

ACCEPTED MANUSCRIPT

Two-Way Continuous-Variable Quantum Key Distribution in Fast-Fading Channels

To cite this article before publication: Yayou Zou *et al* 2026 *Phys. Scr.* in press <https://doi.org/10.1088/1402-4896/aeb051>

Manuscript version: Accepted Manuscript

Accepted Manuscript is “the version of the article accepted for publication including all changes made as a result of the peer review process, and which may also include the addition to the article by IOP Publishing of a header, an article ID, a cover sheet and/or an ‘Accepted Manuscript’ watermark, but excluding any other editing, typesetting or other changes made by IOP Publishing and/or its licensors”

This Accepted Manuscript is © 2026 IOP Publishing Ltd. All rights, including for text and data mining, AI training, and similar technologies, are reserved..



During the embargo period (the 12 month period from the publication of the Version of Record of this article), the Accepted Manuscript is fully protected by copyright and cannot be reused or reposted elsewhere.

As the Version of Record of this article is going to be / has been published on a subscription basis, this Accepted Manuscript will be available for reuse under a CC BY-NC-ND 4.0 licence after the 12 month embargo period.

After the embargo period, everyone is permitted to use copy and redistribute this article for non-commercial purposes only, provided that they adhere to all the terms of the licence <https://creativecommons.org/licenses/by-nc-nd/4.0>

Although reasonable endeavours have been taken to obtain all necessary permissions from third parties to include their copyrighted content within this article, their full citation and copyright line may not be present in this Accepted Manuscript version. Before using any content from this article, please refer to the Version of Record on IOPscience once published for full citation and copyright details, as permissions may be required. All third party content is fully copyright protected, unless specifically stated otherwise in the figure caption in the Version of Record.

View the [article online](#) for updates and enhancements.

Two-Way Continuous-Variable Quantum Key Distribution in Fast-Fading Channels

Yayou Zou,¹ Jian Zhou^{1,*}, Weimin Yang,¹ and Guangqiang He²

¹College of Computer and Mathematics, Central South University of Forestry
and Technology, Changsha, Hunan 410004, People's Republic of China

²State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of
Electronic Engineering, Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China

(Dated: September 17, 2026)

This paper presents a theoretical benchmark analysis of selected two-way continuous-variable quantum key distribution (CV-QKD) protocols over fast-fading channels. For uniformly fluctuating transmissivity, a non-CSI benchmark treatment evaluates the mutual information term at the worst transmissivity and averages Eve's information over the fading distribution. Closed-form asymptotic key-rate formulas are derived for specific two-way protocols in the large-modulation regime. The framework also applies to CSI-enabled averaging and truncated log-normal weak-turbulence fading. Numerical results show that, within the adopted ideal asymptotic setting, the evaluated two-way RoR² benchmark retains a broader positive-key-rate region than the corresponding one-way RoR benchmark under uniform non-CSI fading. CSI-enabled averaging and the weak-turbulence extension further characterize the behavior of the selected two-way benchmarks under different channel-knowledge and fading conditions. Overall, these results characterize the performance of the selected two-way protocols across the adopted fast-fading benchmark settings.

I. INTRODUCTION

Quantum key distribution (QKD) [1–3] allows two remote users to establish shared secret keys by transmitting quantum states and exploiting measurement-induced disturbance to detect eavesdropping. Eavesdropping is assessed through parameter estimation, usually including channel transmissivity and excess noise [2, 4]. Recent advances have extended QKD to long-distance optical-fiber and free-space links, including satellite-to-ground continuous-variable QKD [5]. Secure key distribution has been demonstrated over distances of hundreds of kilometers using fiber optics [6, 7] and even over thousands of kilometers using satellite-based quantum communication [8]. Recent free-space quantum communication studies further identify diffraction, atmospheric extinction, turbulence, pointing errors, background noise, and trust assumptions as important factors in realistic security analyses [9–11]. Atmospheric fluctuations in free-space links introduce channel variability and motivate the fast-fading analysis developed below.

QKD protocols are generally divided into discrete-variable QKD (DV-QKD) and continuous-variable QKD (CV-QKD). CV-QKD achieves competitive key rates over urban-area distances through coherent detection and is compatible with standard communication devices and receiver architectures [12–14]. In CV-QKD, two-way schemes employ a round-trip channel configuration and can improve loss and noise tolerance relative to one-way schemes [15, 16]. This motivates examining whether the advantage of the two-way architecture persists under rapidly fluctuating transmissivity when instantaneous channel knowledge is unavailable [17].

Fixed-channel analyses of two-way CV-QKD usually

assume static or slowly varying transmissivity, whereas free-space atmospheric turbulence causes rapid and random transmissivity fluctuations. These channel dynamics can lead to fast-fading effects and increased channel uncertainty [18–23]. It is difficult under these conditions to obtain accurate instantaneous channel state information (CSI).

In the present setting, two-way CV-QKD is studied over fast-fading channels when legitimate parties lack instantaneous CSI. To examine this regime, the non-CSI fast-fading treatment is applied to the established fixed-transmissivity two-way CV-QKD key-rate formulations, yielding closed-form asymptotic benchmark expressions for selected two-way protocols. The obtained results characterize the performance of these protocols within the considered fast-fading benchmark framework. Applying the non-CSI fast-fading treatment to the established fixed-transmissivity formulations extends the benchmark analysis to fluctuating channels while retaining the underlying two-way security model and the fast-fading prescription from previous studies.

The remainder of this paper is organized as follows. Section II reviews the fixed-transmissivity two-way protocol and the fading models and eavesdropping models used as background. Section III incorporates the non-CSI fast-fading treatment into the two-way protocol and formulates the corresponding key-rate criterion. Section IV derives the secret key rate. Section V presents numerical results, and Section VI concludes the paper.

II. BACKGROUND MODELS

A. Fixed-Transmissivity Two-Way Protocol

Protocols for continuous-variable quantum key distribution (CV-QKD) are commonly formulated in the prepare-and-measure (PM) framework [24]. Two-way

* 13142153489@163.com

CV-QKD uses a round-trip configuration of the quantum channel, a feature that can improve noise tolerance and security thresholds relative to one-way schemes. The present setting follows the representative two-way protocol introduced in Ref. [15]. The entanglement-based (EB) representation is adopted for security analysis, being mathematically equivalent to the prepare-and-measure (PM) description.

The static two-way model treats the forward and backward transmissions as two sequential uses of a thermal-loss channel with the same transmissivity T .

Bob first prepares a zero-mean two-mode squeezed vacuum (TMSV) state (B_1, B_2) with variance μ . Its covariance matrix (CM) is

$$V_{B_1 B_2} = \begin{pmatrix} \mu \mathbb{I} & \sqrt{\mu^2 - 1} \sigma_z \\ \sqrt{\mu^2 - 1} \sigma_z & \mu \mathbb{I} \end{pmatrix}, \quad (1)$$

where $\mathbb{I} = \text{diag}(1, 1)$ and $\sigma_z = \text{diag}(1, -1)$. Bob keeps mode B_1 and measures it via heterodyne or homodyne detection [25]. The other mode B_2 goes to Alice through the forward thermal-loss channel with transmissivity T ; the received mode is B'_2 .

Alice encodes her classical variable on B'_2 by mixing it with the mode A_2 of a local auxiliary EPR state at the modulation beam splitter in the EB representation [26]. The beam-splitter transmissivity is denoted by η , distinct from the channel transmissivity T , and the output modes are

$$\begin{aligned} C_1 &= -\sqrt{1-\eta} B'_2 + \sqrt{\eta} A_2, \\ C_2 &= \sqrt{\eta} B'_2 + \sqrt{1-\eta} A_2. \end{aligned} \quad (2)$$

Alice performs heterodyne detection on the retained auxiliary mode A_1 ; this measurement outcome is the displacement variable in the PM picture via the EB-PM equivalence [26]. In the EB representation, the displacement-modulation limit is obtained by taking the modulation beam splitter to be highly transmissive, $\eta \rightarrow 1$, together with a correspondingly large auxiliary EPR variance. From Eq. (2), the coefficient of the incoming mode B'_2 approaches unity, $\sqrt{\eta} \rightarrow 1$, while the weakly coupled auxiliary contribution $\sqrt{1-\eta} A_2$ provides the Gaussian displacement in the equivalent PM description.

Output mode C_2 then returns through the backward channel and becomes C'_2 . Bob heterodynes C'_2 and obtains the raw data for classical post-processing. In the asymptotic security model adopted here, channel loss and injected noise are attributed to Eve, and Eve is assumed to hold a purification of the joint state shared by Alice and Bob [27].

This fixed-transmissivity description serves as the protocol-level baseline. The next subsection recalls the fading and Gaussian-attack models, which are later incorporated into this two-way structure in Sec. III.

B. Fading and Gaussian Attack Models

Atmospheric turbulence induces fluctuations in the transmissivity of free-space optical links [19]; hence the channel transmissivity often appears as a random parameter. Uniformly distributed transmissivity has been considered as a benchmark model in previous studies of fading CV-QKD channels [20, 28]. This uniform-transmissivity model was subsequently discussed and contrasted with a physically derived satellite fading distribution by Dequal *et al.* [5]. Accordingly, the uniform distribution is adopted here as a controlled theoretical benchmark. Its bounded support permits a transparent comparison among different protocols and allows the influence of rapid transmissivity fluctuations to be isolated before considering the more physically motivated truncated log-normal weak-turbulence model. Previous fast-fading CV-QKD analyses adopt a benchmark prescription in which the legitimate-party correlation is evaluated at a worst-case transmissivity, while Eve's information is averaged over the fading distribution.

The fading distribution specifies how the channel transmissivity T varies, whereas the security analysis additionally requires a model of Eve's interaction for each instantaneous channel realization. For Gaussian-modulated protocols, the states and correlations resulting from this interaction can be characterized by covariance matrices. Collective-attack reductions provide a standard asymptotic security framework for QKD [29]. Under a fixed covariance-matrix constraint, the Gaussian optimality theorem allows Gaussian attacks to be used to upper-bound Eve's Holevo information [30, 31]. Collective Gaussian attacks are therefore adopted here as benchmark attack models for the asymptotic analysis.

In the two-way architecture, Eve may interact with both the forward and backward transmissions. For the fixed-transmissivity benchmark formulas used below, the independent one-mode Gaussian-attack model of Ref. [15] is adopted, in which each channel use is attacked by a separate entangling cloner. Correlated two-mode attacks between the two channel uses are not included in the present benchmark analysis.

The entangling-cloner representation is adopted to describe Eve's interaction with the two channel uses [15]. Eve injects ancillary modes E_1 and E_2 into the forward and backward paths, respectively. For each channel use, E_i is one mode of an EPR pair with variance W , while the corresponding idler mode E''_i is retained by Eve. After the beam-splitter interaction, the ancillary output is denoted by E'_i , and Eve may retain both E'_i and E''_i for a subsequent collective measurement. For the independent one-mode Gaussian-attack benchmark considered here, the injected modes E_1 and E_2 are initially uncorrelated, while each E_i remains correlated with its retained idler E''_i .

These fading and eavesdropping assumptions are used in the non-CSI fast-fading formulation of the following section. Their covariance-matrix representation is introduced in Sec. IV-A.

III. NON-CSI FAST-FADING TREATMENT FOR THE TWO-WAY PROTOCOL

A. Integration of Fast Fading into the Two-Way Protocol

This subsection specifies the assumptions required to incorporate fast fading into the fixed-transmissivity two-way protocol described in Sec. II-A. In the non-CSI setting considered here, the legitimate parties cannot access the instantaneous channel realization for each round trip and can only estimate the transmissivity distribution $p(T)$ [20]. In practice, CSI requires sufficiently accurate and timely estimation or tracking of the instantaneous transmissivity. When such information is available, it can be used for each channel realization before averaging the resulting key-rate contribution over $p(T)$; otherwise, the non-CSI evaluation relies only on the fading statistics. Channel randomness is therefore incorporated by treating the transmissivity of each round trip as a random variable drawn from the distribution $p(T)$. Under the non-CSI assumption, the benchmark prescription summarized in Sec. II-B is applied using the transmissivity distribution $p(T)$.

The analysis is performed in the large-modulation asymptotic regime, with the modulation variance taken to the limit $V \rightarrow \infty$. This limit enables the closed-form asymptotic key-rate expressions derived below. The restriction of these expressions to ideal reconciliation, $\beta = 1$, is discussed in Sec. IV-A.

Atmospheric-channel reciprocity provides the basis for relating the forward and backward propagation paths [32], while the influence of temporal delay on this reciprocity has been analyzed in Ref. [33]. Accordingly, the propagation time of a single round trip is assumed to be shorter than the characteristic evolution time of atmospheric turbulence, so that the channel can be treated as approximately quasi-static over one round trip. Under this condition, the shared-transmissivity approximation is adopted

$$T_1^{(i)} \simeq T_2^{(i)} = T^{(i)}. \quad (3)$$

The shared realization applies only within a single round trip; across successive round trips, $T^{(i)}$ varies according to $p(T)$.

Irreducible two-mode attacks associated with channel memory may require additional countermeasures, such as ON/OFF switching. These mechanisms are not included in the primary fast-fading analytical model and remain for future theoretical extensions.

The resulting fast-fading channel model is illustrated in Fig. 1.

The next subsection presents the integrated protocol and specifies how fast-fading randomness enters the key-rate expression.

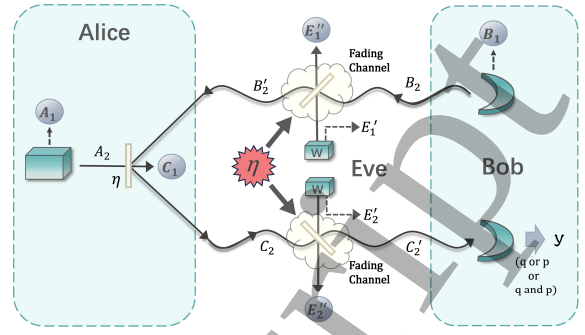


Figure 1. Two-way CV-QKD over a fast-fading channel. Both forward and backward transmissions experience fading. In the present model, a single round trip satisfies $T_1^{(i)} \simeq T_2^{(i)} = T^{(i)}$, while $T^{(i)}$ varies across round trips according to $p(T)$.

B. Two-Way Fast-Fading Protocol and Key-Rate Formulation

The fixed-transmissivity two-way protocol described in Sec. II-A is adopted under the non-CSI and shared-transmissivity assumptions established above. Alice's encoded variable X_A and Bob's decoding variable X_B form the correlated raw data used for reconciliation. For homodyne detection, the corresponding quadrature variables are correlated, whereas for heterodyne detection the two-dimensional variables $X_A = \{Q_A, P_A\}$ and $X_B = \{Q_B, P_B\}$ are used. Across successive round trips, the transmissivity $T^{(i)}$ varies according to $p(T)$, and the legitimate parties rely on this statistical distribution rather than on individual instantaneous realizations.

The asymptotic secret-key rate under fast fading combines the mutual-information term I_{AB} and Eve's corresponding Holevo information χ_E [13, 34]. Here, I_{AB} denotes the mutual-information term for a chosen modulation and detection scheme and reconciliation direction, while χ_E denotes Eve's Holevo information under the Gaussian attack model considered in Sec. II. Fast fading imposes an asymmetric treatment of these two terms [20, 27]. The term I_{AB} is evaluated at the worst-case transmissivity $T_{\min}$, whereas $\chi_E(T)$ is evaluated for each instantaneous transmissivity and then averaged over the fading distribution. The resulting fast-fading secret-key rate, denoted by K_{ff} , is therefore written as

$$K_{\text{ff}} = \beta I_{AB}(T_{\min}) - \int_{T_{\min}}^{T_{\max}} p(T) \chi_E(T) dT. \quad (4)$$

Here, β is the reconciliation efficiency, and $[T_{\min}, T_{\max}]$ denotes the support interval of the channel transmissivity. In Eq. (4), $\chi_E(T)$ is evaluated for each instantaneous transmissivity within the support of $p(T)$ and then averaged over the fading distribution. The averaged quantity $\int p(T) \chi_E(T) dT$ is not generally a worst-case upper bound on Eve's information for every individual fading realization. Accordingly, Eq. (4) provides an asymptotic distribution-level benchmark under the adopted fading statistics and Gaussian-attack model.

For the uniform fast-fading model, the probability density is

$$p(T) = \frac{1}{T_{\max} - T_{\min}}, \quad T \in [T_{\min}, T_{\max}]. \quad (5)$$

For later use, the notation $\Delta T := T_{\max} - T_{\min}$ is introduced, so that $T_{\max} = T_{\min} + \Delta T$. Only intervals satisfying $T_{\min} + \Delta T \leq 1$ are used, so that the sampled transmissivity remains within the physical range $0 < T \leq 1$.

This subsection completes the formulation of the two-way fast-fading model. The next section derives explicit expressions for $I_{AB}(T_{\min})$ and $\chi_E(T)$ from the two-way protocol and the one-mode Gaussian-attack model implemented by independent entangling cloners introduced in Sec. II. The shared-transmissivity condition in Eq. (3) and the benchmark key-rate prescription in Eq. (4) are then used to obtain the key-rate expressions for the subsequent numerical comparisons.

IV. SECURITY ANALYSIS AND KEY RATE

In this section, the covariance matrices required for the security analysis are derived from the eavesdropping model introduced in Sec. II. The selected benchmark set includes both direct-reconciliation (DR) and reverse-reconciliation (RR) cases under the asymptotic assumptions specified below.

A. Asymptotic Regime and Covariance-Matrix Formalism

The analysis is conducted in the entanglement-based (EB) representation. The EB variances are assumed to approach infinity ($V_A = V_B \rightarrow \infty$) in accordance with the large-modulation setting introduced in Sec. III-A, alongside the assumption of ideal reconciliation ($\beta = 1$). For compactness, the common asymptotic variance is denoted by V , i.e., $V_A = V_B \equiv V$. The large-modulation limit and ideal reconciliation are mathematically coupled in the present asymptotic derivation. For the protocols considered here, the large-modulation limit is used to extract the leading contributions in the key-rate expressions. Following the standard large-modulation treatment adopted in asymptotic CV-QKD analyses [15], the mutual-information and Eve-information terms exhibit the same leading large-modulation behavior. Under ideal reconciliation efficiency $\beta = 1$, the corresponding leading contributions cancel, yielding the finite asymptotic closed-form expressions used below. For $\beta < 1$, this cancellation is incomplete, and the key rate should be evaluated with a finite modulation variance and the corresponding reconciliation efficiency, as both parameters affect the contributions from the mutual information and Eve's information. Accordingly, all key rates, cut-off thresholds, and protocol comparisons reported in this work are restricted to the ideal $V \rightarrow \infty$, $\beta = 1$ benchmark.

For a fixed instantaneous transmissivity T , the interaction between an input signal mode $\hat{a}_{\text{in}}$ and Eve's ancillary mode $\hat{e}_{\text{in}} \in \{E_1, E_2\}$ is represented by the beam-splitter transformation [15]

$$\hat{a}_{\text{out}} = \sqrt{T} \hat{a}_{\text{in}} + \sqrt{1-T} \hat{e}_{\text{in}}. \quad (6)$$

For the independent one-mode Gaussian-attack benchmark introduced in Sec. II-B, the injected modes E_1 and E_2 are initially uncorrelated thermal modes with variance W . Their reduced input covariance matrix is

$$V_{E_1 E_2} = \begin{pmatrix} W\mathbb{I} & \mathbf{0} \\ \mathbf{0} & W\mathbb{I} \end{pmatrix}. \quad (7)$$

Here, $W \geq 1$ is Eve's ancillary thermal-state variance and $\mathbb{I}$ is the 2×2 identity matrix. Each injected mode E_i is purified by the corresponding idler E_i'' retained by Eve and remains correlated with it through the covariance term $\sqrt{W^2 - 1} \sigma_z$.

Bob's EPR variance is denoted by V_B [35]. In the quadrature-space covariance-matrix representation, the same forward signal-ancilla interaction is described by the symplectic transformation

$$S_{\text{fwd}}(T) = \begin{pmatrix} \sqrt{T} \mathbb{I}_2 & \sqrt{1-T} \mathbb{I}_2 \\ -\sqrt{1-T} \mathbb{I}_2 & \sqrt{T} \mathbb{I}_2 \end{pmatrix}. \quad (8)$$

The backward interaction within the same round trip follows the shared-transmissivity condition in Eq. (3) and is therefore described by the same symplectic transformation,

$$S_{\text{bwd}}(T) = S_{\text{fwd}}(T). \quad (9)$$

This two-way evolution determines the covariance matrices required for the subsequent security analysis at each fixed realization T . Under the adopted one-mode Gaussian-attack model, the two entangling cloners are independent at the input stage, while the sequential propagation of the signal through the forward and backward channel uses can generate correlations among Eve's output modes. These correlations are retained in the covariance-matrix description below. The system adopts the mode ordering $(E'_1, E''_1, E'_2, E''_2)$, where E'_i designates the output ancillary mode after the beam-splitter interaction and E''_i denotes the retained idler mode. The output covariance matrix of Eve's modes takes the form

$$\gamma_E^{\text{out}}(T) := \begin{pmatrix} \epsilon \mathbb{I}_2 & \phi \sigma_z & \chi \mathbb{I}_2 & \mathbf{0} \\ \phi \sigma_z & W \mathbb{I}_2 & \theta \sigma_z & \mathbf{0} \\ \chi \mathbb{I}_2 & \theta \sigma_z & \gamma \mathbb{I}_2 & \phi \sigma_z \\ \mathbf{0} & \mathbf{0} & \phi \sigma_z & W \mathbb{I}_2 \end{pmatrix}, \quad (10)$$

where

$$\epsilon := (1-T)V_B + TW, \quad (11)$$

$$\chi := -\sqrt{T(1-T)}(W - V_B), \quad (12)$$

$$\theta := -(1-T)(W^2 - 1), \quad (13)$$

$$\gamma := T(1-T)V_B + (1-T+T^2)W, \quad (14)$$

$$\phi := \sqrt{T(W^2 - 1)}. \quad (15)$$

These fixed- T variables supply the essential components to evaluate the Holevo bound alongside the corresponding mutual information between the legitimate parties. The subsequent subsection integrates these parameters into the fast-fading key-rate framework established in Sec. III.

B. Uniform Fast-Fading Secret-Key Rates

This subsection specifies the fixed-transmissivity components required for the evaluated two-way protocols based on the general fast-fading prescription in Eq. (4). The uniform density defined in Eq. (5) explicitly reduces the Eve-information average in Eq. (4) to

$$\int_{T_{\min}}^{T_{\max}} p(T) \chi_E(T) dT = \frac{1}{\Delta T} \int_{T_{\min}}^{T_{\min} + \Delta T} \chi_E(T) dT, \quad (16)$$

Thus, for each protocol considered below, the mutual information term is evaluated at $T_{\min}$, while the corresponding Eve-information term is averaged over the uniform fading interval.

For clarity, the superscripts DR and RR denote direct and reverse reconciliation, respectively; $\otimes$ denotes collective protocols, while labels without $\otimes$ denote individual protocols. The superscript 2 in Hom^2 and Het^2 denotes the corresponding two-way protocols.

Standard two-way analysis provides a broader catalogue of fixed-transmissivity rates [15]. The present analysis applies the uniform fast-fading prescription to the four two-way rates used in the subsequent numerical comparisons. These are the two collective direct reconciliation (DR) rates, $\otimes\text{Hom}^2$ and $\otimes\text{Het}^2$, and the two individual benchmark rates, Het^2 in DR and Hom^2 in RR.

The remaining four cases are not expanded explicitly. Collective RR cases, $\otimes\text{Hom}^2\text{-RR}$ and $\otimes\text{Het}^2\text{-RR}$, are not selected because the corresponding $I(B:E)$ bound is generally too large to give a useful comparison in the standard two-way analysis [15]. The individual $\text{Hom}^2\text{-DR}$ case is not listed separately because it coincides with the collective homodyne DR expression in the asymptotic setting considered here [15]. The individual $\text{Het}^2\text{-RR}$ case is not included in the closed-form benchmark set adopted for the present numerical simulations.

Here R denotes a secret-key rate. All quantities in the following fixed-transmissivity decomposition are evaluated at a fixed transmissivity T . Standard two-way analysis organizes the individual and collective key rates as [15]

$$R(T) = I(X_A:X_B) - \begin{cases} I(X_A:E), & \text{DR,} \\ I(X_B:E), & \text{RR,} \end{cases} \quad (17)$$

$$R_{\otimes}(T) = I(X_A:B) - \begin{cases} I(X_A:E), & \text{DR,} \\ I(B:E), & \text{RR.} \end{cases} \quad (18)$$

Here, X_A and X_B are Alice's and Bob's classical variables, while B denotes Bob's quantum system. In partic-

ular, the collective reverse-reconciliation term involves

$$I(B:E) = S_B + S_E - S_{BE}, \quad (19)$$

For the individual benchmarks with Gaussian classical variables, the mutual information between Alice and Bob, $I_{AB}(T) = I(X_A:X_B)$, can be written in the variance-ratio form

$$I_{AB}(T) = \frac{1}{2} \log_2 \frac{V_B(T)}{V_{B|A}(T)}, \quad (20)$$

where $V_B(T)$ is the variance of Bob's decoding variable and $V_{B|A}(T)$ is the conditional variance given Alice's encoding. A two-quadrature decoding variable directly sums the independent quadrature contributions.

For Gaussian states, von Neumann entropy is computed from the symplectic eigenvalues of the corresponding covariance matrix [2, 36]. If the relevant symplectic spectrum is denoted by $\{\nu_i\}$, then

$$S = \sum_i h(\nu_i), \quad (21)$$

where

$$h(x) = \frac{x+1}{2} \log_2 \frac{x+1}{2} - \frac{x-1}{2} \log_2 \frac{x-1}{2}. \quad (22)$$

When Eve's information is evaluated as a Gaussian Holevo quantity, $\chi_K(T)$ denotes Eve's information associated with the reconciled variable or system K and can be written as

$$\chi_K(T) = \sum_i h(\nu_i^E(T)) - \sum_j h(\tilde{\nu}_j^{E|K}(T)), \quad (23)$$

where $\{\nu_i^E(T)\}$ is obtained from Eve's unconditional covariance matrix and $\{\tilde{\nu}_j^{E|K}(T)\}$ is obtained from Eve's covariance matrix conditioned on K . Here, K denotes the variable or quantum system used to condition Eve's state: $K = X_A$ for direct reconciliation; for reverse reconciliation, $K = X_B$ for the individual benchmark and $K = B$ for the collective benchmark. The following closed-form expressions use the asymptotic setting specified in Sec. IV-A.

The subsequent derivation initially introduces the homodyne-type mutual information term

$$I_{\text{Hom}^2}(T) = \frac{1}{2} \log_2 \frac{TV}{(1-T^2)W}. \quad (24)$$

This term is used for the collective $\otimes\text{Hom}^2$ direct-reconciliation rate and for the individual Hom^2 reverse-reconciliation benchmark.

The mutual information term for the collective two-way homodyne protocol under DR is given by

$$I^{\text{DR}}[\otimes\text{Hom}^2](T) = I_{\text{Hom}^2}(T). \quad (25)$$

The corresponding Eve-information term is

$$\chi^{\text{DR}}[\otimes\text{Hom}^2](T) = \frac{1}{2} \log_2 \frac{V(1-T)}{(1+T)W} + h(W). \quad (26)$$

The resulting uniform fast-fading benchmark expression is obtained by applying Eq. (4) to the above fixed-transmissivity quantities:

$$R_{\text{ff}}^{\text{DR}}[\otimes \text{Hom}^2] = \frac{1}{2} \log_2 \frac{T_{\min}}{1 - T_{\min}^2} - h(W) + \frac{\Phi(T_{\min} + \Delta T) - \Phi(T_{\min})}{2\Delta T \ln 2}, \quad (27)$$

where

$$\Phi(T) = (1 - T) \ln(1 - T) + (1 + T) \ln(1 + T). \quad (28)$$

For the collective two-way heterodyne protocol under DR, denoted by $R_{\text{ff}}^{\text{DR}}[\otimes \text{Het}^2]$, both the mutual information and Eve-information terms are twice their homodyne counterparts:

$$I^{\text{DR}}[\otimes \text{Het}^2](T) = 2I_{\text{Hom}^2}(T), \quad (29)$$

$$\chi^{\text{DR}}[\otimes \text{Het}^2](T) = 2\chi^{\text{DR}}[\otimes \text{Hom}^2](T). \quad (30)$$

The resulting uniform fast-fading benchmark expression is obtained by applying Eq. (4) to these fixed-transmissivity quantities:

$$R_{\text{ff}}^{\text{DR}}[\otimes \text{Het}^2] = \log_2 \frac{T_{\min}}{1 - T_{\min}^2} - 2h(W) + \frac{\Phi(T_{\min} + \Delta T) - \Phi(T_{\min})}{\Delta T \ln 2}. \quad (31)$$

Individual-protocol benchmarks are adopted from the fixed-transmissivity closed-form rates of the standard two-way analysis and inserted into the same fast-fading prescription. For the individual two-way heterodyne protocol under DR, the auxiliary function $D(T)$ is defined as

$$D(T) = 1 + T^2 + (1 - T^2)W. \quad (32)$$

The mutual-information term is

$$I^{\text{DR}}[\text{Het}^2](T) = \log_2 \frac{TV}{D(T)}. \quad (33)$$

The corresponding Eve-information term is

$$\chi^{\text{DR}}[\text{Het}^2](T) = \log_2 \frac{eV(1 - T)}{2(1 + T)} + h(W). \quad (34)$$

The resulting uniform fast-fading benchmark expression is obtained by applying Eq. (4) to these fixed-transmissivity quantities:

$$R_{\text{ff}}^{\text{DR}}[\text{Het}^2] = \log_2 \frac{2T_{\min}}{eD(T_{\min})} - h(W) + \frac{\Phi(T_{\min} + \Delta T) - \Phi(T_{\min})}{\Delta T \ln 2}. \quad (35)$$

The mutual-information term for the two-way homodyne individual protocol under RR is given by

$$I^{\text{RR}}[\text{Hom}^2](T) = I_{\text{Hom}^2}(T). \quad (36)$$

The corresponding Eve-information term is

$$\chi^{\text{RR}}[\text{Hom}^2](T) = \frac{1}{2} \log_2 \frac{TV(1 - T)}{(1 + T)W(1 - T + T^2)} + h(W). \quad (37)$$

The resulting uniform fast-fading RR benchmark expression is obtained by applying Eq. (4) to the above fixed-transmissivity quantities:

$$R_{\text{ff}}^{\text{RR}}[\text{Hom}^2] = \frac{1}{2} \log_2 \frac{T_{\min}}{1 - T_{\min}^2} - h(W) - \frac{\Psi(T_{\min} + \Delta T) - \Psi(T_{\min})}{2\Delta T \ln 2}, \quad (38)$$

where

$$\Psi(T) = T \ln T - \Phi(T) - \left(T - \frac{1}{2}\right) \ln(1 - T + T^2) + T - \sqrt{3} \arctan \frac{2T - 1}{\sqrt{3}}. \quad (39)$$

These four expressions provide the key-rate quantities used in the numerical comparison under the uniform worst-case fast-fading model. Extensions involving CSI-assisted processing and turbulence-distributed transmissivity are introduced in the following subsection by modifying the treatment of the transmissivity distribution.

C. Extension to CSI and Weak-Turbulence Fading

This subsection extends the preceding framework to CSI-assisted processing and atmospheric fading statistics relevant to free-space channel modeling [37]. The non-CSI formulation remains the primary distribution-level benchmark considered here. The CSI-enabled case is introduced as a complementary idealized benchmark where the instantaneous transmissivity is tracked.

The key rate is averaged over the transmissivity distribution in the presence of CSI:

$$K_{\text{CSI}}^{\text{unif}} = \frac{1}{\Delta T} \int_{T_{\min}}^{T_{\min} + \Delta T} [\beta I_{AB}(T) - \chi_E(T)] dT. \quad (40)$$

The CSI expression averages the full instantaneous key-rate contribution, in contrast to the non-CSI prescription. For weak-turbulence fading, these two prescriptions are implemented using the transmissivity distribution $P(T)$ introduced below. The received irradiance is modeled as log-normal under weak atmospheric turbulence [38, 39]. The scintillation index is defined by [18]

$$\sigma_I^2 = \frac{\langle I^2 \rangle}{\langle I \rangle^2} - 1. \quad (41)$$

If $\ln I \sim \mathcal{N}(\mu_I, \sigma_{\ln I}^2)$, then

$$\frac{\langle I^2 \rangle}{\langle I \rangle^2} = \exp(\sigma_{\ln I}^2), \quad \sigma_{\ln I}^2 = \ln(1 + \sigma_I^2). \quad (42)$$

The transmissivity fluctuation is modeled as proportional to the normalized irradiance fluctuation,

$$T = T_0 \frac{I}{\langle I \rangle}. \quad (43)$$

Under the weak-turbulence assumption, the untruncated log-normal density of T is

$$P_{\text{LN}}(T) = \frac{1}{T\sqrt{2\pi\sigma^2}} \exp\left[-\frac{(\ln T - \mu)^2}{2\sigma^2}\right], \quad T > 0, \quad (44)$$

with

$$\sigma^2 = \ln(1 + \sigma_I^2), \quad \mu = \ln T_0 - \frac{\sigma^2}{2}. \quad (45)$$

Here, σ_I^2 is the scintillation index and T_0 is the nominal transmissivity of the underlying untruncated weak-turbulence model.

For the numerical weak-turbulence analysis, the nominal channel loss is defined as $L = -10 \log_{10} T_0$.

The log-normal density is truncated and normalized over $[T_L, T_U]$ to confine the transmissivity within a physical interval, where

$$0 < T_L < T_U \leq 1. \quad (46)$$

Here, T_L and T_U denote the lower and upper truncation bounds of the log-normal weak-turbulence distribution and define the transmissivity interval retained after truncation. The notation $T_{\min}$ and $T_{\max}$ is reserved for the support bounds of the uniform fast-fading model.

The truncated density is

$$P(T) = \frac{P_{\text{LN}}(T)}{\int_{T_L}^{T_U} P_{\text{LN}}(x) dx}, \quad T \in [T_L, T_U]. \quad (47)$$

The truncation does not rescale the variable T , but only renormalizes the probability density and changes the resulting moments. The domain $\mathcal{D}_T$ is defined as $[T_L, T_U]$ in this turbulence model.

For the numerical simulations, the truncation bounds are set to $T_L = 10^{-6}$ and $T_U = 1 - 10^{-5}$.

For the non-CSI weak-turbulence case, the same distribution-level prescription is retained, with the uniform density $p(T)$ replaced by the truncated weak-turbulence density $P(T)$. Accordingly, the outage-based operating transmissivity T_{wc} is defined by

$$\int_{T_L}^{T_{\text{wc}}} P(T) dT = \varepsilon_{\text{out}}. \quad (48)$$

The mutual-information term is then evaluated at T_{wc} , while Eve's information term is averaged with respect to $P(T)$ over $[T_L, T_U]$. Since realizations with $T < T_{\text{wc}}$ occur with probability ε_{out} , T_{wc} should be interpreted as an outage-based operating point rather than as the minimum transmissivity of every channel realization. The resulting weak-turbulence rate is therefore used here as an outage-based distribution-level benchmark.

With this construction, the fixed-transmissivity quantities derived above are reused directly, and the extension enters through the choice of $P(T)$ and the associated averaging prescription.

V. NUMERICAL SIMULATIONS AND PERFORMANCE ANALYSIS

Fast-fading key-rate expressions derived in Sec. IV are evaluated numerically in this section. Simulations focus on two aspects: the performance comparison between the two-way RoR² benchmark and the corresponding one-way RoR benchmark under uniform fading, and the behavior of the evaluated two-way benchmarks under different channel-knowledge assumptions and fading statistics. Sec. V-A gives the common simulation setup. Sec. V-B establishes the non-CSI uniform-fading baseline through a direct comparison between the one-way RoR and two-way RoR² benchmarks. Sec. V-C examines the effect of CSI-assisted averaging on the positive-key-rate region, whereas Sec. V-D examines the positive-key-rate behavior of the evaluated two-way benchmarks under truncated log-normal weak-turbulence fading. Finally, Sec. V-E combines CSI-assisted averaging with the weak-turbulence model to provide an idealized CSI-assisted benchmark.

A. Simulation Setup and Threat Model

A common benchmark setting is adopted to compare the evaluated Het² and Hom² protocols [40]. The simulations use the key-rate framework developed in Sec. IV under the asymptotic conditions specified in Sec. IV-A.

Table I summarizes the simulation parameters used in the numerical comparisons, including the fading, noise, and protocol parameters. The numerical simulations adopt the shared-transmissivity condition in Eq. (3) and the fading distributions defined in Sec. IV-C.

The fading statistics are parameterized by either the uniform transmissivity width ΔT or the scintillation index σ_I^2 of the truncated log-normal weak-turbulence model. The weak-turbulence simulations use the truncated log-normal distribution defined in Sec. IV-C.

The parameter values in Table I are selected to define consistent benchmark settings for the corresponding numerical comparisons. The value $V = 10^6$ is used as a sufficiently large finite value to numerically approximate the asymptotic large-modulation limit $V \rightarrow \infty$. The uniform fading width $\Delta T = 0.1$ is selected as a representative benchmark width that has been used in previous uniform fast-fading CV-QKD studies [20]. The scintillation index $\sigma_I^2 = 0.2$ is chosen to represent weak scintillation, consistent with the weak-fluctuation regime of atmospheric optical propagation [18]. The outage probability $\varepsilon_{\text{out}} = 10^{-3}$ is adopted as a representative outage benchmark; target outage probabilities of this order have also been considered in free-space optical communication

studies [41]. Within each numerical comparison, the parameters not under examination are kept fixed, so that the observed differences can be associated with the protocol, channel-knowledge condition, or fading model being varied.

Table I. Simulation Parameters Used in the Numerical Comparisons

Parameter	Value
<i>Modulation</i>	
V : large-modulation variance	10^6
<i>Channel</i>	
ΔT : uniform fading width	0.1
σ_I^2 : scintillation index	0.2
<i>Noise</i>	
W : Eve's ancillary thermal-state variance	1.01
<i>Protocol</i>	
β : reconciliation efficiency	1
ε_{out} : outage probability	10^{-3}

In the figure legends, Hom and Het denote homodyne and heterodyne detection, respectively. Specific labels RoD^2 , ReD^2 , and RoR^2 represent the two-way protocols Hom²-DR, Het²-DR, and Hom²-RR, respectively. The symbol $\otimes$ explicitly identifies collective benchmarks, whereas unmarked labels designate individual benchmarks. For the one-way RoR reference used in Fig. 2, the fixed-transmissivity one-way RR key-rate expression [15] is incorporated into the same uniform non-CSI fast-fading framework as the two-way benchmarks. Specifically, the mutual-information term is evaluated at $T_{\min}$, while Eve's information is averaged over the same fading distribution.

B. Baseline Performance under Uniform Worst-Case Fading

Primary numerical results from the uniform worst-case fast-fading prescription (Sec. IV) appear in Fig. 2. For the uniform-fading simulations, the horizontal-axis loss is defined from the worst-case transmissivity as $L = -10 \log_{10} T_{\min}$, so that $T_{\min} = 10^{-L/10}$. The one-way RoR and two-way RoR^2 benchmarks are plotted under the same uniform non-CSI fading condition using the common setting specified in Sec. V-A.

As shown in Fig. 2, the one-way RoR benchmark approaches the zero-rate boundary near 7.10 dB, whereas the corresponding two-way RoR^2 benchmark remains positive up to approximately 7.50 dB. Thus, within the adopted uniform non-CSI benchmark, the two-way RoR^2 benchmark retains a broader positive-key-rate region than the corresponding one-way RoR benchmark. As discussed in Sec. IV-B, these two RR results correspond

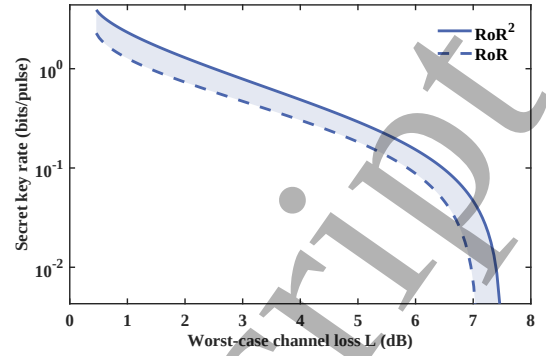


Figure 2. Secret-key-rate benchmarks for the one-way RoR and two-way RoR^2 protocols under uniform non-CSI fast fading. The solid line denotes the two-way benchmark and the dashed line denotes the corresponding one-way benchmark; the shaded region highlights the separation between the two key-rate curves.

to individual-protocol analytical benchmarks rather than collective-RR security benchmarks.

The difference between the two zero-rate boundaries is specific to the present ideal asymptotic benchmark and should not be interpreted as a practical attenuation limit or as a general security guarantee.

C. Impact of CSI

This subsection examines the role of instantaneous channel knowledge under the same uniform fading statistics as the non-CSI baseline. Fig. 3 compares the non-CSI and CSI-enabled results for the two-way RoR^2 benchmark. As defined in Sec. IV-C, the CSI case averages the full instantaneous key-rate contribution over the fading distribution, whereas the non-CSI benchmark evaluates the mutual-information term at $T_{\min}$ and averages Eve's information separately. Both curves use the common benchmark setting specified in Sec. V-A.

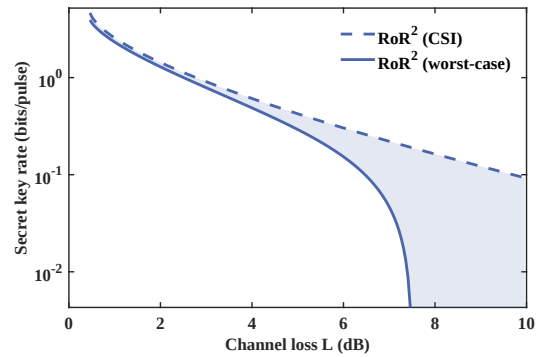


Figure 3. Secret-key-rate benchmarks for the two-way RoR^2 protocol under uniform fading, comparing the non-CSI prescription with CSI-enabled averaging. The solid line denotes the non-CSI benchmark and the dashed line denotes the CSI-enabled benchmark; the shaded region highlights the separation between the two key-rate curves.

As shown in Fig. 3, the non-CSI RoR² benchmark approaches the zero-rate boundary near 7.50 dB, whereas the CSI-enabled curve remains positive throughout the simulated loss range up to 10 dB. Since the CSI-assisted curve does not reach the zero-rate boundary within this range, no numerical CSI cutoff is assigned. Within the same ideal asymptotic individual-RR benchmark, this comparison shows that instantaneous channel information enlarges the positive-key-rate region of the evaluated two-way RoR² protocol under the adopted uniform fading model.

D. From Uniform Fading to Weak-Turbulence Statistics

Here the comparison examines whether the evaluated two-way benchmarks retain positive-key-rate behavior when the uniform fading distribution is replaced by a physically motivated truncated log-normal weak-turbulence model. The non-CSI distribution-level benchmark framework is retained, with the weak-turbulence transmissivity distribution introduced in Sec. IV-C [42].

Fig. 4 shows the positive-key-rate behavior of the evaluated two-way benchmarks under the uniform and weak-turbulence fading models. Under the adopted outage-based prescription, replacing the uniform distribution with the truncated log-normal weak-turbulence distribution changes the statistical weighting of the transmissivity realizations and consequently modifies the resulting key-rate behavior.

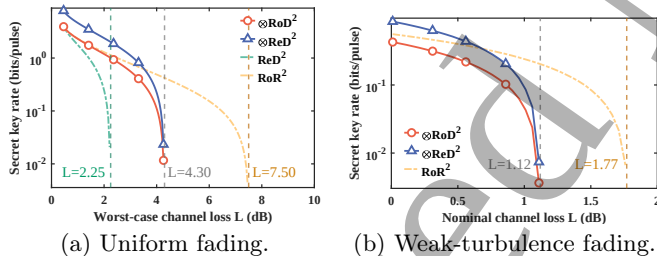


Figure 4. Secret-key rates of the two-way protocols under non-CSI distribution-level benchmarks: (a) uniform fading using the $T_{\min}$ -based worst-case prescription, and (b) truncated log-normal weak-turbulence fading using the T_{wc} -based outage prescription. This comparison examines whether the evaluated two-way protocols retain a positive-key-rate region under the weak-turbulence model.

Under uniform fading, the collective Hom²-DR and Het²-DR branches approach the zero-rate boundary near 4.30 dB, whereas under the adopted weak-turbulence configuration the corresponding nominal-loss cutoff is near 1.12 dB. Because the horizontal-axis loss is defined from $T_{\min}$ for the uniform model and from T_0 for the weak-turbulence model, these numerical cutoff values should be interpreted within their respective fading models rather than as directly equivalent channel-loss thresholds. The individual Het²-DR branch shows no positive-key-rate region under this weak-turbulence configuration

and is therefore omitted from the plotted positive-rate curves. The evaluated collective two-way benchmarks nevertheless retain positive-key-rate regions under both fading models. Because the present weak-turbulence comparison includes only the evaluated two-way protocols, no direct performance comparison between one-way and two-way protocols is made for this fading model.

E. CSI-Assisted Weak-Turbulence Benchmark

This final comparison applies CSI-assisted averaging to the truncated log-normal weak-turbulence model introduced in Sec. IV-C, keeping the fading statistics unchanged while replacing the non-CSI outage-based prescription.

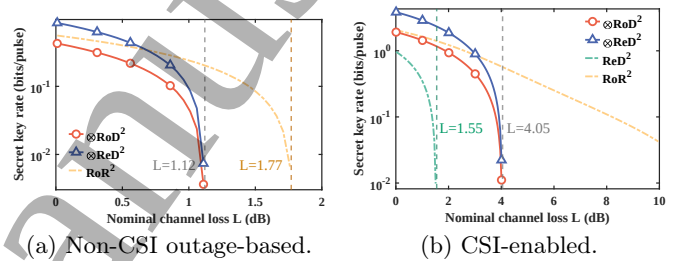


Figure 5. Secret-key rates of the two-way protocols under truncated log-normal weak-turbulence fading: (a) non-CSI outage-based prescription, and (b) CSI-enabled averaging. This comparison provides an idealized CSI-assisted benchmark for channel tracking under the adopted weak-turbulence model.

As shown in Fig. 5, with CSI the collective Hom²-DR and Het²-DR nominal-loss cutoffs increase from about 1.12 dB to 4.05 dB, and the individual Het²-DR branch again shows a positive-key-rate region. The individual Hom²-RR benchmark remains positive throughout the simulated loss range. Overall, CSI-enabled averaging enlarges the positive-key-rate region of the evaluated two-way benchmarks under the adopted weak-turbulence model.

VI. CONCLUSION

This work applies the adopted fast-fading prescription to established fixed-transmissivity two-way CV-QKD formulas and obtains benchmark key-rate expressions for the selected protocols. Under the stated model and the ideal benchmark $V \rightarrow \infty$, $\beta = 1$, the numerical results show that the evaluated two-way RoR² benchmark retains a wider positive-key-rate region than the corresponding one-way RoR benchmark under the adopted uniform non-CSI fast-fading model.

Beyond the primary uniform fast-fading analysis, the framework also applies to CSI-enabled evaluations and truncated log-normal weak-turbulence fading. CSI-enabled averaging enlarges the positive-key-rate region

of the evaluated benchmarks under the adopted channel models. Under the adopted weak-turbulence model, the evaluated collective two-way benchmarks also retain a positive-key-rate region. These extensions characterize the behavior of the evaluated two-way benchmarks under the specific CSI-enabled and weak-turbulence settings considered here, without making a direct performance comparison between one-way and two-way protocols under the weak-turbulence model.

ACKNOWLEDGMENTS

The research was supported by the Youth Foundation of the Natural Science Foundation of Hunan Province,

China (Grant No. 2025JJ60411).

DATA AVAILABILITY

All data that support the findings of this study are included within the article.

-
- [1] Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, page 8, Bangalore, India, 1984. IEEE.
 - [2] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of modern physics*, 84(2):621–669, 2012.
 - [3] Jinyi Li, Jian Zhou, Yanyan Feng, Ronghua Shi, and Jinjing Shi. Discrete modulation continuous variable quantum key distribution under fast fading channel. *Physica Scripta*, 99(11):115118, 2024.
 - [4] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A—Atomic, Molecular, and Optical Physics*, 81(6):062343, 2010.
 - [5] Daniele Dequal, Luis Trigo Vidarte, Victor Roman Rodrigo, Giuseppe Vallone, Paolo Villoresi, Anthony Leverrier, and Eleni Diamanti. Feasibility of satellite-to-ground continuous-variable quantum key distribution. *npj Quantum Information*, 7(1):3, 2021.
 - [6] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussièrès, Ming-Jun Li, et al. Secure quantum key distribution over 421 km of optical fiber. *Physical review letters*, 121(19):190502, 2018.
 - [7] Jiu-Peng Chen, Chi Zhang, Yang Liu, Cong Jiang, Weijun Zhang, Xiao-Long Hu, Jian-Yu Guan, Zong-Wen Yu, Hai Xu, Jin Lin, et al. Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km. *Physical review letters*, 124(7):070501, 2020.
 - [8] Sheng-Kai Liao, Wen-Qi Cai, Wei-Yue Liu, Liang Zhang, Yang Li, Ji-Gang Ren, Juan Yin, Qi Shen, Yuan Cao, Zheng-Ping Li, et al. Satellite-to-ground quantum key distribution. *Nature*, 549(7670):43–47, 2017.
 - [9] Stefano Pirandola. Limits and security of free-space quantum communications. *Physical Review Research*, 3:013279, 2021.
 - [10] Masoud Ghalaii and Stefano Pirandola. Quantum communications in a moderate-to-strong turbulent space. *Communications Physics*, 5(1):38, 2022.
 - [11] Zhiyue Zuo, Masoud Ghalaii, and Stefano Pirandola. Realistic threat models for fiber and free-space continuous variable quantum key distribution. *Physical Review Research*, 8:013185, 2026.
 - [12] Jiayan Fu, Bangjie Su, Jian Zhou, Ronghua Shi, and Jinjing Shi. Four-state continuous variable quantum key distribution with two accelerating partners. *Physics Letters A*, 501:129399, 2024.
 - [13] Runbo Zhao, Jian Zhou, Ronghua Shi, and Jinjing Shi. Unidimensional continuous variable quantum key distribution under fast fading channel. *Annalen der Physik*, 536(5):2300401, 2024.
 - [14] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):15043, 2017.
 - [15] Stefano Pirandola, Stefano Mancini, Seth Lloyd, and Samuel L Braunstein. Continuous-variable quantum cryptography using two-way quantum communication. *Nature Physics*, 4(9):726–730, 2008.
 - [16] Carlo Ottaviani and Stefano Pirandola. General immunity and superadditivity of two-way gaussian quantum cryptography. *Scientific reports*, 6(1):22225, 2016.
 - [17] Yue Tian, Jian Zhou, Runbo Zhao, Ronghua Shi, Jinjing Shi, and Yanyan Feng. Thermal state continuous-variable quantum key distribution via fast fading channel. *Physica Scripta*, 100(7):075119, 2025.
 - [18] Larry C Andrews and Ronald L Phillips. *Laser beam propagation through random media*. SPIE press, 2005.
 - [19] D Yu Vasylyev, AA Semenov, and W Vogel. Atmospheric quantum channels with weak and strong turbulence. *Physical Review Letters*, 117(9):090501, 2016.
 - [20] Panagiotis Papanastasiou, Christian Weedbrook, and Stefano Pirandola. Continuous-variable quantum key distribution in fast fading channels. *Physical Review A*, 97(3):032311, 2018.
 - [21] Vladyslav C Usenko, Bettina Heim, Christian Peuntinger, Christoffer Wittmann, Christoph Marquardt, Gerd Leuchs, and Radim Filip. Entanglement of gaussian states and the applicability to quantum key distribution over fading channels. *New Journal of Physics*, 14(9):093048, 2012.
 - [22] Bettina Heim, Christian Peuntinger, Nathan Killoran, Imran Khan, Christoffer Wittmann, Ch Marquardt, and

- Gerd Leuchs. Atmospheric continuous-variable quantum communication. *New Journal of Physics*, 16(11):113018, 2014.
- [23] AA Semenov and W Vogel. Quantum light in the turbulent atmosphere. *Physical Review A—Atomic, Molecular, and Optical Physics*, 80(2):021802, 2009.
- [24] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical review letters*, 88(5):057902, 2002.
- [25] Christian Weedbrook, Andrew M Lance, Warwick P Bowen, Thomas Symul, Timothy C Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Physical review letters*, 93(17):170504, 2004.
- [26] Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, 2003.
- [27] Anthony Leverrier. Composable security proof for continuous-variable quantum key distribution with coherent states. *Physical review letters*, 114(7):070501, 2015.
- [28] László Ruppert, Christian Peuntinger, Bettina Heim, Kevin Günthner, Vladyslav C Usenko, Dominique Elser, Gerd Leuchs, Radim Filip, and Christoph Marquardt. Fading channel estimation for free-space continuous-variable secure quantum communication. *New Journal of Physics*, 21(12):123036, 2019.
- [29] Renato Renner and J Ignacio Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Physical review letters*, 102(11):110504, 2009.
- [30] Michael M Wolf, Geza Giedke, and J Ignacio Cirac. Extremality of gaussian quantum states. *Physical review letters*, 96(8):080502, 2006.
- [31] Raul Garcia-Patron and Nicolas J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable qkd. *Physical Review Letters*, 97(19):190503–190503, 2006.
- [32] Jeffrey H Shapiro. Reciprocity of the turbulent atmosphere. *Journal of the Optical Society of America*, 61(4):492–495, 1971.
- [33] Haifeng Yao, Chunyi Chen, Xiaolong Ni, Shoufeng Tong, Bo Li, Prosper Chidike, Zhi Liu, Yiwu Zhao, and Huilin Jiang. Analysis and evaluation of the performance between reciprocity and time delay in the atmospheric turbulence channel. *Optics express*, 27(18):25000–25011, 2019.
- [34] Stefano Pirandola, Samuel L. Braunstein, and Seth Lloyd. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. *Physical Review Letters*, 101(20):200504, 2008.
- [35] Kamel Bencheikh, Th Symul, A Jankovic, and Juan-Ariel Levenson. Quantum key distribution with continuous variables. *Journal of Modern Optics*, 48(13):1903–1920, 2001.
- [36] Gerardo Adesso, Sammy Ragy, and Antony R Lee. Continuous variable quantum information: Gaussian states and beyond. *Open Systems & Information Dynamics*, 21(01n02):1440001, 2014.
- [37] Nadasadat Hosseinidehaj and Robert Malaney. Gaussian entanglement distribution via satellite. *Physical Review A*, 91(2):022304, 2015.
- [38] M Klen and AA Semenov. Numerical simulations of atmospheric quantum channels. *Physical Review A*, 108(3):033718, 2023.
- [39] Christian Peuntinger, Bettina Heim, Christian R Müller, Christian Gabriel, Christoph Marquardt, and Gerd Leuchs. Distribution of squeezed states through an atmospheric channel. *Physical review letters*, 113(6):060502, 2014.
- [40] Quntao Zhuang, Zheshen Zhang, Norbert Lütkenhaus, and Jeffrey H Shapiro. Security-proof framework for two-way gaussian quantum-key-distribution protocols. *Physical Review A*, 98(3):032332, 2018.
- [41] José M Garrido-Balsells, F Javier Lopez-Martinez, Miguel Castillo-Vázquez, Antonio Jurado-Navas, and Antonio Puerta-Notario. Performance analysis of fso communications under los blockage. *Optics express*, 25(21):25278–25294, 2017.
- [42] Nadasadat Hosseinidehaj, Nathan Walk, and Timothy C Ralph. Composable finite-size effects in free-space continuous-variable quantum-key-distribution systems. *Physical Review A*, 103(1):012605, 2021.