UNIVERSITY of York

This is a repository copy of *Continuous-variable quantum key distribution with a single quadrature measurement at an arbitrary reference frame*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/id/eprint/232947/

Version: Published Version

Article:
Nagaraja Rao, Vinod, MEDLOCK, EMMA, SPILLER, TIMOTHY PAUL orcid.org/0000-0003-1083-2604 et al. (1 more author) (2025) Continuous-variable quantum key distribution with a single quadrature measurement at an arbitrary reference frame. Physical Review A. 042406. ISSN: 1094-1622

https://doi.org/10.1103/g465-pm47

Reuse
This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here: https://creativecommons.org/licenses/

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Continuous-variable quantum key distribution with a single quadrature measurement at an arbitrary reference frame

Vinod N. Rao [1,2,*] Emma Tien Hwai Medlock [1] Timothy Spiller [1,2] and Rupesh Kumar [1,2,†]
[1]*School of Physics, Engineering & Technology and York Centre for Quantum Technologies, University of York, YO10 5FT York, United Kingdom*
[2]*Quantum Communications Hub, University of York, United Kingdom*

(Received 27 May 2025; revised 5 September 2025; accepted 15 September 2025; published 3 October 2025)

We propose a simplified measurement scheme for a Gaussian modulated coherent state (GMCS) protocol for continuous variable quantum key distribution (CV-QKD), utilizing homodyne detection without quadrature switching. The reference frame of measurement is taken to be at an arbitrary angle, however, reconciliation converges the proposed scheme to GMCS with switching quadrature protocol. The arbitrary frame of measurement could also include the unknown random thermal drift within Bob's optical measurement setup. We found this scheme is advantageous for practical free-space and fiber-based GMCS protocol-based CV-QKD systems as it does not require a phase modulator for random measurement selection quadrature at Bob.

DOI: 10.1103/g465-pm47

I. INTRODUCTION

Quantum key distribution (QKD) enables two parties to share a secret key, in the presence of an eavesdropper [1]. The advantage of QKD over the classical counterpart, is that the latter relies on the computational hardness of a problem for security. Whereas, in QKD, information-theoretic security is provided, which is proven by the laws of physics [2,3]. The security of QKD relies on no-go theorems, such as, the no-cloning theorem [4], impossibility in perfectly distinguishing nonorthogonal states [5], monogamy of entanglement [6], the uncertainty principle among two noncommuting observables [7], and so on. The earlier proposals [1,8,9] and demonstrations [10–13] for QKD were based on discrete variables (DV) using weak coherent states, based on polarization or phase qubits and single photon detectors. Recently, newer protocols were developed and demonstrated for longer transmission distances [14–16].

Continuous variable (CV) QKD protocols [17–19] utilize amplitude and phase modulation of coherent states to encode the secure key information and shot noise limited detection for decoding. Squeezed as well as thermal states-based protocols have also been proposed for implementing CV-QKD protocols [17]. Among the various CV-QKD protocols, the Gaussian modulated coherent state (GMCS) protocol [20,21] has been thoroughly studied for its security and demonstrated over fiber as well as free-space channels. The amplitude and phase of the coherent state are modulated such that the field quadratures follow the Gaussian probabilistic distribution.

There are two versions of the GMCS protocol based on the measurement of the quadratures. In switching quadrature protocol (GG02) [20], Bob randomly selects the quadrature for the measurement using a homodyne detector. In the nonswitching version of the GG02 protocol [22], Bob measures both quadratures with a heterodyne detector. The nonswitching protocol has higher information decoding capacity for shorter distances [23–25], while the switching protocol is more suitable for long distances CV-QKD demonstrations [26–28]. At the detectors, the relative phase of 0° or 90°, between the CV-QKD signal with a strong reference signal, referred to as the local oscillator (LO), sets the reference frame for the quadrature measurement.

There are also two variants for CV-QKD protocol implementation. In the transmitting local oscillator (TLO) scheme, the LO is transmitted along with the CV-QKD signal [20]. Since both the signal and the LO pass through the same channel, the phase drift from the channel is negligible. However, with the local local oscillator (LLO) scheme, only the reference pulse is sent by Alice to Bob and the LO is locally generated inside Bob's station [24].

In theoretical analysis, the reference frames of state preparation at Alice and that of the state measurement at Bob are assumed to be fixed and known to Eve. To avoid Eve replacing the coherent states with squeezed states, either a random selection of the quadrature or measuring both of them at the same time is necessary. However, in practice, the frame of measurement is continuously rotated at an arbitrary rate. Measurement of quadrature along the arbitrary frame of reference has been already proposed in Ref. [24], however, this is a quadrature switching version with the homodyne detector. We propose the arbitrary frame of measurement scheme without switching quadratures and using a homodyne detector. We consider the measurement frame of reference to be dynamic

*Contact author: vinod.rao@york.ac.uk
†Contact author: rupesh.kumar@york.ac.uk

Published by the American Physical Society under the terms of the Creative Commons Attribution 4.0 International license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

during the protocol run. The initial angle, the rate of rotation, and the direction of the rotation of the frame of measurement are taken to be random as well. We also assume that over the protocol run, the frame of measurement could be rotated to all the possible angles. The phase drift can collectively be caused by: Alice's preparation setup, θ_{Alice}; transmission channel, θ_{ch}; and Bob's measurement setup, θ_{Bob}. We note here that the current work addresses the phase drift that happens at Bob's measurement setup inside his station, and works for both transmitted/local local oscillator schemes.

In this paper, we aim to validate that the GG02 protocol can be performed using homodyne detection and without actively switching the quadratures as originally proposed and demonstrated over the last two decades. We prove that our scheme retains the characteristics of the GG02 protocol and, thus does not create any new security loopholes. Specifically, the aspect of security that is considered here is for the collective attack by the eavesdropper Eve and we show that the protocol is secure in the asymptotic limit. We also show an optimal intercept and resend attack by Eve, and highlight that it is different from the one in GG02-like protocols. Additionally, our proposed scheme works not only with a TLO setup, but with a LLO setup as well. In the LLO variant of the proposed protocol, all the quantum parts would remain same as in a standard LLO protocol. The only difference would be that Bob sets his LO to a random quadrature in the phase space and then correlates to the reference pulse sent by Alice.

The paper is structured as follows. The Sec. II provides the outline of Gaussian modulated CV-QKD protocol GG02. In Sec. III, we describe the arbitrary rotation of the frame of reference in Bob's measurement and prove its equivalence to GG02. Finally, discussion and conclusion of our results is in Sec. IV.

II. GAUSSIAN MODULATED COHERENT STATE PROTOCOL

A brief introduction to conventional GMCS protocols is given below. These protocols utilize coherent states, $|\alpha\rangle = |\hat{q}_{\text{A}} + i\hat{p}_{\text{A}}\rangle$, as the information carriers, wherein the state quadratures, $\hat{q}_{\text{A}}$ and $\hat{p}_{\text{A}}$, are randomly modulated by Alice such that the quadratures follow Gaussian distribution, $\mathcal{N}(0, \mathbb{V}_{\text{A}})$, of variance $\mathbb{V}_{\text{A}}$ and mean at zero. Along with the signal states, Alice also sends the LO pulses and thus involves them of being suitably multiplexed by Alice and demultiplexed by Bob. The signal states undergo attenuation and noise is added to it during the transmission from Alice to Bob. At Bob, the quadratures of the modulated coherent states, $\hat{q}_{\text{B}}$ and $\hat{p}_{\text{B}}$, are measured with a shot noise (vacuum noise) limited homodyne (switching protocol) or heterodyne detector (nonswitching protocol). The variance of the measurement at Bob can be written as $\mathbb{V}_{\text{B}} = T * \mathbb{V}_{\text{A}} + \xi_t$, in which T is the transmittance of the channel and ξ_t is the total noise variance added to the quadratures.

During the classical post-processing, Bob publicly announces the chosen quadrature for measurement and Alice chooses the respective variance. Additionally, Bob also announces the variance $\mathbb{V}_{\text{B}}$ of a fraction of transmitted states, to Alice for quantifying error in the channel. The remaining data is used for secure key generation after error correction and privacy amplification. In the switching version of the protocol, Bob has to disclose the quadrature he measures (not the measurement outcomes) as well and that forms the sifting. The noise variance term ξ_t comprises of the shot noise variance, electronic noise variance of the detector, noise from eavesdropping among others. One can assume that the channel transmittance T, along with the excess noise, is controlled by Eve.

The feature that prevents the possibility of CV-QKD with fixed quadrature measurement is the following. By knowing the frame of Bob's measurement, Eve can launch the intercept and resend (IR) attack, during which she can resend a suitable squeezed state along the frame of quadrature measurement and hides her presence. Given Bob's selection of quadrature for the measurement (among $\hat{q}_{\text{B}}$ and $\hat{p}_{\text{B}}$) is unknown to Eve, she has 50% chance to hide her attack with squeezed states. To prevent Eve from using a squeezed state, one has to either switch between the quadratures randomly [20] or measure both quadratures [22].

Therefore, both versions of the CV-QKD protocol offers security against individual attacks by Eve. In case of collective attack such as Eve using an entangled cloner, she entangles her own n-mode squeezed states with the state sent by Alice. In the switching version of the protocol, she waits for Bob to announce his choice of quadrature to and measures her n-mode state (stored in the quantum memory). In no-switching version, Eve does not need to wait for Bob's announcement. However, as in the case of individual attack, the action of entangling $|\alpha\rangle$ with her own n-mode squeezed state increases the excess noise [29].

For the switching protocol, a specific quadrature for measurement at Bob is chosen at random, by suitably selecting the phase of the LO. The relative phase of LO at Bob with respect to the initial phase during the coherent state preparation defines the chosen quadrature for measurement, which is conventionally taken to be 0° for $\hat{q}_{\text{A}}$ quadrature and 90° for $\hat{p}_{\text{A}}$ quadrature. However, in practice, the relative phase between signal and LO inside Bob's station is continuously drifting due to thermal fluctuations and relative frequency drift. Primarily, the fluctuations could be due to the different paths that the signal and LO take after demultiplexing within Bob's measurement setup. Additionally, in the case of the LLO scheme, it can happen due to the frequency drift of the laser at Bob's station. Limiting our arguments in the rest of the paper to phase drift inside Bob's station θ_{Bob} alone, we attribute this relative phase drift to the signal. If the phase drift is relatively slow compared to the QKD repetition rate, which is a requirement for our scheme to work, this can be associated to phase noise [24]. However, if the repetition rate is slower than that of the phase drift then it requires heterodyne detection for phase estimation. Also, the key rate would significantly drop, as the correlation between Alice and Bob would reduce. This phase drift is unknown to Bob, but he could easily estimate it after measurement. In principle, Eve could probe this phase drift with a very high intense beam but there are countermeasures to prevent such attacks [30]. Also, high-intensity probe beams saturate the measurements and can be detected as well [31]. The phase drift creates an additional postprocessing routine, as either Bob or Alice has to rotate their frame of reference to compensate for the drift and match reference frames with each

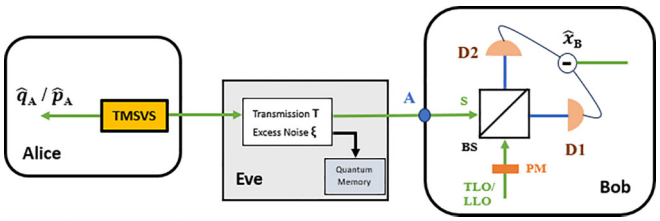

FIG. 1. CV-QKD with the homodyne detection setting. Alice prepares two mode squeezed vacuum states (TMSVS) and sends one of the modes to Bob. Bob's setup interferes the signal (S) with the local oscillator (LO) pulses using a beam splitter (BS) and performs homodyne measurements using photodiodes (D1 and D2). There could be a relative phase drift between signal and LO inside Bob's station (from the blue marker, A, to the BS) represented by θ_{Bob} (see text below), that is independent from the phase drift in the channel and Alice's station. Contrary to standard homodyne measurement, we do not use a phase modulator (PM) in our scheme. $\hat{x}_B$ is the quadrature output of the homodyne along the measurement angle θ_{Bob}. The eavesdropping by Eve is characterized by reduced transmittivity T, and excess noise from the channel ξ.

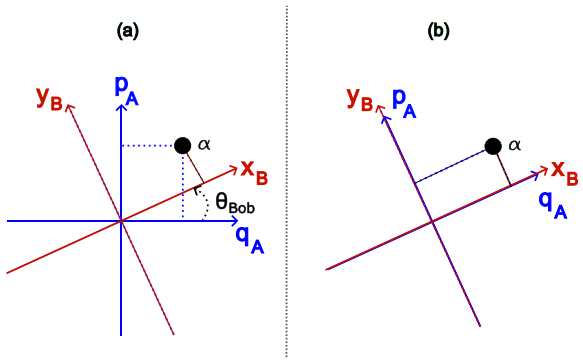

FIG. 2. (a) Rotated frame of measurement by the receiver Bob. He always measures along the quadrature $\hat{x}_B = \cos\theta_{\text{Bob}}(\hat{q}_B) + \sin\theta_{\text{Bob}}(\hat{p}_B)$, where θ_{Bob} is the angle of the rotation with respect to $\hat{q}_B$ (as well as $\hat{q}_A$). (b) After Bob's announcement of the angle θ_{Bob}, Alice rotates her frame to coincide with $\hat{x}_B$.

other. Therefore, even assuming that Eve controls the drift in the channel, she would still have no knowledge of the phase drift inside Bob's (or Alice's) station. There are proposals to use machine learning algorithms for estimating the phase drift in the channel [32], however, this is beyond the scope of the current work.

In the case where Bob actively compensates for phase drift in real time, a fixed choice of phase enables Eve to launch IR attack as the frame of measurement at Bob matches with that of state preparation at Alice. But, in the case where Alice compensates her quadrature data for the phase drift during the postprocessing and thereby matches with Bob's frame of measurement, a single (fixed) quadrature measurement can be implemented without switching the quadrature. In the next section, we provide evidence that no switching GMCS protocol with single quadrature measurement at an arbitrary choice of θ_{Bob} is equivalent to GG02 protocol.

III. ARBITRARY ROTATION IN MEASUREMENT FRAME OF REFERENCE

Continuing with the discussions of GMCS protocol given in the previous section, we follow the prepare and measure (PM)-based description of the protocol. The unconditional security of the PM-based protocols can be verified by mapping it to an equivalent of the entanglement-based (EB) protocol. In the EB scheme, Alice prepares two-mode squeezed vacuum states (TMSVS), keeps one of the modes with herself, and sends the other to Bob as in Fig. 1. The covariance matrix formalism helps to find the respective mutual information quantities between Alice and Bob, as well as that of Eve with Alice or Bob. Here, the covariance matrix is obtained by finding the expectation values of the respective quadratures. Since Alice's quadratures are $\hat{q}_A$ and $\hat{p}_A$, we find the first entry in the matrix as, $\langle \hat{q}_A^2 \rangle - \langle \hat{q}_A \rangle^2$ and similarly for the other elements. The covariance matrix of the TMSVS is,

$$\Sigma = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{V^2-1}\sigma_z \\ \sqrt{V^2-1}\sigma_z & V\mathbb{1}_2 \end{pmatrix}, \tag{1}$$

where $\mathbb{1}_2$, σ_z are the respective Pauli matrices, V is the variance of the squeezed states. This is for the case wherein channel transmittivity $T = 1$ and noise $\xi = 0$. The corresponding rows (and columns) here represent the variances of Alice's quadratures, $\hat{q}_A$, $\hat{p}_A$ of mode-1, Bob's quadratures, $\hat{q}_B$ and $\hat{p}_B$, of mode-2, such that $[\hat{q}_A, \hat{p}_A] = [\hat{q}_B, \hat{p}_B] = i/2$. The respective quadratures can be perfectly correlated during postprocessing, such that $\hat{q}_A = \hat{q}_B$ and $\hat{p}_A = \hat{p}_B$. Bob measures either both the quadratures of mode-2 simultaneously with a heterodyne detector, or one of them at random with a homodyne detector. We find that the variance, $V(\hat{q}_B) = V(\hat{p}_B) = V$, identical to that of Alice's quadratures.

Consider the case wherein Bob chooses to perform single quadrature measurement of the mode-2 throughout the protocol, at an arbitrary angle of measurement θ, thanks to the phase drift, as shown in Fig. 2. For convention, we take that he chooses to measure in the $\hat{x}_B = \cos\theta_{\text{Bob}}(\hat{q}_B) + \sin\theta_{\text{Bob}}(\hat{p}_B)$ quadrature. While the other quadrature would be $\hat{y}_B$, with $[\hat{x}_B, \hat{y}_B] = 2i$, we shall restrict the case to Bob always choosing quadrature $\hat{x}_B$ for measurement. In other words, Bob only acquires the homodyne detector outcome and refers to it as x_B. After Bob's announcement of the angle θ_{Bob}, Alice rotates her frame to coincide with $\hat{x}_B$. However, there could be a small phase mismatch between Alice and Bob as the phase is drifting continuously at Bob's station, which is addressed in Figs. 3 and 4. In the following, we consider three different scenarios in which the measurement frame of reference, θ_{Bob}, is (i) fixed and known to Eve, (ii) fixed and unknown to Eve, and (iii) varying and unknown to both Eve and Bob.

A. θ_{Bob} is fixed and known to Eve

Here we consider the reference frame of measurement is rotated by a fixed angle θ_{Bob} and Eve has the knowledge about the rotation. She is also aware that Bob will be measuring only one of the quadratures ($\hat{x}_B$) throughout the protocol run. In this scenario, Eve can successfully perform a trivial IR

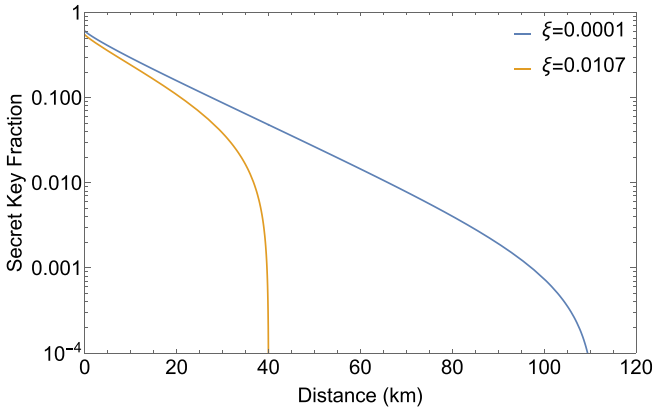

FIG. 3. Secret key fraction as a function of distance. Here the angle of rotation is chosen to be $\theta_{\text{Bob}} = 90^\circ$. Blue (orange) line corresponds to the noise $\xi = 0.0001$ ($\xi = 0.0107$, for a phase drift of 5°).

attack without introducing any error in Bob's measurement. Though the variance of the other quadrature ($\hat{y}_{\text{B}}$) increases due to eavesdropping, since it is never measured, the protocol becomes completely insecure. This would be identical to Eve knowing Bob's choice of quadrature for each pulse in the homodyne based conventional CV-QKD protocol. The requirement of θ_{Bob} being unknown to Eve makes the single quadrature measurement strategy interesting and secure. We will analyze this case in the following section.

B. θ_{Bob} is fixed and unknown to Eve

Here, we consider Bob's reference frame of measurement is rotated by a fixed angle θ_{Bob}, as in the previous case. Additionally, we take that Eve does not have knowledge of the angle θ_{Bob} until the announcement by Bob via public channel, as in the case of GG02 of Eve not knowing the chosen quadrature until announcement. We also assume that there are proper countermeasures implemented to prevent Eve from probing the angle, such as an optical isolator at Bob's input. So we limit our arguments to a trusted device scenario, and this assumption is equivalent to the one in GG02

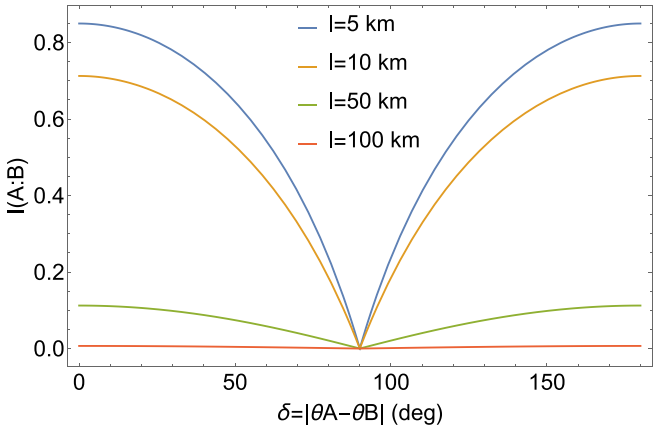

FIG. 4. Mutual information between Alice and Bob, as a function of the relative angle of the frame of references.

protocol, of using countermeasures to check for Trojan-horse-like attacks [33]. We find the covariance matrix considering Bob measuring with angle θ_{Bob} and choosing only $\hat{x}_{\text{B}}$ all the times. The matrix elements $\Sigma_{11}, \Sigma_{12}, \Sigma_{21}, \Sigma_{22}$ are identical to that in Eq. (1). However, other entries are different, in that $\Sigma_{33} = \langle \hat{x}_{\text{B}}^2 \rangle - \langle \hat{x}_{\text{B}} \rangle^2$, and so on. Thus the covariance matrix is found to be,

$$\Sigma_{\text{AB}} = \begin{pmatrix} V\mathbb{1}_2 & \sqrt{V^2-1}P \\ \sqrt{V^2-1}P^{\text{T}} & V\mathbb{1}_2 + \frac{(V+1)}{2}R \end{pmatrix}, \tag{2}$$

as we find that $V(\hat{x}_{\text{B}}) = V(\hat{p}_{\text{B}}) = V$, and where $P = \{\{\cos\theta_{\text{Bob}}, 0\}, \{-\sin\theta_{\text{Bob}}, -1\}\}$ and $R = \{\{0, \sin\theta_{\text{Bob}}\}, \{\sin\theta_{\text{Bob}}, 0\}\}$. Also, keeping $\theta_{\text{Bob}} = 0$, we get Eq. (1).

Since θ_{Bob} is unknown to Eve, an IR attack will not be successful, as the interception would increase the variance with a high probability, when Bob measures. Thus the excess noise induced by the attack would lead to termination of the protocol. Here we consider Eve's collective attack via an entangled cloner, wherein she entangles her probe with mode-2 of the TMSVS sent by Alice to Bob. Eve's cloner could be n-mode, and use one of the modes to entangle with mode-2. However, this can be reduced to Eve using a TMSVS and using one of the modes to entangle, due to monogamy of entanglement. Thus we consider Eve's TMSVS and the covariance matrix of her entangling cloner, similar to that of Alice-Bob in Eq. (2), is

$$\Sigma_{\text{E}} = \begin{pmatrix} W\mathbb{1}_2 & \sqrt{W^2-1}Q \\ \sqrt{W^2-1}Q^{\text{T}} & W\mathbb{1}_2 + \frac{(W+1)}{2}S \end{pmatrix}, \tag{3}$$

where $\Sigma_{\text{E}} = \Sigma_{\text{E}_1\text{E}_2}$ corresponds to the Eve's TMSVS (with $\text{E}_{1,2}$ representing the respective mode), $Q = \{\{\cos\phi, 0\}, \{-\sin\phi, -1\}\}$ and $S = \{\{0, \sin\phi\}, \{\sin\phi, 0\}\}$, and ϕ being the angle of measurement by Eve. Assuming that Eve replaces the lossy quantum channel with a beam splitter (BS) of transmission T, the symplectic BS [34] acting on the mode-2 and E_1 is represented by,

$$\Sigma_{\text{BS}} = \begin{pmatrix} \mathbb{1}_2 & 0 & 0 & 0 \\ 0 & \sqrt{T}\mathbb{1}_2 & \sqrt{1-T}\mathbb{1}_2 & 0 \\ 0 & -\sqrt{1-T}\mathbb{1}_2 & \sqrt{T}\mathbb{1}_2 & 0 \\ 0 & 0 & 0 & \mathbb{1}_2 \end{pmatrix}. \tag{4}$$

The action of the BS on the joint system of Alice, Bob, and Eve is described by,

$$\Sigma' = \Sigma_{\text{BS}}\Sigma_{\text{ABE}}\Sigma_{\text{BS}}^{\text{T}}, \tag{5}$$

with $\Sigma_{\text{ABE}} = \Sigma_{\text{AB}} \oplus \Sigma_{\text{E}}$ corresponding to the joint system of Alice, Bob, and Eve.

Using Σ' in Eq. (A1), we find the reduced covariance matrix of Alice-Bob as

$$\Sigma'_{\text{AB}} = \begin{pmatrix} V\mathbb{1}_2 & \mathcal{X}_+P \\ \mathcal{X}_+P^{\text{T}} & \mathcal{Z}_1 \end{pmatrix}, \tag{6}$$

and that of Eve is

$$\Sigma'_{\text{E}} = \begin{pmatrix} \mathcal{Z}_2 & \mathcal{Y}_+Q \\ \mathcal{Y}_+Q^{\text{T}} & W\mathbb{1}_2 + \frac{(W+1)}{2}S \end{pmatrix}, \tag{7}$$

where $\mathcal{X}_+, \mathcal{Y}_+, \mathcal{Z}_1, \mathcal{Z}_2$ are given in Appendix A.

From Eq. (6), the respective mode variances are, $V_{\rm A} = V[= V(\hat{q}_{\rm A}) = V(\hat{p}_{\rm A})]$ and $V_{\rm B} = TV + (1-T)W[= V(\hat{x}_{\rm B})]$. For $T = 1$, we obtain Eq. (1). As expected, we find that $V(\hat{q}_{\rm B}) = V(\hat{p}_{\rm B}) = V(\hat{x}_{\rm B})[= V(\hat{y}_{\rm B})]$. Since the rotation in the frame of measurement is a unitary operation on mode-2, the variance does not change. Thus Bob measures as much variance in a rotated frame as he would have for the standard $\hat{q}$ or $\hat{p}$ quadrature. After the announcement of $\theta_{\rm Bob}$ via public channel by Bob and establishing the correlation with Alice's quadrature data values, they estimate their mutual information as follows. By choosing Eve's variance to be $W = 1 + \frac{\xi}{1-T}$ [34], we find $V_{\rm B} = T(V-1) + 1 + \xi$. Therefore, the signal variance at Bob's station is given by, $V_s = T(V-1)$ and the noise variance is $V_n = 1 + \xi$. Thus, we find the mutual information between Alice and Bob to be [35]

$$I(A:B) = \frac{1}{2}\log_2\left(1 + \frac{V_s}{V_n}\right) = \frac{1}{2}\log_2\left(1 + \frac{T(V-1)}{1+\xi}\right), \tag{8}$$

where ξ is the excess noise. Here, we note that the mutual information between Alice and Bob is identical to that in the case when Bob performs homodyne measurements along the conventional ($\hat{q}$ or $\hat{p}$) quadratures [34].

To quantify the information leaked to Eve, Alice, and Bob need to estimate $\chi = S_{\rm E} - S_{\rm E|B}$, where $S_{(x)} = -{\rm Tr}[x\log(x)]$ corresponds to the von Neumann entropy. Given $\rho_{\rm ABE}$ represents the joint state of Alice, Bob, and Eve, let $\rho_{\rm AB} = {\rm Tr}_{\rm E}(\rho_{\rm ABE})$ and $\rho_{\rm E} = {\rm Tr}_{\rm AB}(\rho_{\rm ABE})$. Since the von Neumann entropy depends only on the coefficients of the Schmidt decomposition (which are found to be identical for $\rho_{\rm AB}$ and $\rho_{\rm E}$ [35]), we find that $\chi = S_{\rm E} - S_{\rm E|B} = S_{\rm AB} - S_{\rm A|B}$. To find $S_{\rm AB}$, we find the symplectic eigenvalues of the covariance matrix $\Sigma'_{\rm AB}$. Similarly, we find $S_{\rm A|B}$ by the symplectic eigenvalues of the covariance matrix $\Sigma'_{\rm A|B}$, taking the partial measurements on the covariance matrix as given in Eq. (B2). The elucidation of the same is given in Appendix B.

The secret key fraction is thus found to be,

$$\begin{aligned} r &= \beta\, I({\rm A}:{\rm B}) - \chi \\ &= \frac{\beta}{2}\log_2\left(1 + \frac{T(V-1)}{1+\xi}\right) - g(\nu_+) - g(\nu_-) + g(\nu), \end{aligned} \tag{9}$$

where ν_+, ν_-, ν are the respective symplectic eigenvalues of $S_{\rm AB}$ and $S_{\rm A|B}$, given in Eq. (B3) and Eq. (B4). The Fig. 3, corresponds to the secret key fraction after the public announcement of $\theta_{\rm Bob}$ by Bob to Alice. Here the frame of reference is kept along the $\hat{p}_{\rm B}$ quadrature. We also include the possible key rate for a potential phase drift of 5°, that corresponds to an excess noise of $\xi = 0.0107$ [36]. We note that this phase drift is assumed to be happening within Bob's station. This phase error could be due to inaccurate phase estimation by Bob, which is fundamentally limited by the shot noise with the pattern signal measurements. In TLO scheme, the phase drift is estimated using the pattern signals, which are comparatively at higher intensity than the QKD signals and are sent with each block of QKD signals [37–39]. However, the residual phase mismatch is common in any CV-QKD system, independent of the receiver architecture and protocol.

In Fig. 4, we plot the mutual information between Alice and Bob with the variation in the angle of rotation in their frame of measurements prior to the public announcement of $\theta_{\rm Bob}$ by Bob. In particular, similar to Bob, Alice also measures the variance with rotating her frame of measurement to $\theta_{\rm A}$, which is independent of Bob's rotation. The mutual information then is found to be

$$I({\rm A}:{\rm B}) = \frac{1}{2}\log_2\left(1 + \frac{T(V'-1)}{1+\xi}\right), \tag{10}$$

similar to the earlier case in Eq. (8), but where $V' = (V_a\cos\theta_{\rm Bob})/\cos\theta_{\rm A}$ is Bob's variance and V_a is Alice's variance along $\theta_{\rm A}$. We get maximum information for the relative angle of the frame of references $\delta \mid \theta_{\rm Bob} - \theta_{\rm A} \mid = 0$, showing perfect coinciding of Alice's and Bob's quadratures after the public announcement. Various distances are considered that also provides the upper bound on the respective mutual information.

C. $\theta_{\rm Bob}$ is drifting, and unknown to Bob and Eve

The practical implementation of CV-QKD experiences random drift in $\theta_{\rm Bob}$, which is unknown before the measurement but can be monitored by Bob. The aspect of quantifying the phase drift in Bob's measurement is already explored in various works [24,27,28,40,41]. This rotation is typically slow compared to the CV-QKD signal generation and detection rate. Specifically, the phase drift inside Bob's station could be due to various factors, including thermal effects. If the phase drift is relatively slow and/or the linewidth of the laser is narrow, the phase noise within the QKD data postprocessing blocks is minimal [24]. However, if the phase drift is quick and impulsive, the phase noise plays a role in limiting the achievable transmission distance in CV-QKD [42,43].

In Fig. 5, we plot the graph showing the phase drift inside Bob's station (from point A to BS in Fig. 1) being random and slow. This is experimentally measured, with the data taken from an asymmetric Mach-Zehnder interferometer, having 100 ns delay between the paths of signal and LO. This in principle mimics the phase drift inside Bob's station. We can see the change in the quadrature values, wherein the output is measured for certain intervals, as shown. One can think of this as effectively restarting the measurement afresh at the beginning of each measurement interval. We notice that the phase drift is random in nature. Additionally, it is also evident from the figure that the variation of phase drift is slow. In particular, compared to the QKD repetition rate (MHz), the frequency of phase drift is happening on the scale of ms (kHz). Therefore, over a short period of time ($\leqslant$ ms), $\theta_{\rm Bob}$ can be treated as constant for a block of quadrature measurements. In other words, in order to estimate the phase drift by Bob, the clock rate must be comparatively higher than the rate of the phase drift for our scheme to work. Bob later discloses $\theta_{\rm Bob}$ for each block of samples to Alice. This is then equivalent to the previous case in which the frame of measurement is fixed but unknown to Eve.

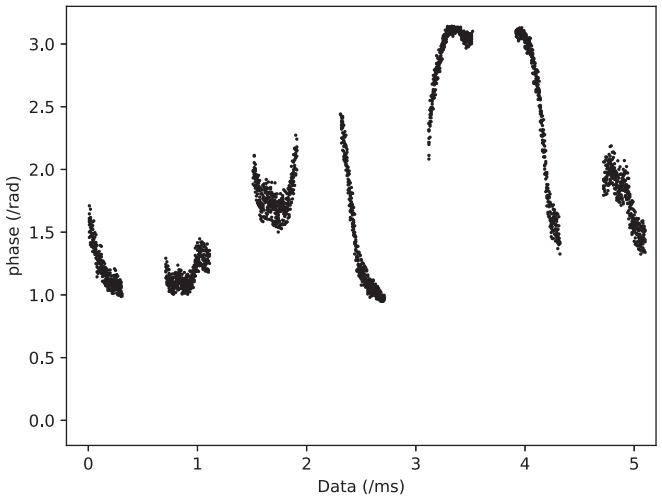

FIG. 5. Experimentally measured phase drift θ_{Bob} inside Bob's station, from the point A to BS in Fig. 1. The figure shows the randomness in the phase drift fluctuations along with the frequency of phase drift. We have taken the data with an asymmetric Mach-Zehnder interferometer, having 100 ns delay between the two paths: of signal and LO. This in principle emulates the phase drift due to thermal fluctuations inside Bob's station in a CV-QKD implementation.

IV. DISCUSSIONS AND CONCLUSIONS

The GMCS CV-QKD enables Alice and Bob to share secret keys using the amplitude- and phase-modulated coherent states. Bob randomly switches between the quadratures to monitor the variance of them. This prevents Eve from eavesdropping as she will have to necessarily increase the variance along certain angle even for the most optimal attack. Here, we have proposed a modified scheme, wherein the measurement of a single quadrature is performed by Bob along an arbitrary angle θ_{Bob} in the phase space. Bob estimates the angle θ_{Bob} and later, during the postprocessing, discloses it over the authenticated classical channel to Alice. By knowing the angle of rotation of the frame of measurement, Alice can apply an equivalent counterrotation ($-\theta_{\text{Bob}}$), and obtain a single quadrature value that coincides with that at Bob. The security of this single quadrature measurement scheme lies in the fact that Eve (as well as Alice) has no knowledge of the arbitrary angle θ_{Bob} during the quantum states transmission period. We also show that the eventual key rates with the proposed modification would yield identical results to that of GG02 protocol, specifically when θ_{Bob} is fixed. This is essentially due to the fact that when Alice's and Bob's reference frames are correlated, the maximum yield is same as GG02 protocol. However, as seen in Fig. 3, a phase drift of 5° would correspond to excess noise of $\xi = 0.0107$ resulting in a reduced key. In the simplest case of intercept and resend attack [44], Eve necessarily would have to squeeze along a certain angle of the intercepted signal, as she would introduce noise and increase the variance along that angle. And this will be observed by Bob as excess noise, and hence cannot evade her detection.

We consider the case of collective attack by Eve using an entangled cloner, wherein she entangles an ancillary mode to the coherent state sent by Alice. Her best strategy would be to measure her ancilla after the public announcement of the measurement basis, here the angle θ_{Bob}. The announcement of θ_{Bob} by Bob is equivalent to his announcement of choice of quadrature for the measurement in GG02 protocol. Here we map our scheme to an entanglement-based one, such that Alice prepares a TMSVS state and Eve entangles one of her modes of squeezed vacuum state with it to extract information. We notice that the reduction in entanglement between mode-1 and mode-2 of the TMSVS is correlated with the difference between the variances of the Alice's and Bob's quadratures, as given in Eq. (6). Thus, any such attack by Eve would change the variance of mode-2, and which is quantifiable for estimating the information leakage to Eve.

Another possible attack by Eve would be having multimode entanglement with mode-2, instead of using TMSVS of Eq. (3). In this case, Eve would necessarily use an entangled cloner of higher dimension, so that she can measure along all the possible values of θ_{Bob}. This would be similar to Eve using multimode in the case of a typical GMCS QKD protocol and measure along both the quadratures [45]. This would enable her to get the information before Bob's announcement of the measurement quadrature (θ_{Bob} in our case). However, she will have to squeeze the state along a certain angle and the footprint of Eve's entanglement in mode-2 is inevitable, observed as the increase of variance $V(\hat{x}_{\text{B}})$ in Eq. (6). Thus, any entanglement from Eve would necessarily increase the variance and this is inevitable. The primary advantage of using multimode entanglement would be to overcome the hurdle of waiting for Bob's announcement. Note that though Eve is enabled to have a cloner of higher dimension, it is still the collective attack.

The primary assumption in our scheme is that Bob needs an arbitrary angle of rotation in his frame of reference, which Eve has no knowledge of it beforehand. This is similar to the assumption of having random measurement of one of the quadrature, which Eve could not possibly influence. The proposed scheme is shown to be as feasible and secure as GMCS protocol, under the collective attack by Eve. Also, the proposed scheme is different from unidimensional CV-QKD protocols [46–49], in that, the state preparation in these protocols involve modulation of a single quadrature. Alice modulates only one quadrature in these protocols, but Bob measures both the quadratures to verify the uncertainty between them. In contrast, the Alice setup in our case remains to be identical to the GG02 protocol, and so is the proposed scheme more closer to it.

We note here that the single quadrature measurement scheme in this work is close to that in Ref. [50]. However, the basis of choice by Bob is continuously drifting for every hundreds of measurements in the former. In particular, Bob chooses $\theta_{\text{Bob}} \in [0, 2\pi]$ such that it is continuously changing. Whereas, in the current work, it can be kept constant for the whole run. In the GMCS protocol with homodyne measurement, for the case when Bob always measures in single quadrature and later announces the choice, Eve's success probability to hide her attack is 50%. One can think of a similar attack in the present case as well, wherein Eve too randomly chooses her rotated frame of measurement to be

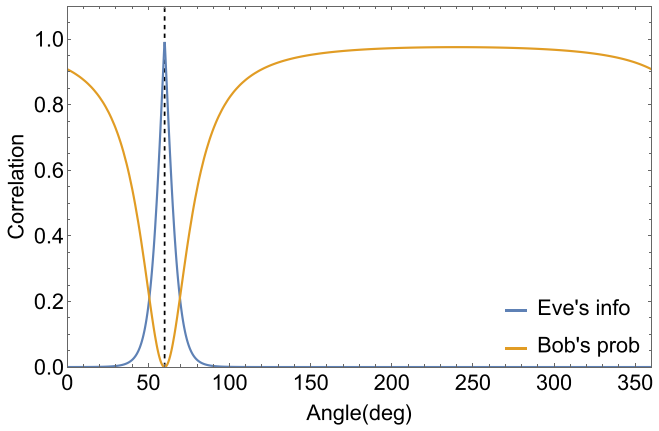

FIG. 6. The blue line indicates the normalized information of Eve with respect to the choice of her measurement angle. The orange line indicates the normalized probability of Bob finding about Eve's presence. Here the normalization is based on the phase space splicing by Bob, with the angle of measurement is taken to be 60°.

an arbitrary angle. But this is a nonoptimal attack, as Eve's success rate reduces with the increase in the resolution of the phase space of Bob's apparatus. Ideally, the probability to detect Eve's presence is

$$P_{\text{Bob}} = \frac{1}{N_{\{i\}}} \sum_i p_i, \tag{11}$$

where p_i is the respective probability of the phase space resolutions and $N_{\{i\}}$ is the resolution-dependent normalization factor. We note that Eve is unaware of Bob's angle of rotation in frame of reference (and the phase drift), until Bob's public announcement of the same. Let the arbitrary angle of measurement by Eve be θ_{E}. Thus, only at the angle $\theta_{\text{Bob}} = \theta_{\text{E}}$, $p_j = 0$. As $|\theta_{\text{Bob}} - \theta_{\text{E}}|$ increases, Eve's information decreases and Bob's probability to detect her increases.

Note that the above-mentioned attack is neither optimal nor realistic. Eve could further reduce P_{Bob} if she performs this nonoptimal attack probabilistically. In particular, only on a fraction f of the total transmissions, she could do this attack along a random angle. The primary advantage of this attack is that the footprint that she leaves is a fraction of the earlier case. That is, the probability of detection by Bob in this case would be $P'_{\text{Bob}} = f \cdot P_{\text{Bob}}$. However, the information that she gets is also reduced by the same factor, as ideally the success probability is equal for all the pulses. Below we quantify the normalized information that Eve would get and the corresponding probability of Bob finding about Eve's presence, for $f = 1$.

In the above case, let the resolution in the phase space be $\frac{1}{2\pi}$ for both Bob (and Eve). We find that the corresponding coefficient of the quadrature value for Eve is a function of $\cos(\theta_{\text{E}} \pm \theta_{\text{Bob}})$, with $\pm$ indicating the relative angle. Thus, the correlation between information leakage due to Eve's measurement and Bob's probability of finding squeezing by Eve is given in blue in Fig. 6. Here the normalization is due to the resolution in phase space. Let us consider the usual squeezing parameter quantifying the reduced variance with $V = 10^{\frac{-V_{\text{dB}}}{10}} = e^{-2r}$. Also, $\chi = re^{i\theta_{\text{Bob}}}$ is the squeezing parameter along the direction of θ_{Bob}. Thus, if we consider a total squeezing of $V_{\text{dB}} = 10$ dB by Eve, which corresponds to the squeezing parameter being $\chi = 1.15e^{i\theta_{\text{E}}}$. Thus, we find the probability of detecting Eve's presence to be,

$$P_{\text{E}} = \frac{1}{2\pi}\left[\frac{\mathcal{V}_{\text{B}}}{|\cos(\pi + (\theta_{\text{E}} \pm \theta_{\text{Bob}})/2)|}\right], \tag{12}$$

where $\mathcal{V}_{\text{B}}$ is the limiting factor for shot-noise measurement of Bob's detector. This is given in orange in Fig. 6. Thus, the success probability of Eve would be much lower in this case, and is quantified by the resolution of phase space and the respective weightages. Here we note that as the resolution of the phase space becomes finer, Eve's probability of concealing her presence decreases.

The current work limits its arguments and results to the Gaussian distribution-based protocol. The necessity of switching between the two quadratures is relaxed in a homodyne detection scheme and the protocol is shown to be identical to GG02 protocol [20]. The announcement of the angle of rotation by Bob is similar to that of announcement of chosen quadrature in the latter protocol. This works for the LLO-based systems as well as the TLO-based system used in this analysis. Conventionally, for LLO scheme, a homodyne detection setting is used for signal and heterodyne for reference pulses [24]. In TLO scheme, the phase drift is estimated using the pattern signals, which are comparatively at higher intensity than the QKD signals and are sent with each block of QKD signals [37–39]. The homodyne detection of signal in LLO scheme is particularly for reaching maximum transmission distance, however, it still involves switching between the two quadratures. Thus, our scheme avoids the use of phase modulator for homodyne detection of the signal, in GG02-like protocols, regardless if a TLO or LLO is implemented. Thus the proposed modification simplifies the protocol for CV-QKD systems that have homodyne detection setting as it overcomes the necessity of a randomly varying phase modulator at Bob's station. This is highly beneficial for practical implementation, especially in free-space CV-QKD with Gaussian modulation protocol.

ACKNOWLEDGMENTS

The authors thank Frédéric Grosshans for the useful discussions. V.N.R, T.S, and R.K acknowledge the funding support from EPSRC Quantum Communications Hub (Grant No. EP/T001011/1). E.T.H.M. thanks the School of Physics, Engineering and Technology, University of York for PhD funding.

DATA AVAILABILITY

The data that support the findings of this article are openly available [1].

APPENDIX A: COVARIANCE MATRIX

To find the covariance matrix of a two-mode squeezed vacuum states (TMSVS), we follow the standard formalism. In particular, each element of the covariance matrix at different stages are found as the follows. The diagonal ones are found

using $\langle\hat{\mathcal{Q}}_n^2\rangle - \langle\hat{\mathcal{Q}}_n\rangle^2$, where $\mathcal{Q}$ is the quadrature chosen for measurement in mode n. The off-diagonal elements are similarly found, except it is the average of the expectation values of the product of the modes as $1/2(\langle\hat{\mathcal{Q}}_n\hat{\mathcal{Q}}_m\rangle + \langle\hat{\mathcal{Q}}_m\hat{\mathcal{Q}}_n\rangle)$.

We find that the joint matrix of system ABE after Eve's entanglement with mode-2 to be,

$$\Sigma' = \begin{pmatrix} V\mathbb{1}_2 & \mathcal{X}_+P & \mathcal{X}_-P & 0 \\ \mathcal{X}_+P^{\mathrm{T}} & \mathcal{Z}_1 & \mathcal{Z} & \mathcal{Y}_-Q \\ \mathcal{X}_-P^{\mathrm{T}} & \mathcal{Z} & \mathcal{Z}_2 & \mathcal{Y}_+Q \\ 0 & \mathcal{Y}_-Q^{\mathrm{T}} & \mathcal{Y}_+Q^{\mathrm{T}} & W\mathbb{1}_2 + \frac{(W+1)}{2}S \end{pmatrix}, \quad \text{(A1)}$$

where,

$$\begin{aligned} \mathcal{X}_+ &= \sqrt{T(V^2-1)}, \\ \mathcal{X}_- &= -\sqrt{(1-T)(V^2-1)}, \\ \mathcal{Y}_- &= \sqrt{(1-T)(W^2-1)}, \\ \mathcal{Y}_+ &= \sqrt{T(W^2-1)}, \\ \mathcal{Z} &= \sqrt{T(1-T)}[W\mathbb{1}_2 - (V\mathbb{1}_2 + R)], \\ \mathcal{Z}_1 &= T(V\mathbb{1}_2 + R) + (1-T)(W\mathbb{1}_2), \\ \mathcal{Z}_2 &= (1-T)(V\mathbb{1}_2 + R) + T(W\mathbb{1}_2). \end{aligned}$$

APPENDIX B: QUANTIFYING EVE'S INFORMATION

Given Alice prepares TMSVS and keeps one mode to herself while sending another to Bob, we find that the commutation relation between them would be,

$$[\hat{x}_j, \hat{x}_k] = 2i\Omega_{jk}, \quad \text{(B1)}$$

where $\Omega = \oplus\{\{0,1\},\{-1,0\}\}$ is a 4×4 standard antisymmetric matrix, and $\hat{x} = (\hat{q_{\mathrm{A}}}, \hat{p_{\mathrm{A}}}, \hat{q_{\mathrm{B}}}, \hat{p_{\mathrm{B}}})^{\mathrm{T}}$ is the displacement vector. When the covariance matrix is of the form

$$V = \begin{pmatrix} A & C \\ C^{\mathrm{T}} & B \end{pmatrix}, \quad \text{(B2)}$$

with $A = A^{\mathrm{T}}$ and $B = B^{\mathrm{T}}$, the symplectic eigenvalues are given by,

$$\nu_\pm = \sqrt{\frac{\mu \pm \sqrt{\mu^2 - 4\,(\det V)}}{2}} \quad \text{(B3)}$$

where $\mu := (\det A) + (\det B) + 2(\det C)$ and $\det(\cdot)$ is the determinant. Thus, the von Newmann entropy of Σ'_{AB} is given by $S_{\mathrm{AB}} = g(\nu_+) + g(\nu_-)$, where

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

Similarly, we find $S_{\mathrm{A|B}}$ by the symplectic eigenvalues of the covariance matrix $\Sigma'_{A|B}$, taking the partial measurements on the covariance matrix of Eq. (B2). In particular, for a homodyne detection at Bob's station, we define the partial measurement of mode-2 transforming mode-1 as,

$$\Sigma'_{\mathrm{A|B}} = A - C(\Pi_x B\,\Pi_x)^{-1}C^{\mathrm{T}}, \quad \text{(B4)}$$

where $\Pi_x = \{\{\cos\theta, 0\}, \{0, \sin\theta\}\}$ being the measurement setting of Bob and $(\cdot)^{-1}$ indicating the pseudoinverse. Thus, we find the symplectic eigenvalue ν of $\Sigma'_{\mathrm{A|B}}$, and $S_{\mathrm{A|B}} = g(\nu)$.

APPENDIX C: GENERALIZED CASE

All the earlier cases involves Alice measuring in standard quadratures and Bob in his rotated frame of measurement. However, in principle, Alice too might measure in an arbitrary rotated angle and later establish the correlation of the angle with Bob. This would be a general case, wherein the measurement of TMSVS is θ_{A} for mode-1 and θ_{B} for mode-2. The covariance matrix for such a system is

$$\Sigma_{\mathrm{AB}} = \begin{pmatrix} V\mathbb{1}_2 + \frac{(V+1)}{2}R'_1 & \sqrt{V^2-1}P_1 \\ \sqrt{V^2-1}P_1^{\mathrm{T}} & V\mathbb{1}_2 + \frac{(V+1)}{2}R_1 \end{pmatrix}, \quad \text{(C1)}$$

where $R'_1 = \{\{0, \sin\theta_{\mathrm{A}}\}, \{\sin\theta_{\mathrm{A}}, 0\}\}$, $P_1 = \{\{CS, -\sin\theta_{\mathrm{A}}\}, \{-\sin\theta_{\mathrm{B}}, -1\}\}$, and $R_1 = \{\{0, \sin\theta_{\mathrm{B}}\}, \{\sin\theta_{\mathrm{B}}, 0\}\}$, with $CS = \cos\theta_{\mathrm{A}}\cos\theta_{\mathrm{B}} - \sin\theta_{\mathrm{A}}\sin\theta_{\mathrm{B}}$. The consequent joint system of ABE would be similar to Eq. (A1), but with different variances. However, after the announcement of θ_{B} and Alice rotating her frame to match, the respective mutual information and leaked information would be identical to the earlier case.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of the International Conference on Computers, Systems and Signal Processing* (1984).

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

[3] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, Advances in quantum cryptography, Adv. Optics Photon. **12**, 1012 (2020).

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

[5] I. D. Ivanovic, How to differentiate between non-orthogonal states, Phys. Lett. A **123**, 257 (1987).

[6] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[7] M. Koashi, Unconditional security of quantum key distribution and the uncertainty principle, J. Phys. Conf. Ser. **36**, 98 (2006).

[8] A. K. Ekert, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett. **67**, 661 (1991).

[9] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett. **68**, 3121 (1992).

[10] C. Marand and P. D. Townsend, Quantum key distribution over distances as long as 30 km, Opt. Lett. **20**, 1695 (1995).

[11] R. J. Hughes, G. L. Morgan, and C Glen Peterson, Quantum key distribution over a 48 km optical fibre network, J. Mod. Opt. **47**, 533–547 (2000).

[12] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, Quantum key distribution over 67 km with a plug&play system, New J. Phys. **4**, 41 (2002).

[13] C. Wang, J. Zhang, P. Wang, F. Deng, Q. Al, and G. Long, Experimental realization of quantum cryptography communication in free space, Sci. China. Ser. G **48**, 237 (2005).

[14] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[15] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).

[16] S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, P. Ye, Y. Zhou, G.-J. Fan-Yuan, F.-X. Wang, W. Chen *et al.*, Twin-field quantum key distribution over 830-km fibre, Nature Photon. **16**, 154 (2022).

[17] T. C. Ralph, Continuous variable quantum cryptography, Phys. Rev. A **61**, 010303(R) (1999).

[18] M. Hillery, Quantum cryptography with squeezed states, Phys. Rev. A **61**, 022309 (2000).

[19] M. D. Reid, Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations, Phys. Rev. A **62**, 062308 (2000).

[20] Frédéric Grosshans and P. Grangier, Continuous variable quantum cryptography using coherent states, Phys. Rev. Lett. **88**, 057902 (2002).

[21] S. L. Braunstein and P. Van Loock, Quantum information with continuous variables, Rev. Mod. Phys. **77**, 513 (2005).

[22] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Quantum cryptography without switching, Phys. Rev. Lett. **93**, 170504 (2004).

[23] U. L. Andersen, G. Leuchs, and C. Silberhorn, Continuous-variable quantum information processing, Laser Photon. Rev. **4**, 337 (2010).

[24] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Self-referenced continuous-variable quantum key distribution protocol, Phys. Rev. X **5**, 041010 (2015).

[25] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang *et al.*, Continuous-variable qkd over 50 km commercial fiber, Quantum Sci. Technol. **4**, 035006 (2019).

[26] P. Jouguet, Sébastien Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Experimental demonstration of long-distance continuous-variable quantum key distribution, Nat. Photon. **7**, 378 (2013).

[27] D. Huang, P. Huang, D. Lin, and G. Zeng, Long-distance continuous-variable quantum key distribution by controlling excess noise, Sci. Rep. **6**, 19201 (2016).

[28] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, Long-distance continuous-variable quantum key distribution over 202.81 km of fiber, Phys. Rev. Lett. **125**, 010502 (2020).

[29] C. Lupo, Towards practical security of continuous-variable quantum key distribution, Phys. Rev. A **102**, 022623 (2020).

[30] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and Grégoire Ribordy, Trojan-horse attacks on quantum-key-distribution systems, Phys. Rev. A **73**, 022320 (2006).

[31] H. Qin, R. Kumar, and R. Alléaume, Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution, Phys. Rev. A **94**, 012325 (2016).

[32] Z. Xing, X. Li, X. Ruan, Y. Luo, and H. Zhang, Phase compensation for continuous variable quantum key distribution based on convolutional neural network, in *Photonics* (MDPI, 2022), Vol. 9, p. 463.

[33] Y. Pan, L. Zhang, and D. Huang, Practical security bounds against trojan horse attacks in continuous-variable quantum key distribution, Appl. Sci. **10**, 7788 (2020).

[34] F. Laudenbach, C. Pacher, Chi-Hang Fred 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).

[35] C. Weedbrook, S. Pirandola, Raúl García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Gaussian quantum information, Rev. Mod. Phys. **84**, 621 (2012).

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

[37] S. J. A. G. Cosijns, M. J. Jansen, and H. Haitjema, Advanced optical incremental sensors: encoders and interferometers, in *Smart sensors and MEMS* (Elsevier, Amsterdam, 2018), pp. 245–290.

[38] X. Tang, R. Kumar, C. Sun, L. Zhang, Z. Chen, R. Jiang, H. Wang, and A. Zhang, Towards underwater coherent optical wireless communications using a simplified detection scheme, Opt. Express **29**, 19340 (2021).

[39] X. Tang, Z. Chen, Z. Zhao, R. Kumar, and Y. Dong, Experimental study on underwater continuous-variable quantum key distribution with discrete modulation, Opt. Express **30**, 32428 (2022).

[40] 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).

[41] N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, A. Kordts, S. Pirandola, T. B. Pedersen, M. Kolb, B. Ömer *et al.*, Practical continuous-variable quantum key distribution with composable security, Nat. Commun. **13**, 4740 (2022).

[42] B. Qi, Simultaneous classical communication and quantum key distribution using continuous variables, Phys. Rev. A **94**, 042340 (2016).

[43] A. Marie and R. Alléaume, Self-coherent phase reference sharing for continuous-variable quantum key distribution, Phys. Rev. A **95**, 012316 (2017).

[44] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, Experimental quantum cryptography, J. Cryptol. **5**, 3 (1992).

[45] Y. Zhang, Y. Bian, Z. Li, S. Yu, and H. Guo, Continuous-variable quantum key distribution system: Past, present, and future, Appl. Phys. Rev. **11** (2024).

[46] V. C. Usenko and Frédéric Grosshans, Unidimensional continuous-variable quantum key distribution, Phys. Rev. A **92**, 062337 (2015).

[47] V. C. Usenko, Unidimensional continuous-variable quantum key distribution using squeezed states, Phys. Rev. A **98**, 032321 (2018).

[48] P. Wang, X. Wang, and Y. Li, Security analysis of unidimensional continuous-variable quantum key distribution using uncertainty relations, Entropy **20**, 157 (2018).

[49] D. Bai, P. Huang, Y. Zhu, H. Ma, T. Xiao, T. Wang, and G. Zeng, Unidimensional continuous-variable measurement-device-independent quantum key distribution, Quantum Info. Proc. **19**, 1 (2020).

[50] W. Liu, J. Peng, P. Huang, S. Wang, T. Wang, and G. Zeng, Continuous-variable quantum key distribution based on continuous random basis choice, Chin. Phys. B **27**, 070305 (2018).