-way classical postprocessing. The first step, known as sifting of the keys, consists of producing compatible data by discarding any measurement where encoding and measurement basis disagree. The second step, commonly referred to as parameter estimation, allows to obtain an upper bound on the amount of information lost in the quantum channel by statistically estimating the quantum channel losses and noise photon number. Then, a classical reconciliation algorithm, depending on whether DR or RR has been chosen, is used to generate a common key. The performance of this algorithm is characterized with a reconciliation efficiency $\beta$. Alice and Bob further proceed to a confirmation step to validate a recovered common key. Finally, a classical privacy amplification algorithm produces a secret key by discarding any eavesdropped bits of the common key.

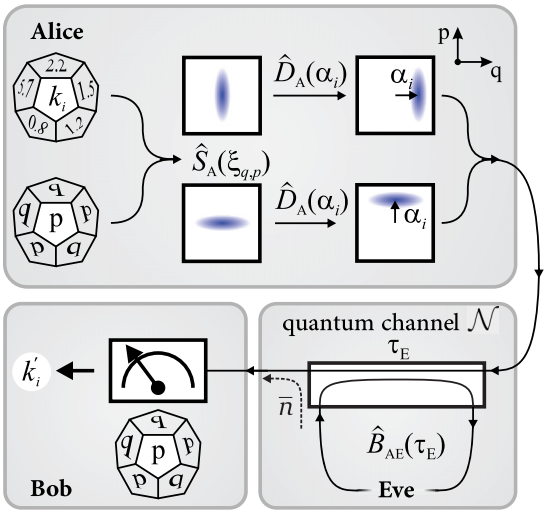


FIG. 1. General scheme of a QKD protocol based on displaced squeezed states. Here, Alice starts by generating a random continuous-variable number $k_i$ corresponding to Alice's symbol and randomly choosing among one of the two possible encoding bases, $q$ or $p$. This procedure results in propagating states which are squeezed along one or the other quadrature with the complex squeezing amplitude $\xi$. Every symbol $k_i$ is encoded via a displacement amplitude $\alpha_i$, such that $|\alpha_i| = |k_i|$. The resulting displaced squeezed state is sent through a quantum channel $\mathcal{N}$ with transmissivity $\tau_E$. This channel is assumed to be under full control of a potential eavesdropper, Eve, who also induces extra noise photon $\bar{n}$. At the end, Bob receives a state which he measures in a random basis $q$ or $p$ in order to obtain an estimate, $k'_i$, of the original symbol.

To describe the quantum channel $\mathcal{N}$, we quantify losses using a quantum channel transmissivity $\tau_E$ and quantum channel coupled noise photons $\bar{n}$, which represents an average noise photon number referred to the output of the channel. Generally, these losses and noise represent interactions between the propagating states and environment. In the worst case, from the standpoint of security, the quantum channel is under the full control of a potential eavesdropper, Eve. This implies that our estimated secure bit rates are lower bounds of realistically achievable secure bit rates. Here, we analyze an asymptotic case, where Alice communicates an infinitely long key, $N \to \infty$. Using this assumption, we can restrict our analysis to collective Gaussian attacks [22], while considering them as the most general attacks [23,24]. Lastly, since in practical QKD protocols only a finite number of symbols can be communicated, we consider so-called finite-size effects [25], which effectively reduce the maximal secure communication distance. For details of derivation of the finite-size effects, we refer to Appendix B.

In collective Gaussian attacks, all physical Gaussian states remain Gaussian states throughout the quantum communication. Additionally, Eve is assumed to interact individually with

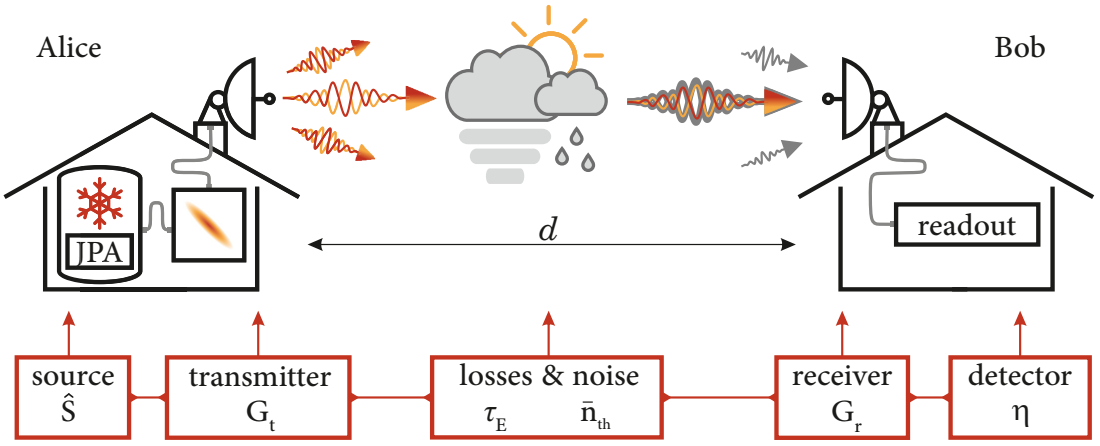


FIG. 2. Schematics of main components for an open-air MQC. Source denotes a squeezing generator, typically implemented with a JPA in a cryogenic environment. Transmitter and receiver represent corresponding microwave antennae with gains $G_t$ and $G_r$, respectively. These antennae belong to different communication parties, Alice and Bob, and are separated by a distance $d$. Atmospheric absorption losses are quantified using transmissivity $\tau_E$ which couples the quantum communication channel to the open-air environment with the thermal noise photon number $\bar{n}_{th}$. Readout is modeled as a homodyne detector with an overall quantum efficiency $\eta$.

each state sent by Alice and to store all her extracted states in a quantum memory before applying a joint measurement on her state ensemble at the end of the classical postprocessing. Then, Eve's eavesdropping attack can be extended, i.e., dilated, into an entangling cloner attack [26]. In this attack, Eve starts with a two-mode squeezed (TMS) vacuum state [27] for each incoming state from Alice. One of these modes is coupled to the quantum channel via a beam splitter with transmissivity $\tau_E$, while Eve preserves the other uncoupled mode (for details, see Appendix A). After interaction with Alice's signal, this coupled mode contains partial information on the communicated key. A general TMS state features quantum entanglement, implying that both Eve's modes are strongly correlated. Then, Eve can use these correlations to extract as much information as possible on the sent key.

We model our CV-QKD protocol using an input state $\hat{\rho}_{in}$ for each symbol $k_i$. This input state contains three modes. The first mode is used by Alice to generate the displaced squeezed states. The remaining two modes describe Eve's TMS state. The first mode of Eve's TMS state locally looks like a thermal state coinciding with the environmental noise state, but possessing quantum entanglement with the third, retained, Eve mode. Following this formalism, we denote the final state $\hat{\rho}_{out}$, which is also a three-mode state, where its first mode corresponds to the local state which Bob receives after Eve's attack. Similarly, the remaining two modes describe Eve's modes after her attack. The final state can be written as

$$\hat{\rho}_{out} = \hat{T}_{AE}\,\hat{\rho}_{in}\,\hat{T}_{AE}^{\dagger}, \quad \hat{T}_{AE} = \hat{B}_{AE}(\tau_E)\,\hat{D}_A(\alpha_i)\,\hat{S}_A(\xi), \qquad (1)$$

where $\hat{B}_{AE}(\tau_E)$ is a beam splitter operator (see Appendix A) with transmissivity $\tau_E$, which describes coupling Alice's mode to environment (Eve's mode). Similarly, $\hat{D}_A(\alpha_i)$ represents the displacement operator [28] applied to Alice's mode, with the displacement amplitude encoding a specific symbol, $|\alpha_i| = |k_i|$. Additionally, $\hat{S}_A(\xi)$ corresponds to the squeeze operator [15] acting on Alice's mode, and $\xi$ is the complex squeezing amplitude. Considering that all states in this protocol are Gaussian states, we derive from Eq. (1) the variance $\sigma_B^2$ of Bob's measured key $\mathcal{K}'$ as

$$\begin{aligned}\sigma_B^2 &= \tau_E\,\sigma_{as}^2 + (1-\tau_E)\sigma_E^2 + n_{amp}/2 \\ &= \tau_E\,\sigma_{as}^2 + (1-\tau_E)/4 + \bar{n} + n_{amp}/2\,, \end{aligned} \qquad (2)$$

where we further introduce $n_{amp}$ as the noise photon number added by Bob's measurement (see Sec. III B).

## III. EXPERIMENTAL SETUP CONSIDERATIONS

An open-air implementation of the above introduced CV-QKD protocol requires various aspects to be taken into account. In this paper, we focus on the central components to realize such an open-air MQC and present the associated generic scheme in Fig. 2. We analyze the generation and detection of propagating squeezed states at millikelvin temperatures. Detection is modeled by a homodyne quadrature measurement with quantum efficiency $\eta$. Coupling of the squeezed states to the open-air environment (atmosphere) is modeled with two antennae with corresponding gain coefficients. The environment is assumed to be at ambient temperature, $T = 300\,\mathrm{K}$, and is described by frequency-dependent absorption losses. The latter may also be subject to imperfect weather conditions, as it will be discussed later.

### A. Generation of quantum microwave states

The experimental realization of the CV-QKD protocol requires the generation of propagating displaced squeezed states. In the microwave regime, flux-driven JPAs provide a well-established tool to generate squeezed states with tunable squeezing level and angle [18,29]. Typically, JPAs consist of a coplanar waveguide $\lambda/4$ resonator, which is short-circuited to ground by a direct current superconducting quantum interference device (dc-SQUID). This dc-SQUID acts as flux-tunable inductance which can be modulated by applying an external magnetic flux resulting in a flux tunability of the resonance frequency of the JPA. Applying a microwave pump signal

inductively coupled to the $\lambda/4$ resonator, JPAs can provide phase-insensitive or phase-sensitive amplification of incident signals [30]. The latter regime is directly related to the generation of squeezed microwave states. According to Cave's theory of noise in linear amplifiers [31], phase-insensitive bosonic amplifiers are quantum limited in the sense that they add at least half a noise photon to an input signal. In contrast, a phase-sensitive amplifier can, in principle, achieve noiseless amplification. In practice, JPAs have proven to approach both these limits, which makes them well qualified for MQC applications. Over the course of many experiments, JPAs operating in the GHz regime were shown to reach noise levels well below the quantum limit, reaching noise levels on the order of 0.1 added noise photons in the phase-sensitive regime [18,32,33]. Presently, the noise performance of JPAs is known to be limited by fabrication imperfections, pump-induced noise [32,33], or higher-order nonlinearities [34]. Lastly, the displacement operation required by our CV-QKD protocol can be experimentally realized by applying strong coherent drive tones to cryogenic directional couplers [28]. Ultimately, the combination of JPAs with subsequent directional couplers allows one to generate displaced squeezed states with a desired displacement amplitude $\alpha$.

### B. Microwave antennae and amplification noise

In order to couple propagating microwave states, generated at millikelvin temperatures, to the open-air quantum channel one requires a microwave interface between the corresponding cryogenic environment and the open-air medium. A microwave antenna serves as such kind of interface. The antenna may be modeled by a transmission line of spatially varying impedance connecting the 50-$\Omega$ matched cryogenic circuits to open-air channels with characteristic impedance of 377 $\Omega$. A central figure of merit of the transmitter and receiver antennae is their passive antenna gain, $G$. In general, for microwave antennae, the gain reads [35]

$$G = \eta_{\mathrm{rad}}\, D, \tag{3}$$

where $0 \leqslant \eta_{\mathrm{rad}} \leqslant 1$ is the radiation efficiency and accounts for the antenna losses, while $D$ represents the antenna directivity. The latter expresses the ability of the antenna to focus the emitted power into a specific direction and strongly depends on the antenna geometry. An antenna with a well-defined physical aperture area, $A$, has the directivity

$$D = \frac{4\pi A}{\lambda^2}\, e_{\mathrm{A}}, \tag{4}$$

where $A$ is determined by the size and shape of the antenna, $\lambda$ is the signal wavelength, and $e_{\mathrm{A}}$ is the aperture efficiency, defined as the ratio between the effective aperture and physical aperture areas. Cryogenic to open-air transmission of microwave signals is a current technological challenge. First proposals already exist [36]. For communication distances of approximately 50 m, an open-air geometric attenuation of signals, also known as the path loss, is around 80 dB (see Sec. III C) at the frequency of 5 GHz. In general, the path loss can be compensated by using transmitter and receiver antennae with sufficient gain. For instance, a parabolic transmitter and receiver antenna with a diameter of around $D_{\mathrm{ant}} = 2$ m could compensate for the aforementioned path loss. A more detailed analysis on antennae designs, gains, and related path losses goes beyond the scope of this paper and is discussed elsewhere [37]. Here, we assume that antenna gains fully compensate for the path loss and focus on the effects of atmospheric absorption losses as the main source of communication imperfections.

Lastly, in order to finalize the prepare-and-measure CV-QKD protocol, one has to perform a homodyne quadrature measurement. In the microwave regime, this task requires usage of linear amplifiers with a certain quantum efficiency, $\eta_{\mathrm{mw}}$, to quantify the amplification chain noise performance. The quantum efficiency is defined as the ratio between vacuum fluctuations and fluctuations in output signals resulting from additional noise photon number $n_{\mathrm{amp}}$ due to amplification, where $n_{\mathrm{amp}}$ is referred to the input of the detection chain. Therefore, we can express the quantum efficiency as [32]

$$\eta_{\mathrm{mw}} = \frac{1}{1 + 2n_{\mathrm{amp}}}. \tag{5}$$

State-of-the-art traveling-wave parametric amplifiers (TWPAs) allow for phase-insensitive amplification with high gain values ($\approx$20 dB) and broad bandwidths ($\approx$3 GHz) at cryogenic temperatures. These TWPAs are also potentially able to approach the quantum-limited regime characterized by $n_{\mathrm{amp}} = 0.5$ for the phase-insensitive mode of operation [31]. Conversely, as mentioned in [38], a phase-sensitive linear amplifier could achieve noiseless amplification of a single quadrature, at the cost of deamplifying the conjugate quadrature. Such a detection scheme can be used to implement a microwave homodyne detection similar to its optical counterpart [39]. In cryogenic microwave experiments, one typically uses chained quantum-limited amplifiers followed by cryogenic high-electron-mobility transistor amplifiers. In this case, we can use the Friis formula to estimate the total amplification noise $n_{\mathrm{amp}}$ of the detection chain. For instance, for the case of two chained amplifiers and in the limit of large amplification, $G_{1,2} \gg 1$, the total amplification noise reads

$$n_{\mathrm{amp}} = n_1 + \frac{n_2}{G_1}, \tag{6}$$

where $n_1$ and $G_1$ are the noise photon number and gain of the first amplifier in the chain, while $n_2$ describes the input noise photon number of the second amplifier. Thus, the total noise $n_{\mathrm{amp}}$ depends mainly on the noise properties of the first amplifier. For homodyne detectors at telecom wavelengths, the quantum efficiency is usually modeled by additional losses, introduced by a nonunity transmissivity within a beam splitter model. For the case of a purely lossy optical detector, both approaches are known to be equivalent, as described in [34]. However, we emphasize that our definition of the quantum efficiency is well suited for the study of microwave quantum communication, as the efficiency of signal readout is primarily limited by amplification noise in this case.

### C. Losses and noise budget

We conclude this section with a brief analysis of losses and noise in open-air communication channels, where losses scale with the communication distance. We distinguish between

two categories of losses: (i) the path loss which represents geometric attenuation of propagating signals and (ii) absorption losses due to coupling to the environment, such as the atmospheric absorption losses or weather-induced losses. For signals transmitted and received via the antennae, the path loss $L_{\rm p}$, describing the fraction of the initial signal power lost during the communication, is commonly described using the Friis transmission formula [35]

$$L_{\rm p} = 10\log_{10}\left[G_{\rm t}G_{\rm r}\left(\frac{\lambda}{4\pi d}\right)^2\right]. \tag{7}$$

Here, $G_{\rm t}$ ($G_{\rm r}$) is the transmitter (receiver) antenna gain, $\lambda$ is the wavelength of the communication signals, and $d$ is the propagation distance. As mentioned above, we consider in the remainder of the paper that the experimental implementation of the QKD protocol is done with antennae that fully compensate for path losses. With this assumption, we focus our analysis on purely physical limitations expressed in terms of losses and coupled noise photon number. To this end, we model the absorption and scattering power losses via a single effective beam splitter with transmissivity $\tau_{\rm E}$ given by

$$\tau_{\rm E} = 10^{-\gamma d/10}, \tag{8}$$

where $\gamma$ is the total specific attenuation (dB/km) given by the sum of each specific attenuation $\gamma_i$ associated with their respective loss mechanism. In our case, we attribute these losses to atmospheric absorption and weather conditions such as rain or haze. Empirical models show that for microwave frequencies around $\omega_{\rm mw}/2\pi \simeq 5\,$GHz, propagation losses mainly arise due to molecular oxygen absorption [40]. For the ideal case of dry weather, we estimate the corresponding specific attenuation of $\gamma_{\rm mw} = 6.3\times10^{-3}\,$dB/km [40]. To describe the coupling of the propagating quantum bosonic signal $\hat{a}$ to the noisy environmental modes, we use the input-output formalism. The output signal mode $\hat{a}'$ can be expressed as

$$\hat{a}' = \sqrt{\tau_{\rm E}}\,\hat{a} + \sqrt{1-\tau_{\rm E}}\,\hat{h}_{\rm env}, \tag{9}$$

where $\hat{h}_{\rm env}$ corresponds to the environmental thermal mode. The latter may be a vacuum or thermal state, depending on the carrier frequency and environment temperature. For a thermal background, the average thermal noise photon number $\bar{n}_{\rm th}$ per mode is given by the Planck distribution as

$$\bar{n}_{\rm th} = \frac{1}{\exp\left(\frac{\hbar\omega}{k_{\rm B}T}\right)-1}, \tag{10}$$

where $\hbar$ is the reduced Planck constant, $k_{\rm B}$ is the Boltzmann constant, $\omega/2\pi$ is the signal frequency, and $T$ is the background temperature. From Eq. (9), the relation between the photon number $\bar{n}_{\rm th}$ and the coupled noise photon number $\bar{n}$ is expressed as

$$\bar{n} = \tfrac{1}{2}(1-\tau_{\rm E})\,\bar{n}_{\rm th}. \tag{11}$$

Finally, it is instructive to consider open-air losses at telecom wavelengths. We emphasize that Eq. (7) is also applicable in the optical frequency range. Then, $G_{\rm t}$ and $G_{\rm r}$ correspond to the effective passive gain of optical lenses used to focus and collect optical beams. Typical telecom wavelengths (780–850 and 1520–1600 nm) are chosen to suffer from the lowest possible atmospheric absorption losses. At the telecom wavelength of 1550 nm, absorption losses of less than $1.0\times10^{-2}\,$dB/km can be reached [12]. In this case, open-air attenuation is mainly caused by scattering losses, such as Rayleigh or Mie scattering [12]. The corresponding open-air specific attenuation is $\gamma_{\rm tel} = 2.02\times10^{-1}\,$dB/km. We discuss the additional attenuation due to rain and haze in more detail in Sec. V.

## IV. SECURITY ANALYSIS

### A. Secret key

In order to assess the experimental feasibility of our CV-QKD protocol, it is mandatory to analyze its security. The latter is quantified by the secret key $K_{\rm exp}$, which represents the amount of secure information per communicated symbol. The secret key is bounded by

$$K_{\rm exp} \geqslant K = \beta\, I(A{:}B) - \chi_{\rm E}. \tag{12}$$

Here, $I(A{:}B)$ is the mutual information between Alice and Bob and measures correlations between the key sent by Alice and that measured by Bob. Additionally, $\chi_{\rm E}$ is the Holevo quantity [41] of Eve and gives an upper bound on the information that Eve obtains during her attack (see Appendix A). It should be noted that experimental values $\beta > 0.9$ have been obtained and can be commonly achieved with current classical postprocessing error correction algorithms [42]. A positive value of $K$ indicates a secure communication, as Alice and Bob share more information than Eve can in principle obtain. In order to take into account the finite size of the communicated key between Alice and Bob, the secret key expression must be modified as [37]

$$K_{\rm exp} \geqslant K_N = \frac{n_{\rm ec}\,p_{\rm ec}}{N}[K(\hat{\tau}_{\rm E}^{\star},\hat{\bar{n}}^{\star}) - \Delta(n_{\rm ec})], \tag{13}$$

where $n_{\rm ec} \leqslant N$ denotes the number of symbols kept for the reconciliation algorithm while $m = N - n_{\rm ec}$ symbols are used for parameter estimation. The latter is assumed to succeed with a probability of $p_{\rm ec}$. The additional term $\Delta(n_{\rm ec})$ corresponds to a correction term due to the key finite size. Lastly, $\hat{\tau}_{\rm E}^{\star}$ ($\hat{\bar{n}}^{\star}$) is a statistical estimator of $\tau_{\rm E}$ ($\bar{n}$) built after Alice's and Bob's communication using $m$ symbols (see Appendix B for more details).

In Fig. 3, we show results of numerical evaluation of the secret key as a function of the transmissivity $\tau_{\rm E}$ and noise photon number $\bar{n}$ in the quantum channel. Remarkably, in the DR case a secure communication cannot exist when $\tau_{\rm E}$ exceeds a threshold value of 0.5, which illustrates the well-known result that secure CV-QKD communication in DR schemes is limited to 3 dB of losses [43,44]. The reason for this fact is that communication with DR cannot be secure when Eve receives more than 50% of Alice's information. In this scenario, Eve effectively replaces Bob as the communication partner. As illustrated in Fig. 3, this limit can be entirely circumvented by using the RR scheme. Then, Bob's measured key is treated as a reference and Alice needs to correct her own key according to it. For RR, if we imagine that Eve only induces losses during the quantum communication, Alice has always more information than Eve on Bob's measured key. This is because, in her attack, Eve is assumed to induce losses by using a

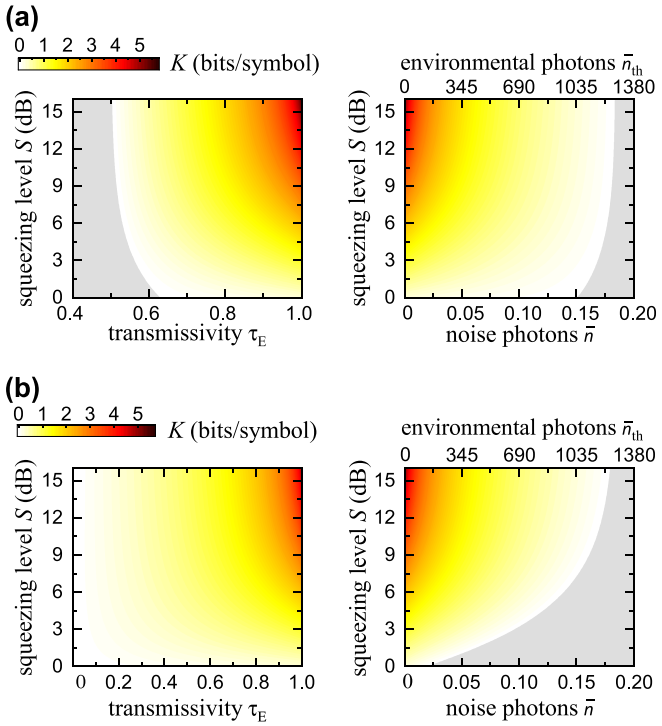


FIG. 3. Secret key $K$ of the CV-QKD protocol plotted as a function of the squeezing level $S$ (measured in dB below the vacuum limit), transmissivity $\tau_E$, and noise $\bar{n}$, for ideal detection efficiency $\eta_{mw} = 1$. (a), (b) The cases of DR and RR, respectively. The number of environmental noise photons, $\bar{n}$, is shown for a fixed communication distance, $d = 200$ m, and microwave specific attenuation, $\gamma_{mw} = 6.3 \times 10^{-3}$ dB/km. Gray areas represent the regions of negative keys, i.e., insecure communication.

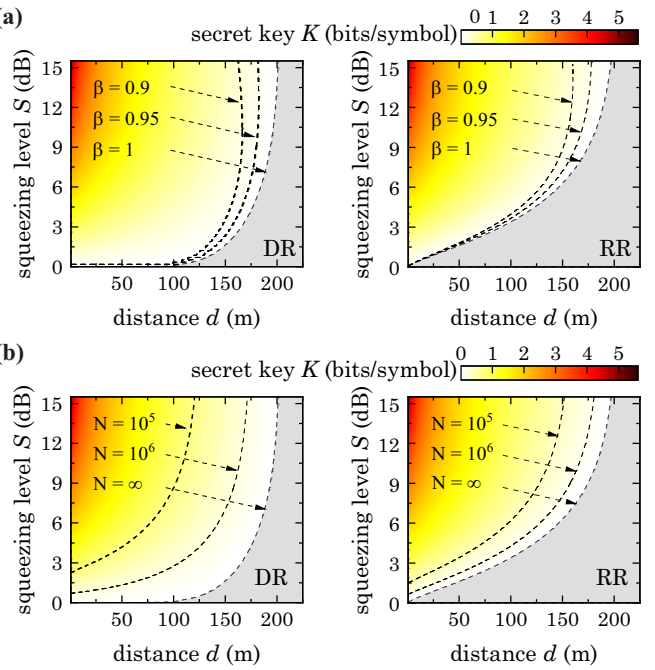


FIG. 4. Secret key $K$ of the CV-QKD protocol as a function of communication distance $d$ and squeezing level $S$. The left (right) plot corresponds to the DR (RR) case. The dashed lines represent $K = 0$ for different values of $\beta$ in panel (a) and different values of $N$ in panel (b). Squeezing is given in dB below the vacuum level. Detection efficiency is assumed to be ideal, $\eta_{mw} = 1$. We assume the average environmental noise photon number $\bar{n}_{th} = 1250$ and transmission losses $\gamma_E = \gamma_{mw} \simeq 6.3 \times 10^{-3}$ dB/km. Gray areas represent the regions of negative keys, i.e., insecure communication.

beam splitter to get part of the signals sent by Alice. As a result, Eve can only obtain a fraction of Alice's information. Furthermore, in the case of very large losses ($\tau_E \to 0$), Bob receives only a tiny fraction of the signal coming from Alice, meaning that his signal is largely uncorrelated with Eve's eavesdropped signal. As a consequence, Eve's information reveals very little about Bob's measured key, making the communication secure. If Eve couples noise photons in addition to the previous losses, the correlations between the key sent by Alice and that measured by Bob decrease. At the same time, Eve gains more information on the key measured by Bob. In particular, the communication is secure up to a coupled noise photon threshold value $\bar{n}$ of 0.183 for both reconciliation cases. This result is consistent with the well-known Pirandola-Laurenza-Ottaviani-Banchi upper bounds for Gaussian channels [45]. This noise threshold corresponds to the crossover of the quantum channel capacity from finite values to zero. It is also important to note that these noise numbers do not account for noise photons which can be added by Bob during his measurements. Finally, we observe that an increase in squeezing level results in an increase of the secret key. This increase can be understood as a decrease of the displacement uncertainty encoding the symbols, while also allowing for higher displacement amplitudes [21].

Next, we extend our analysis of the microwave CV-QKD protocol to variable communication distances $d$, for both DR and RR. To this end, we use Eq. (9) in combination with the specific attenuation given in Sec. III C to convert communication distances $d$ into corresponding transmissivities $\tau_E$. We additionally consider the effects of imperfect reconciliation and finite-size effects. The corresponding secret keys are shown in Fig. 4. Remarkably, we observe positive secret key values over communication distances of up to 200 m, in both DR and RR. These results suggest the experimental feasibility of microwave QKD in open-air conditions. No major distinction in communication distances is observed between the reconciliation cases, although one could intuitively expect RR to yield larger distances according to our previous discussion. This behavior originates from the presence of the bright microwave thermal background which couples to propagating states during the communication. Consequently, the effects of coupled noise largely outweigh the effects of losses and make the RR and DR cases more similar. As shown in Fig. 4(a), we observe that an imperfect reconciliation with $0.9 \leqslant \beta \leqslant 1$ leads only to a slight decrease of the maximal secure communication distance with positive secret key values still up to 176 m (167 m) for $\beta = 0.95$ ($\beta = 0.9$). However, we note that finite-size effects have a more significant impact on the secret key values as presented in Fig. 4(b). Here, the total length $N$ of the key critically determines the secure communication distance. For instance, a practical key length of $N = 10^5$ decreases the secure communication distance to 122 m(154 m) in the

DR case (RR case). These effects can be overcome by extending the key length to larger values. A realistic but more demanding key length of $N = 10^6$ extends the secure communication distance to 172 m(183 m) in the DR case (RR case). Lastly, we comment on the Gaussian modulation for our protocol as compared to a discrete modulation regime. To this end, we consider the discrete modulation homodyne detection quadrature phase shift keying CV-QKD protocol [46,47]. Our preliminary analysis indicates that the CV-QKD protocol with discrete modulation [47] can be realized in the microwave regime and, under ideal conditions, could achieve notably larger secure communication distances than for the protocols with Gaussian modulation. However, under more realistic conditions with noisy detectors, the discrete modulation protocols quickly lose their advantage as a function of the detection noise, as compared to the Gaussian modulation protocols. Further detailed investigations are needed here.

For a more practical evaluation of the QKD performance, one typically uses a secret key rate $R_0$. The latter evaluates the amount of secure bits per second that can be obtained from the communication protocol. Under the asymptotic case assumption, one can express the secret key rate $R_0$ in bits per second using the secret key as

$$R_0 = f_r K, \tag{14}$$

where $f_r$ represents the repetition rate (in symbols per second). This rate encompasses all information postprocessing steps, such as sifting, parameter estimations [5,7], and experimental bandwidths of the involved devices. We use an upper bound on the secret key rate $R$, derived from the Shannon-Hartley theorem and the Nyquist rate [48]

$$R_0 \leqslant R = 2\,\frac{\Delta\omega}{2\pi}\,K, \tag{15}$$

where $\Delta\omega/2\pi$ denotes the experimental detection bandwidth. This upper bound becomes especially useful when comparing different physical QKD platforms, as it is going to be discussed in the next section.

### B. Comparison of telecom and microwave frequency regimes

Here, we now compare the microwave CV-QKD performance to that of QKD at telecom frequencies. For this purpose, we define and numerically compute a communication crossover distance $d_c$:

$$d_c := \max_{R_{mw} \geqslant R_{tel}} (d), \tag{16}$$

where $d$ corresponds to communication distance, while $R_{mw}$ and $R_{tel}$ are the secret key rates for microwave and telecom frequencies, respectively. According to Eq. (15), it is relevant to optimize the detection bandwidth to achieve high secret key rates. To this end, we assume an experimental state-of-the-art broadband squeezing generation and detection at 1550 nm wavelength over a bandwidth of $\Delta\omega_{tel}/2\pi = 1.2$ GHz with a quantum efficiency of $\eta_{tel} = 0.53$, as shown in [49]. In this experiment, the authors also report a squeezing level of 3 dB, which we will use as a common level of vacuum squeezing for both the microwave and telecom regimes. We compute the corresponding crossover distance as a function

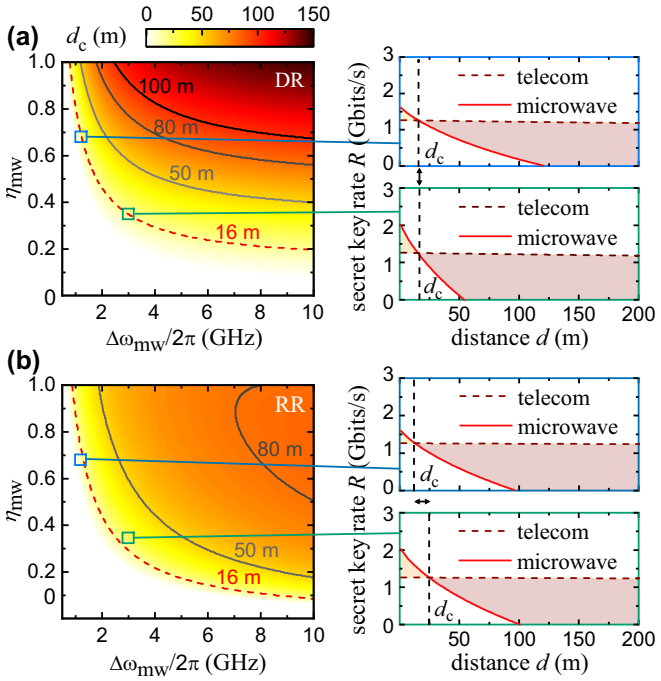


FIG. 5. Crossover distance $d_c$ between microwave and telecom CV-QKD. (a, b) The DR and RR cases, respectively. For the telecom and microwave wavelengths, we assume transmission losses $\gamma_{tel} \simeq 2.02 \times 10^{-1}$ dB/km and $\gamma_{mw} \simeq 6.3 \times 10^{-3}$ dB/km, respectively. For both DR and RR, the secret key rates $R$ of both detection cases are shown in the right column as a function of communication distance $d$. The top blue (bottom green) inset represents a comparison between microwave and telecom secret key rate for a quantum efficiency $\eta_{mw} = 0.695$ ($\eta_{mw} = 0.345$) and detection bandwidth $\Delta\omega_{mw}/2\pi = 1.2$ GHz ($\Delta\omega_{mw}/2\pi = 3.0$ GHz).

of the microwave detection bandwidth $\Delta\omega_{mw}/2\pi$ and quantum efficiency $\eta_{mw}$. The corresponding results are shown in Fig. 5 for both DR and RR. Interestingly, we observe that the microwave CV-QKD protocol can outperform the telecom counterpart for realistic values of $\Delta\omega_{mw}/2\pi$ and $\eta_{mw}$. A clear distinction can be seen between the two reconciliation cases. For the DR case, it is beneficial to aim at a quantum efficiency close to unity and large detection bandwidths. The situation is noticeably different in RR. For the latter, we observe that above a certain detection bandwidth the optimal quantum efficiency is no longer unity. Instead, there exists an optimal detection noise added by Bob, which maximizes the secret key rate depending on the detection bandwidth. The existence of an optimal quantum efficiency is a remarkable feature of RR, which arises when Bob couples additional noise during his measurements [50]. To illustrate the influence of the quantum efficiency and the detection bandwidth, we envision two different microwave homodyne detection cases implemented by a phase-sensitive amplifier. First, we choose a high detection bandwidth $\Delta\omega_{mw}/2\pi = 3$ GHz with a quantum efficiency of $\eta_{mw} = 0.345$. This case is motivated by the existing state-of-the-art superconducting TWPA devices operated in the phase-insensitive regime [51,52]. The second case considers a detection bandwidth of $\Delta\omega_{mw}/2\pi = 1.2\,\text{GHz} = \Delta\omega_{tel}/2\pi$, and we choose a quantum efficiency of $\eta_{mw} = 0.695$, such that both cases yield the same DR crossover distance. This

case originates from recent results on broadband squeezing in the microwave regime [53,54]. By using this set of already experimentally feasible parameters, we can reach a crossover distance of $d_c = 16$ m for both cases. For RR, we observe that the crossover distance can be increased to $d_c = 25$ m. The reason is that RR benefits from a quantum efficiency below unity. Remarkably, high secret key rates $R$ of a few Gbits per second can be reached for all of the previously mentioned sets of parameters. However, we stress that the computed secret key rates $R$ are merely upper bounds for realistically achievable rates. Existing telecom QKD implementations reach secure key rates up to a few Mbits per second [55–57]. Aside from finite quantum detection efficiencies and bandwidths, practical secret key rates are also limited by various factors such as actual experimental repetition rates [7], device-induced noise [56], finite size effects [25], or postprocessing [58]. Nevertheless, the demonstrated results make MQC relevant for short-distance classical communication protocols such as Wifi 802.11 standard (communication range $\simeq 70$ m), Bluetooth 5.0($\simeq$240 m), or more recent technologies such as 5G ($\simeq$305 m) because of matching frequency ranges, distances, and technological infrastructure.

## V. WEATHER INDUCED LOSS EFFECTS

### A. Nonoptimal weather conditions

So far, we have investigated open-air CV-QKD under ideal weather conditions. However, it is well known that realistic, nonoptimal weather conditions may drastically affect absorption losses for propagating signals. Such effects are especially prominent in the telecom frequency range. Therefore, it is natural to investigate effects of these nonoptimal conditions on the MQC as well. Specifically, we focus on two nonideal weather scenarios: rain and haze. In the context of microwave communication, the ITU-P. 838 and ITU-P. 840 recommendations provide empirical prediction models for the induced attenuation on propagating microwave signals due to rainfall and haze, respectively. More precisely, the specific attenuation $\gamma_{\mathrm{mw,r}}$ due to rain along a horizontal path can be expressed as [59]

$$\gamma_{\mathrm{mw,r}} = k(\omega)\, R_{\mathrm{r}}^{\alpha(\omega)}, \tag{17}$$

where $k$ and $\alpha$ are coefficients which depend on the communication microwave frequency $\omega/2\pi$, while $R_{\mathrm{r}}$ (mm/h) is the rain rate. The haze specific attenuation $\gamma_{\mathrm{h}}$ can be obtained from the liquid water concentration $M$ (g/cm$^3$) from a linear relationship as [60]

$$\gamma_{\mathrm{mw,h}} = K_{\mathrm{l}}(\omega, T)\, M, \tag{18}$$

where $K_{\mathrm{l}}$ (dB m$^2$/g) is the specific attenuation coefficient that depends on the considered microwave frequency $\omega/2\pi$ and water temperature $T$ in the atmosphere. The liquid water concentration can be related to a physically more intuitive quantity, the so-called visibility $V$ (km). The latter represents the distance at which the light intensity from an object drops to 2% of its initial value. For a nonpolluted environment, one can link two aforementioned quantities as [61]

$$M = \left(\frac{a}{V}\right)^b, \tag{19}$$

where $a = -\log(0.02)/99$ and $b = 0.92^{-1}$. For the telecom frequencies, rain causes a wavelength-independent attenuation. The specific attenuation $\gamma_{\mathrm{tel,r}}$ can be expressed for a horizontal path as [12]

$$\gamma_{\mathrm{tel,r}} = k\, R_{\mathrm{r}}^{\alpha}, \tag{20}$$

where $R_{\mathrm{r}}$ is the rain rate, $k = 1.076$, and $\alpha = 0.67$. The haze-specific attenuation is empirically derived similarly to the microwave case. Once again, visibility determines the specific attenuation $\gamma_{\mathrm{tel,r}}$. Empirical models for Mie scattering show that [12,62]

$$\gamma_{\lambda,\mathrm{h}} = \frac{C}{V}\left(\frac{\lambda}{550}\right)^{-p(V)}, \tag{21}$$

where $C = 39.1\,\log(e)$, $\lambda$ (nm) corresponds to a certain telecom wavelength, and $p$ is a scattering coefficient that depends on the considered visibility range and varies from 0 to 1.6 [12,62].

### B. Effects of weather conditions

In order to study the effect of nonoptimal weather conditions on the CV-QKD secure key rates, we consider two specific situations: (i) heavy (light) rain with the rain rate $R_{\mathrm{r}} = 7$ mm/h ($R_{\mathrm{r}} = 2$ mm/h) and (ii) (light) haze with a visibility ($V = 4$ km)$V = 1$ km. We compare the telecom and microwave secret key rates in Fig. 6. For the detection bandwidth and quantum efficiency, we stick to the previously analyzed set of parameters ($\Delta\omega_{\mathrm{tel}}/2\pi = 1.2$ GHz, $\eta_{\mathrm{tel}} = 0.53$ and $\Delta\omega_{\mathrm{mw}}/2\pi = 3$ GHz, $\eta_{\mathrm{mw}} = 0.345$). We find that short-distance microwave QKD could potentially yield a higher secret key rates telecom case. The reason is that microwave QKD benefits from higher experimental bandwidths and lower losses due to weather imperfections. We note that telecom QKD allows for secure communication over much larger distances, up to $d \simeq 140$ km using RR. These distances are significantly reduced when the effects of rain and haze are taken into account. For these weather conditions, the maximum secure telecom communication distances can be strongly reduced to $\simeq$300 m (7 km) and $\simeq$70 m (1.7 km), for DR (RR) respectively. Conversely, for microwave frequencies, the maximum secure communication distance is almost unchanged in both reconciliation cases compared to that obtained for optimal weather conditions, highlighting the robustness of microwave CV-QKD to weather effects. The most significant difference arises when considering the effect of light haze. Remarkably, haze induces little to no microwave losses. Even strong haze and fog only weakly disturb microwave signals by causing a small additional attenuation of around $1 \times 10^{-3}$ dB/km. The latter holds even when visibility is reduced to less than 500 m. In contrast, reducing the visibility below 1 km would generate large losses (more than $\approx$20 dB/km) for the telecom frequency, preventing the possibility of any relevant secure quantum communication. These results indicate that an ideal quantum open-air communication network could consist of a combination of microwave-based channels for short distances ($d \leqslant 200$ m) and telecom-based channels for long distances ($d > 200$ m).

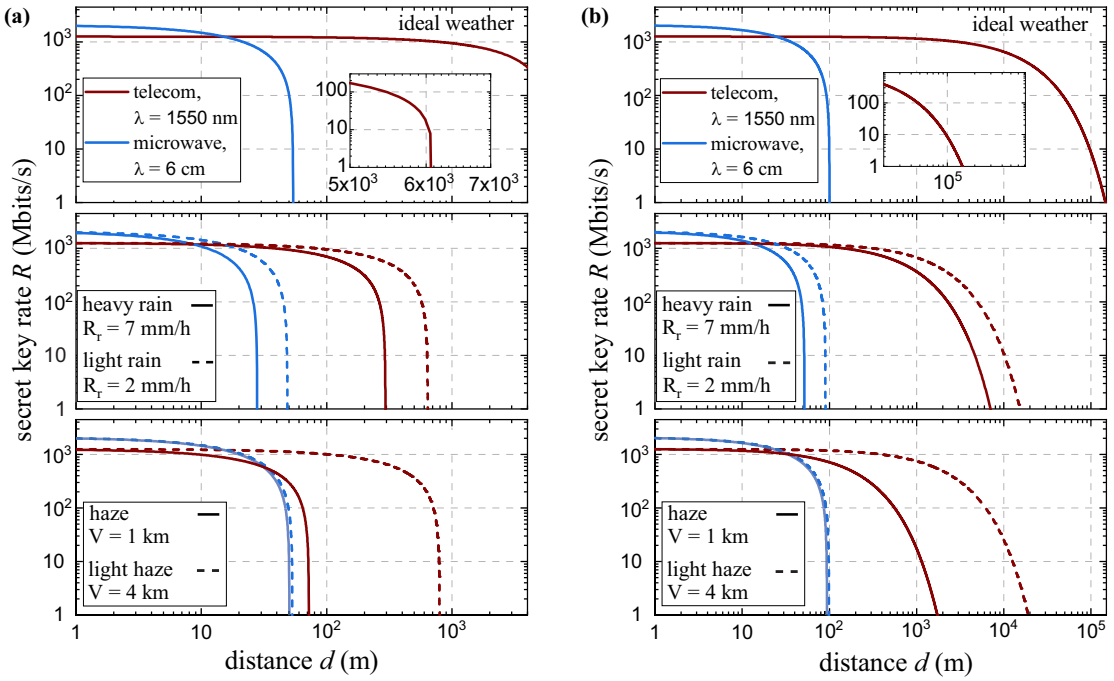


FIG. 6. Secret key rates of the CV-QKD protocol for various weather conditions. Telecom [brown, lower (solid and dashed) lines for distance $d = 1$] and microwave [blue, upper (solid and dashed) lines for distance $d = 1$] secret key rates $R$ are computed for DR in panel (a) and for RR in panel (b) as a function of the communication distance $d$ for the squeezing levels of $S_{\text{tel}} = S_{\text{mw}} = 3$ dB. The insets correspond to a zoom for the telecom secret key rates. Three different weather conditions are considered: ideal weather conditions (visibility of 23 km), heavy (light) rain with a rain rate of 7 mm/$h$ (2 mm/$h$), and (light) haze with a visibility of (1 km) 4 km. The choice of quantum efficiency and detection bandwidth is the same as for the ideal weather conditions. For the telecom case, we consider the total transmission losses $\gamma_{\text{tel}} \simeq 2.02 \times 10^{-1}$ dB/km (optimal), $\gamma_{\text{tel}} \simeq 4.17$ or 1.91 dB/km (heavy rain or light rain), and $\gamma_{\text{tel}} \simeq 17$ or $1.55 \times 10^{-2}$ dB/km (haze or light haze). For the microwave case, we assume the transmission losses $\gamma_{\text{mw}} \simeq 6.3 \times 10^{-3}$ dB/km (optimal), $\gamma_{\text{mw}} \simeq 1.22 \times 10^{-2}$ or $7 \times 10^{-3}$ dB/km (heavy rain or light rain), and $\gamma_{\text{mw}} \simeq 6.7 \times 10^{-3}$ or $6.4 \times 10^{-3}$ dB/km (haze or light haze).

## VI. CONCLUSION

In conclusion, we have performed a comprehensive analysis of microwave CV-QKD and demonstrate its potential for applications in open-air conditions. We have shown that quantum microwaves can yield positive secret key rates for short-distance communication for both DR and RR. Our calculations rely on empirical models for microwave and telecom atmospheric absorption losses. We have estimated the related microwave and telecom specific attenuation for optimal weather conditions to $6.3 \times 10^{-3}$ and $2.02 \times 10^{-1}$ dB/km, respectively. In our analysis, we have assumed microwave homodyne detection based on state-of-the-art TWPAs. Our model for the CV-QKD protocol predicts positive secret key rates for the microwave regime over distances of around 200 m. We have extended our analysis to include imperfect reconciliation and finite-size effects. Here, we have found that an imperfect reconciliation only marginally limits the communication distance and that finite-size effects can be overcome using a key length of $N \geqslant 10^6$. We have employed this model to compare the microwave and telecom cases for different detection quantum efficiencies and bandwidths. Our results show that, based on parameters of state-of-the-art technology, the microwave CV-QKD can potentially outperform the telecom implementations for short distances of around 30 m in terms of the secret key rates. From our analysis, it appears that both reconciliation scenarios are relevant. In particular, DR is favored for high quantum efficiencies, while RR allows for applications with rather lower detection quantum efficiencies $\eta$. The RR case also exhibits a nontrivial dependence of the secret key rate $R$ on $\eta$, which can be explained by the positive impact of detection noise on the protocol security.

Finally, we have considered the open-air CV-QKD protocol under nonideal weather conditions of rain and haze. We have found that these nonidealities strongly reduce the secure communication distance for the telecom regime, from 140 km to several hundred meters. Remarkably, the microwave open-air CV-QKD protocol appears to be largely immune to these weather imperfections with its secure communication distances staying mostly unchanged. We envision that our results could serve as a motivation for building first prototypes of secure microwave quantum local area networks. Our analysis also establishes the foundations for hybrid networks, where short-distance secure communication is carried out by microwave signals. Such hybrid network offer the advantage of providing potential high secret key rates and robustness to weather imperfections, while switching to telecom setups for long-distance communication. Short-distance MQC secure platforms could also complement current classical microwave communication technologies such as Wifi, Bluetooth, and 5G due to the intrinsic frequency and range compatibilities.

Numerical data that support the findings of this paper are available from the corresponding author upon reasonable request.


## ACKNOWLEDGMENTS

We acknowledge support by the German Research Foundation via Germany's Excellence Strategy (EXC-2111-390814868), the Elite Network of Bavaria through the program ExQM, the European Union Flagship project QMiCS (Grant No. 820505), the German Federal Ministry of Education and Research via the project QUARATE (Grant No. 13N15380), and the project QuaMToMe (Grant No. 16KISQ036). This research is part of the Munich Quantum Valley, which is supported by the Bavarian state government with funds from the Hightech Agenda Bayern Plus.

K.G.F. and F.D. suggested the idea of the paper. F.F. and K.G.F. developed the initial theory. F.K. and M.R. helped with the development of the final theory. Q.C., Y.N., and K.H contributed to sections of the manuscript dealing with experimental implementations. K.G.F., A.M., and R.G. supervised this work. F.F. and K.G.F. wrote the manuscript. All authors further contributed to discussions and proofreading of the manuscript.


## APPENDIX A: DESCRIPTION OF BOB'S AND EVE'S QUANTUM STATES

In this section, we provide details about the quantum states of Bob and Eve. To describe these states, we first need to consider the matrix representing the beam splitter operator:

$$\mathcal{B}(\tau) = \begin{pmatrix} \sqrt{\tau}\,\mathbf{I}_2 & \sqrt{1-\tau}\,\mathbf{I}_2 \\ -\sqrt{1-\tau}\,\mathbf{I}_2 & \sqrt{\tau}\,\mathbf{I}_2 \end{pmatrix}. \tag{A1}$$

Here, $\tau$ is the transmissivity associated with the beam splitter and $\mathbf{I}_2$ denotes the $2 \times 2$ identity matrix. Further, we introduce the direct sum for matrices $\mathbf{A}$ and $\mathbf{B}$ as

$$\mathbf{A} \oplus \mathbf{B} = \begin{pmatrix} \mathbf{A} & \mathbf{0} \\ \mathbf{0} & \mathbf{B} \end{pmatrix}. \tag{A2}$$

Since we assume all states in the protocol to be Gaussian, these states are characterized by their displacement vector $\hat{x}$ and covariance matrix $\mathbf{V}$ [7]. In this formalism, the displacement vector of an $N$-mode Gaussian state reads as

$$\hat{x} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N), \tag{A3}$$

where $\hat{q}_i$ and $\hat{p}_i$ are the conjugate quadrature operators of the $i$th mode. The displacement vector fulfills the commutation relation

$$[\hat{x}_i, \hat{x}_j] = \frac{i}{2}\mathbf{\Omega}_{ij}, \quad \mathbf{\Omega} = \bigoplus_{i=1}^{N} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{A4}$$

We use the expression $\bar{\mathbf{x}}$ to refer to the expectation value of the displacement vector, i.e.,

$$\bar{\mathbf{x}} = \langle \hat{x} \rangle. \tag{A5}$$

The elements of the covariance matrix of a mode are computed as

$$\mathbf{V}_{ij} = \langle \hat{x}_i \hat{x}_j + \hat{x}_i \hat{x}_j \rangle / 2 - \langle \hat{x}_i \rangle \langle \hat{x}_j \rangle. \tag{A6}$$

Using the previously introduced matrices in combination with Eq. (1), we can express the mean displacement vector of Bob's mode (Eve's mode) $\bar{\mathbf{x}}_B$ ($\bar{\mathbf{x}}_E$) as well as the covariance matrix of Bob's mode (Eve's mode) $\mathbf{V}_B$ ($\mathbf{V}_E$) as

$$\begin{aligned} (\bar{\mathbf{x}}_B, \bar{\mathbf{x}}_E)^T &= \mathbf{\Sigma}(\bar{\mathbf{x}}_0, \bar{\mathbf{x}}_{E,in})^T + \mathbf{\Sigma}_E(\bar{\mathbf{x}}_A, \bar{\mathbf{0}}_{E,in})^T, \\ \begin{pmatrix} \mathbf{V}_B & \mathbf{C}_{BE} \\ \mathbf{C}_{BE}^T & \mathbf{V}_E \end{pmatrix} &= \mathbf{\Sigma}(\mathbf{V}_0 \oplus \mathbf{V}_{E,in})\mathbf{\Sigma}^T, \end{aligned} \tag{A7}$$

with

$$\begin{aligned} \mathbf{\Sigma}_E &= \mathcal{B}(\tau_E) \oplus \mathbf{I}_2, \quad \mathbf{\Sigma}_A = \big(\mathbf{R}(\varphi/2)\,\mathbf{S}_{sq}(r)\big) \oplus \mathbf{I}_4, \\ \mathbf{\Sigma} &= \mathbf{\Sigma}_E\,\mathbf{\Sigma}_A. \end{aligned} \tag{A8}$$

Here, $\bar{\mathbf{x}}_0$ ($\mathbf{V}_0$) represents the mean displacement vector (covariance matrix) of the initial vacuum state. Furthermore, $\bar{\mathbf{x}}_A$ represents Alice's mean displacement vector, and $\bar{\mathbf{x}}_{E,in}$ represents Eve's initial mean displacement vector of her TMS state. Additionally, $r$ and $\varphi$ correspond to the squeezing factor and squeezing angle of the generated squeezed states by Alice, respectively. Correlations between Bob's and Eve's individual states are described by the submatrix $\mathbf{C}_{BE}$. Finally, $\mathbf{R}$ corresponds to a two-dimensional rotation matrix while $\mathbf{S}_{sq}$ is a $2 \times 2$ matrix, which we calculate as

$$\begin{aligned} &\mathbf{R}(\varphi/2)\,\mathbf{S}_{sq}(r) \\ &= \begin{pmatrix} \cos(\varphi/2) & \sin(\varphi/2) \\ -\sin(\varphi/2) & \cos(\varphi/2) \end{pmatrix} \begin{pmatrix} \exp(-r) & 0 \\ 0 & \exp(r) \end{pmatrix}. \end{aligned} \tag{A9}$$

Using Eq. (A7), the variance of Bob's states reads

$$\begin{aligned} \mathbf{V}_B &= \tau_E \mathbf{V}_A + (1-\tau_E)\tfrac{1}{4}(1+2n_{Eve})\mathbf{I}_2 \\ &= \tau_E \mathbf{V}_A + \big[\tfrac{1}{4}(1-\tau_E) + \bar{n}\big]\mathbf{I}_2, \end{aligned} \tag{A10}$$

where $\mathbf{V}_A$ represents Alice's state variance, while the covariance matrix of Eve's mode coupled to Alice's mode is given by $0.25(1+2n_{Eve})\mathbf{I}_2$. Lastly, we incorporate the noise of the amplification chain by using the following input-output formalism for a bosonic signal mode $\hat{a}$ [31]:

$$\hat{a}' = \sqrt{G}\,\hat{a} + \sqrt{G-1}\,\hat{h}_{amp}^{\dagger}. \tag{A11}$$

Here, $G$ is the gain of the amplification chain and $\hat{h}_{amp}$ is an environmental mode, modeled as a thermal state. For $G \gg 1$, this results in the final covariance matrix for Bob:

$$\mathbf{V}_B = \tau_E \mathbf{V}_A + \big[\tfrac{1}{4}(1-\tau_E) + \bar{n} + \bar{n}_g\big]\mathbf{I}_2. \tag{A12}$$

Here, $\bar{n}_g = \bar{n}_{amp}/2$ is the added quadrature noise from the amplification chain expressed in an average photon number. In the previous equation, the covariance matrix has been divided by the gain $G$ as this gain can always be determined from calibration measurements. In the third step, we compute the mutual information $I(A{:}B)$ using the expression

$$I(A{:}B) = h(B) - h(B|A), \tag{A13}$$

where $h$ denotes the differential entropy. Local measurements of Bob on individual states, which he receives during the

communication, are represented by a classical random variable $B|A$. Then, $B$ is a classical random variable representing Bob's overall measurements over all received states (i.e., representing Bob's final key estimation $\mathcal{K}' = \{k'_1, \ldots, k'_N\}$). From Eq. (A12), we derive the variance $\sigma^2_{\mathrm{B|A}}$ of the variable $B|A$ as

$$\sigma^2_{\mathrm{B|A}} = \tau_{\mathrm{E}}\,\sigma_{\mathrm{s}}^2 + (1-\tau_{\mathrm{E}})/4 + \bar{n} + n_{\mathrm{g}}. \tag{A14}$$

Then, by averaging over Bob's Gaussian codebook and from the relation $\sigma_{\mathrm{s}}^2 + \sigma_{\mathrm{A}}^2 = \sigma_{\mathrm{as}}^2$, we similarly obtain the variance $\sigma_{\mathrm{B}}^2$ of the variable $B$ as

$$\sigma_{\mathrm{B}}^2 = \tau_{\mathrm{E}}\,\sigma_{\mathrm{as}}^2 + (1-\tau_{\mathrm{E}})/4 + \bar{n} + n_{\mathrm{g}}. \tag{A15}$$

For a Gaussian random variable $X$ of variance $\sigma_X^2$, the differential entropy simplifies to

$$h(X) = \tfrac{1}{2}\log_2\left(2\pi\,\sigma_X^2\right). \tag{A16}$$

As a result, we write the mutual information in Eq. (A13) as

$$I(A{:}B) = \frac{1}{2}\log_2\left(\frac{\sigma_{\mathrm{B}}^2}{\sigma^2_{\mathrm{B|A}}}\right). \tag{A17}$$

Furthermore, to compute Eve's Holevo quantity for DR (denoted as $\chi_{\mathrm{E}}^{\blacktriangleright}$) and for RR (denoted as $\chi_{\mathrm{E}}^{\blacktriangleleft}$), we first start by finding Eve's average state. To this end, we introduce an integer $c \in \{0, 1\}$ describing the choice of Bob's measurement basis, $q$ or $p$. Note that, due to the sifting step, Bob's measurement basis matches Alice's encoding basis. Eve's average state reads as

$$\hat{\rho}_{\mathrm{avg,E}} = \sum_{c=0}^{1}\int_{-\infty}^{\infty} f_{\mathrm{A,C}}(k_i, c)\,\hat{\rho}_{\mathrm{E,A}}^{k_i}\,dk_i. \tag{A18}$$

Here, $\hat{\rho}_{\mathrm{E,A}}^{k_i}$ is the density matrix of an individual state obtained by Eve from the entangling cloner attack. The function $f_{\mathrm{A,C}}(k_i, c)$ is the joint probability density function describing the probability of Alice encoding a symbol $k_i$ in a measurement basis according to $c$. To this end, $C$ represents a binary random variable used to obtain $c$ with the same probability for both outcomes $[P(C=0) = P(C=1) = 1/2]$. Since $c$ is given by a discrete variable and $k_i$ is given by a continuous variable, we use a mixed joint probability density function which gives

$$\begin{aligned} f_{\mathrm{A,C}}(k_i, c) &= f_{\mathrm{A|C}}(k_i|c)p(C=c) \\ &= f_{\mathrm{A}}(k_i)p(C=c) \\ &= \frac{1}{\sqrt{2\pi\,\sigma_{\mathrm{A}}^2}}\exp\left(-\frac{k_i^2}{2\sigma_{\mathrm{A}}^2}\right)\frac{1}{2}. \end{aligned} \tag{A19}$$

Here, $f_{\mathrm{A}}$ is the probability density function of the random variable $A$ representing Alice's random choice for $k_i$. Additionally, $f_{\mathrm{A|C}}$ is the probability density function of a random variable $A|C$ representing Alice's random choice for $k_i$ conditioned on the value of $C$. Note that we use $f_{\mathrm{A|C}} = f_{\mathrm{A}}$, since Alice uses the same random variable to get $k_i$ independently of the value taken by $C$. From this description, we write Eve's Holevo quantity for DR as

$$\chi_{\mathrm{E}}^{\blacktriangleright} = S(\hat{\rho}_{\mathrm{avg,E}}) - \sum_{c=0}^{1}\frac{1}{2}\int_{-\infty}^{\infty} f_{\mathrm{A}}(k_i)\,S\left(\hat{\rho}_{\mathrm{E,A}}^{k_i}\right)dk_i, \tag{A20}$$

where $S$ is the von Neumann entropy. In order to compute $\chi_{\mathrm{E}}^{\blacktriangleleft}$, we need to compute the covariance matrix of Eve's mode after Bob has performed his measurement on either the $q$ or $p$ quadrature. Following [44], the covariance matrix of each individual mode of Eve after Bob's measurement is derived as

$$\mathbf{V}_{\mathrm{E,B}}^{k'_i} = \mathbf{V}_{\mathrm{avg,E}} - \frac{1}{\sigma_{\mathrm{B}}^2}\mathbf{C}_{\mathrm{EB}}\,\mathbf{\Pi}\,\mathbf{C}_{\mathrm{EB}}^{\mathrm{T}}, \tag{A21}$$

where $\sigma_{\mathrm{B}}^2 = \tau_{\mathrm{E}}\,e^{2r}/4 + \bar{n} + \bar{n}_{\mathrm{g}} + (1-\tau_{\mathrm{E}})/4$. Additionally, $\mathbf{\Pi} \in \{\mathbf{\Pi}_q, \mathbf{\Pi}_p\}$ is a projective measurement operator in phase space, meaning that

$$\begin{aligned} \mathbf{\Pi}_q &= \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} (q\text{-quadrature measured}), \\ \mathbf{\Pi}_p &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} (p\text{-quadrature measured}). \end{aligned} \tag{A22}$$

Finally, $\mathbf{C}_{\mathrm{EB}}$ represents the correlations between Eve's mode, which she used during her entangling cloner attack, and Bob's mode. One can derive that

$$\mathbf{C}_{\mathrm{EB}} = (C_1\,\mathbf{I}_2, C_2\,\boldsymbol{\sigma}_{\mathrm{z}})^{\mathrm{T}}, \tag{A23}$$

where $\boldsymbol{\sigma}_{\mathrm{z}}$ is the $Z$ Pauli matrix, and

$$\begin{aligned} C_1 &= -\sqrt{\tau_{\mathrm{E}}}\sqrt{1-\tau_{\mathrm{E}}}[e^{2r}/4 - \bar{n}_{\mathrm{tot}}], \\ C_2 &= \sqrt{1-\tau_{\mathrm{E}}}\sqrt{(\bar{n}_{\mathrm{tot}})^2 - 1}. \end{aligned} \tag{A24}$$

In the previous expression, we used the notation $\bar{n}_{\mathrm{tot}} = (\bar{n} + \bar{n}_{\mathrm{g}})/(1-\tau_{\mathrm{E}}) + 1/4$. Finally, for RR, one can express Eve's Holevo quantity as

$$\chi_{\mathrm{E}}^{\blacktriangleleft} = S(\hat{\rho}_{\mathrm{avg,E}}) - \sum_{c=0}^{1}\frac{1}{2}\int_{-\infty}^{\infty} f_{\mathrm{B}}(k'_i)\,S\left(\hat{\rho}_{\mathrm{E,B}}^{k'_i}\right)dk'_i. \tag{A25}$$

Here, $\hat{\rho}_{\mathrm{E,B}}^{k'_i}$ is the density matrix of Eve's individual mode, which she gets after Bob's individual measurement. Additionally, $f_{\mathrm{B}}$ is the probability density function of the random variable $B$. The corresponding covariance matrix of Eve's individual mode is then given by Eq. (A21).

## APPENDIX B: FINITE-SIZE EFFECTS

For any QKD protocols, Alice and Bob estimate the losses and coupled noise photon number of the quantum channel they use during their communication. In this section, we detail a possible approach in which Alice and Bob build a statistical estimator by publicly disclosing a part of length $m$ of their exchanged key. Using the disclosed data, they compute a square-root transmissivity estimator which can be constructed as

$$\hat{T}_E = \frac{\sum_{i=1}^{m}(k_i - \bar{\mathcal{K}})(k'_i - \bar{\mathcal{K}}')}{\sum_{i=1}^{m}(k_i - \bar{\mathcal{K}})^2}, \tag{B1}$$

where we defined

$$\bar{\mathcal{K}} = \sum_{i=1}^{m} k_i \quad \text{and} \quad \bar{\mathcal{K}}' = \sum_{i=1}^{m} k'_i. \tag{B2}$$

From this estimator, they define $\hat{\tau}_{\mathrm{E}} \coloneqq \hat{T}_{\mathrm{E}}^2$. This estimator is built so that $\langle\hat{\tau}_{\mathrm{E}}\rangle = \tau_{\mathrm{E}}$. As a next step, they define a total noise

photon number estimator [37]:

$$\hat{\bar{n}}_{\text{tot}} = \frac{1}{m}\sum_{i=1}^{m}(k_i' - \hat{T}_{\text{E}}\, k_i)^2, \tag{B3}$$

such that $\langle \hat{\bar{n}}_{\text{tot}} \rangle = \bar{n}_{\text{tot}} = \tau_{\text{E}}\,\sigma_s^2 + (1-\tau_{\text{E}})(1+2n_{\text{Eve}})/4 + \bar{n}_{\text{g}}$. Given a confidence parameter $w$, they compute worst-case unbiased estimators:

$$\hat{\tau}_{\text{E}}^{\star} \coloneqq \hat{\tau}_{\text{E}} - w\sqrt{\text{var}(\hat{\tau}_{\text{E}})} \simeq \hat{\tau}_{\text{E}} - 2w\sqrt{\left(\frac{\bar{n}_{\text{tot}}}{\sigma_{\text{A}}^2} + 2\tau_{\text{E}}\right)\frac{\tau_{\text{E}}}{m}},$$

$$\hat{\bar{n}}_{\text{tot}}^{\star} \coloneqq \bar{n}_{\text{tot}} + w\sqrt{\text{var}(\bar{n}_{\text{tot}})} \simeq \bar{n}_{\text{tot}} + w\sqrt{\frac{\bar{n}_{\text{tot}}^2}{8\,m}}. \tag{B4}$$

For random variables with a normal distribution, the confidence parameter $w$ reduces to

$$w = \sqrt{2}\,\text{erf}^{-1}(1-2\varepsilon_{\text{ec}}), \tag{B5}$$

with $\varepsilon_{\text{ec}}$ defined as an error probability which we set to $10^{-10}$, giving $w \simeq 6.34$. A coupled noise photon number unbiased estimator can be computed as

$$\hat{\bar{n}}^{\star} = \hat{\bar{n}}_{\text{tot}}^{\star} - \frac{(1-\hat{\tau}_{\text{E}}^{\star})}{4} - \bar{n}_{\text{g}} - \hat{\tau}_{\text{E}}^{\star}\,\sigma_{\text{s}}^2. \tag{B6}$$

Since a part of the secret key must be used for parameter estimation, Alice and Bob only exchange a key of finite size $n_{\text{ec}} = N - m$ at the end of the reconciliation step. For our analysis, we fix $n_{\text{ec}} = 0.9\,N$. The resulting secret key $K_{\text{exp}}$ from their communication is then bounded by the finite-size secret key $K_N$ [37]:

$$K_{\text{exp}} \geqslant K_N = \frac{n_{\text{ec}}\,p_{\text{ec}}}{N}\left(K(\hat{\tau}_{\text{E}}^{\star}, \hat{\bar{n}}^{\star}) - \frac{\Delta_{\text{fs}}}{\sqrt{n_{\text{ec}}}} + \frac{\Theta}{n_{\text{ec}}}\right), \tag{B7}$$

where the finite-size terms are defined as

$$\Delta_{\text{fs}} = 4\log_2(\sqrt{d}+2)\sqrt{\log_2\left(\frac{18}{p_{\text{ec}}^2\varepsilon_{\text{s}}^4}\right)},$$

$$\Theta = \log_2\left[p_{\text{ec}}\left(1 - \frac{\varepsilon_{\text{s}^2}}{3}\right)\right] + 2\log_2(\sqrt{2}\varepsilon_{\text{h}}). \tag{B8}$$

Here, the parameter $d$ represents the dimension of Alice's and Bob's effective codebook after the discretization during reconciliation of their respective data. We choose a typical value for CV-QKD protocols of $d = 2^5$ for a 5-bit discretization. The overall success of the protocol is then limited by a tolerance error for the security of the protocol, reflected in a smoothing parameter $\varepsilon_{\text{s}}$ and a hashing parameter $\varepsilon_{\text{h}}$. These parameters determine the total error of the privacy amplification step. Since they can be set to an arbitrary value, we use a conservative value of $\varepsilon_{\text{s}} = \varepsilon_{\text{h}} = 10^{-10}$. Lastly, we use a conservative and realistic success probability for the error correction of $p_{\text{ec}} = 0.9$.


[1] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields, Room temperature single-photon detectors for high bit rate quantum key distribution, Appl. Phys. Lett. **104**, 021101 (2014).

[2] T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, High key rate continuous-variable quantum key distribution with a real local oscillator, Opt. Express **26**, 2794 (2018).

[3] W. Diffie and M. Hellman, New directions in cryptography, IEEE Trans. Inf. Theory **22**, 644 (1976).

[4] R. L. Rivest, A. Shamir, and L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Commun. ACM **21**, 120 (1978).

[5] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[6] W. K. Wootters and W. H. Zurek, A single quantum cannot be cloned, Nature (London) **299**, 802 (1982).

[7] F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations, Adv. Quantum Technol. **1**, 1800011 (2018).

[8] J. Lodewyck, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, Controlling excess noise in fiber-optics continuous-variable quantum key distribution, Phys. Rev. A **72**, 050303(R) (2005).

[9] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Quantum key distribution using gaussian-modulated coherent states, Nature (London) **421**, 238 (2003).

[10] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, Daylight Quantum Key Distribution over 1.6 km, Phys. Rev. Lett. **84**, 5652 (2000).

[11] S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, J.-G. Ren, J. Yin, Q. Shen, Y. Cao, Z.-P. Li *et al.*, Satellite-to-ground quantum key distribution, Nature (London) **549**, 43 (2017).

[12] H. Kaushal, V. Jain, and S. Kar, *Free Space Optical Communication*, Vol. 7 (Springer, New York, 2018).

[13] F. Arute, K. Arya, R. Babbush, D. Bacon, J. C. Bardin, R. Barends, R. Biswas, S. Boixo, F. G. S. L. Brandao, D. A. Buell *et al.*, Quantum supremacy using a programmable superconducting processor, Nature (London) **574**, 505 (2019).

[14] M. Kjaergaard, M. E. Schwartz, J. Braumüller, P. Krantz, J. I. Wang, S. Gustavsson, and W. D. Oliver, Superconducting qubits: Current state of play, Annu. Rev. Condens. Matter Phys. **11**, 369 (2020).

[15] S. Pogorzalek, K. G. Fedorov, M. Xu, A. Parra-Rodriguez, M. Sanz, M. Fischer, E. Xie, K. Inomata, Y. Nakamura, E. Solano *et al.*, Secure quantum remote state preparation of squeezed microwave states, Nat. Commun. **10**, 2604 (2019).

[16] A. Bienfait, K. J. Satzinger, Y. P. Zhong, H.-S. Chang, M.-H. Chou, C. R. Conner, É. Dumur, J. Grebel, G. A. Peairs, R. G. Povey *et al.*, Phonon-mediated quantum state transfer and remote qubit entanglement, Science **364**, 368 (2019).

[17] M. Mirhosseini, A. Sipahigil, M. Kalaee, and O. Painter, Superconducting qubit to optical photon transduction, Nature (London) **588**, 599 (2020).

[18] L. Zhong, E. P. Menzel, R. Di Candia, P. Eder, M. Ihmig, A. Baust, M. Haeberlein, E. Hoffmann, K. Inomata, T. Yamamoto

*et al.*, Squeezing with a flux-driven Josephson parametric amplifier, New J. Phys. **15**, 125013 (2013).

[19] C. Eichler, Y. Salathe, J. Mlynek, S. Schmidt, and A. Wallraff, Quantum-Limited Amplification and Entanglement in Coupled Nonlinear Resonators, Phys. Rev. Lett. **113**, 110502 (2014).

[20] A. L. Grimsmo and A. Blais, Squeezing and quantum state engineering with Josephson travelling wave amplifiers, Npj Quantum Inf. **3**, 20 (2017).

[21] N. J. Cerf, M. Lévy, and G. Van Assche, Quantum distribution of Gaussian keys using squeezed states, Phys. Rev. A **63**, 052311 (2001).

[22] S. Pirandola, S. L. Braunstein, and S. Lloyd, Characterization of Collective Gaussian Attacks and Security of Coherent-State Quantum Cryptography, Phys. Rev. Lett. **101**, 200504 (2008).

[23] R. García-Patrón and N. J. Cerf, Unconditional Optimality of Gaussian Attacks Against Continuous-Variable Quantum Key Distribution, Phys. Rev. Lett. **97**, 190503 (2006).

[24] R. Renner and J. I. Cirac, De Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography, Phys. Rev. Lett. **102**, 110504 (2009).

[25] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of a continuous-variable quantum key distribution, Phys. Rev. A **81**, 062343 (2010).

[26] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables, Quantum Info. Comput. **3**, 535 (2003).

[27] K. G. Fedorov, S. Pogorzalek, U. Las Heras, M. Sanz, P. Yard, P. Eder, M. Fischer, J. Goetz, E. Xie, K. Inomata *et al.*, Finite-time quantum entanglement in propagating squeezed microwaves, Sci. Rep. **8**, 6416 (2018).

[28] K. G. Fedorov, L. Zhong, S. Pogorzalek, P. Eder, M. Fischer, J. Goetz, E. Xie, F. Wulschner, K. Inomata, T. Yamamoto *et al.*, Displacement of Propagating Squeezed Microwave States, Phys. Rev. Lett. **117**, 020502 (2016).

[29] T. Yamamoto, K. Inomata, M. Watanabe, K. Matsuba, T. Miyazaki, W. D. Oliver, Y. Nakamura, and J. S. Tsai, Flux-driven Josephson parametric amplifier, Appl. Phys. Lett. **93**, 042510 (2008).

[30] B. Yurke, L. R. Corruccini, P. G. Kaminsky, L. W. Rupp, A. D. Smith, A. H. Silver, R. W. Simon, and E. A. Whittaker, Observation of parametric amplification and deamplification in a Josephson parametric amplifier, Phys. Rev. A **39**, 2519 (1989).

[31] C. M. Caves, Quantum limits on noise in linear amplifiers, Phys. Rev. D **26**, 1817 (1982).

[32] M. Renger, S. Pogorzalek, Q. Chen, Y. Nojiri, K. Inomata, Y. Nakamura, M. Partanen, A. Marx, R. Gross, F. Deppe *et al.*, Beyond the standard quantum limit for parametric amplification of broadband signals, Npj Quantum Inf. **7**, 160 (2021).

[33] K. G. Fedorov, M. Renger, S. Pogorzalek, R. D. Candia, Q. Chen, Y. Nojiri, K. Inomata, Y. Nakamura, M. Partanen, A. Marx *et al.*, Experimental quantum teleportation of propagating microwaves, Sci. Adv. **7**, eabk0891 (2021).

[34] S. Boutin, D. M. Toyli, A. V. Venkatramani, A. W. Eddins, I. Siddiqi, and A. Blais, Effect of Higher-Order Nonlinearities on Amplification and Squeezing in Josephson Parametric Amplifiers, Phys. Rev. Appl. **8**, 054030 (2017).

[35] D. M. Pozar, *Microwave Engineering*, 4th ed. (Wiley, Hoboken, 2011).

[36] T. Gonzalez-Raya and M. Sanz, Coplanar antenna design for microwave entangled signals propagating in open air, Quantum **6**, 783 (2022).

[37] S. Pirandola, Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks, Phys. Rev. Res. **3**, 043014 (2021).

[38] M. A. Castellanos-Beltran, K. D. Irwin, G. C. Hilton, L. R. Vale, and K. W. Lehnert, Amplification and squeezing of quantum noise with a tunable Josephson metamaterial, Nat. Phys. **4**, 929 (2008).

[39] C. Eichler, D. Bozyigit, and A. Wallraff, Characterizing quantum microwave radiation and its entanglement with superconducting qubits using linear detectors, Phys. Rev. A **86**, 032106 (2012).

[40] C. M. Ho, C. Wang, K. Angkasa, and K. Gritton, Estimation of microwave power margin losses due to earth's atmosphere and weather in the frequency range of 3–30 GHz, Jet Propulsion Laboratory (2004).

[41] A. S. Holevo, Bounds for the quantity of information transmitted by a quantum communication channel, Probl. Inf. Transm. **9**, 177 (1973).

[42] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks, Phys. Rev. A **97**, 052327 (2018).

[43] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. **88**, 057902 (2002).

[44] C. Weedbrook, S. Pirandola, and T. C. Ralph, Continuous-variable quantum key distribution using thermal states, Phys. Rev. A **86**, 022318 (2012).

[45] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[46] J. Lin, T. Upadhyaya, and N. Lütkenhaus, Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution, Phys. Rev. X **9**, 041064 (2019).

[47] W.-B. Liu, C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, X.-Y. Cao, Y.-S. Lu, B.-H. Li, H.-L. Yin, and Z.-B. Chen, Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance, PRX Quantum **2**, 040334 (2021).

[48] H. Nyquist, Certain topics in telegraph transmission theory, Trans. Am. Inst. Electr. Eng. **47**, 617 (1928).

[49] S. Ast, M. Mehmet, and R. Schnabel, High-bandwidth squeezed light at 1550 nm from a compact monolithic PPKTP cavity, Opt. Express **21**, 13572 (2013).

[50] R. García-Patrón and N. J. Cerf, Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels, Phys. Rev. Lett. **102**, 130501 (2009).

[51] C. Macklin, K. O'Brien, D. Hover, M. E. Schwartz, V. Bolkhovsky, X. Zhang, W. D. Oliver, and I. Siddiqi, A near-quantum-limited Josephson traveling-wave parametric amplifier, Science **350**, 307 (2015).

[52] M. Perelshtein, K. Petrovnin, V. Vesterinen, S. H. Raja, I. Lilja, M. Will, A. Savin, S. Simbierowicz, R. Jabdaraghi, J. Lehtinen *et al.*, Broadband continuous variable entanglement generation using Kerr-free Josephson metamaterial, arXiv:2111.06145.

[53] B. H. Schneider, A. Bengtsson, I. M. Svensson, T. Aref, G. Johansson, J. Bylander, and P. Delsing, Observation of

Broadband Entanglement in Microwave Radiation from a Single Time-Varying Boundary Condition, Phys. Rev. Lett. **124**, 140503 (2020).

[54] J. Y. Qiu, A. Grimsmo, K. Peng, B. Kannan, B. Lienhard, Y. Sung, P. Krantz, V. Bolkhovsky, G. Calusine, D. Kim *et al.*, Broadband squeezed microwaves and amplification with a Josephson travelling-wave parametric amplifier, Nat. Phys. **19**, 706 (2023).

[55] D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng, Continuous-variable quantum key distribution with 1 Mbps secure key rate, Opt. Express **23**, 17511 (2015).

[56] X. Tang, R. Kumar, S. Ren, A. Wonfor, R. Penty, and I. White, Performance of continuous variable quantum key distribution system at different detector bandwidth, Opt. Commun. **471**, 126034 (2020).

[57] S. Sarmiento, S. Etcheverry, J. Aldama, I. H. López, L. T. Vidarte, G. B. Xavier, D. A. Nolan, J. S. Stone, M. J. Li, D. Loeber *et al.*, Continuous-variable quantum key distribution over 15 km multi-core fiber, New J. Phys. **24**, 063011 (2022).

[58] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Quantum key distribution over 25 km with an all-fiber continuous-variable system, Phys. Rev. A **76**, 042305 (2007).

[59] S. Shrestha and D.-Y. Choi, Rain Attenuation study over an 18 GHz terrestrial microwave link in South Korea, Int. J. Antennas Propag **2019**, 1 (2019).

[60] Z. Zhao and Z. Wu, Millimeter-wave attenuation due to fog and clouds, J. Infrared Millim. Terahertz Waves **21**, 1607 (2000).

[61] J. Fišák, D. Řezáčová, and J. Mattanen, Calculated and measured values of liquid water content in clean and polluted environments, Stud. Geophys. Geod **50**, 121 (2006).

[62] I. I. Kim, B. McArthur, and E. J. Korevaar, Comparison of laser beam propagation at 785 nm and 1550 nm in fog and haze for optical wireless communications, Proc. SPIE **4214**, 417512 (2001).