Performance analysis of continuous-variable quantum key distribution using non-Gaussian states

L. S. Aguiar1 · L. F. M. Borelli1 · J. A. Roversi1 · A. Vidiella-Barranco1

Received: 15 December 2021 / Accepted: 28 July 2022 / Published online: 20 August 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
In this study, we analyse the efficiency of a protocol with discrete modulation of continuous variable non-Gaussian states, that is, the coherent states having the addition of one photon followed by the subtraction of one photon (PASCS). We calculate lower bounds of the asymptotic key rates against Gaussian collective attacks based on the fact that for sufficiently small modulation variances we remain close to the protocol with Gaussian modulation. We compare the results of a four-state protocol (quadrature phase-shift-keying) using PASCS with the ones using coherent states, and show that under the same environmental conditions, the former always outperforms the latter, allowing to increase the maximum possible distance for secret key generation. Interestingly, we find that for the protocol using discrete-modulated PASCS, the noisier the line, the better will be its performance compared to the protocol using coherent states, showing that continuous variable non-Gaussian states can be considerably more advantageous for performing quantum key distribution in non-ideal situations.

Keywords Quantum cryptography · Quantum key distribution · continuous variables · non-Gaussian

1 Introduction
There has been increasing interest in continuous variables (CV) quantum key distribution (QKD) as an alternative to discrete variables (DV) QKD. An important step towards CV-QKD was the elaboration of a protocol using coherent states with added noise, that is, with Gaussian modulation of coherent states [1]. However, as original proposed, i.e. using direct reconciliation, the aforementioned protocol does not allow to perform QKD in transmission lines having losses greater than 50% (3 dB). This limitation was soon overcome using, for instance, either via post-selection [2] or by
reverse reconciliation procedures [3]. The protocol using Gaussian-modulated coherent states and reverse reconciliation was experimentally implemented with pulses containing a few hundred photons [4], and its security against Gaussian individual attacks based on entanglement was also demonstrated [3]. Later, it was established that the CV-QKD protocol with Gaussian-modulated coherent states is in fact secure against collective attacks [5, 6]. However the performance of such protocol is severely hindered by a lengthy error correction procedure, specially if the signal-to-noise ratio is small [7]. This in practice limits the protocol range to about 30 km, although the transmission distance can be increased up to \( \sim 50 \) km, as shown in [8], using a multi-dimensional reconciliation code, that is, basically creating a virtual binary modulation channel. An alternative approach to increase the range of the CV-QKD protocols is to employ a non-Gaussian (discrete) modulation of coherent states, rather than a Gaussian modulation [9–12]. In this case, the encoding is done using a small number of states (e.g. two or four), having fixed amplitudes, which allows for a much efficient reconciliation procedure and, consequently, a better performance. The security of a protocol with discrete modulation of coherent states against Gaussian attacks has been already proved [10], and more recently we may find in the literature discussions of such protocols against more general attacks, based on numerical optimizations [13, 14] as well as an analytical approach [15]. On the other hand, due to the intrinsic difficulty to implement quantum repeaters using light states with Gaussian statistics [16], it would be convenient to move away from the Gaussian domain. A possible way of circumventing the shortcomings related to quantum repeaters would be using non-Gaussian states of light as signal states. Previous studies have shown that there may be advantages if discrete-modulated continuous variables non-Gaussian states such as phase-coherent states [17] or photon-added-then-subtracted coherent states (PASCS) [18, 19] are used in place of coherent states. Indeed, the robustness of QKD protocols employing CV non-Gaussian states has been demonstrated for specific attacks of the eavesdropper [17–19], e.g., using a post-selection procedure [18]. Also, non-Gaussian operations such as photon subtraction [20] or quantum scissors [21] may improve the performance of discrete-modulated QKD protocols.

In this work, we are going to analyse the performance of a CV-QKD protocol with discrete modulation of PASCS, and compare it to the corresponding protocol based on coherent states. We will discuss a specific case, the four-state (quadrature phase-shift-keying) protocol, assuming that: (i) the signals are transmitted over a linear Gaussian quantum channel characterize by transmittance \( T \) and excess noise \( \xi \), and (ii) Eve is restricted to perform Gaussian collective attacks. Bearing this in mind, we are able to calculate a lower bound for the asymptotic secret key rate provided our signal states, the PASCS, remain close enough to coherent states. We show that the protocol with non-Gaussian states (PASCS) not only outperforms the equivalent protocol using coherent states regarding the transmission distance but is also significantly more robust against excess noise in the line.

This paper is organized as follows. In Sect. 2, we introduce the basic ideas of a protocol based on discrete modulation of coherent states and the functioning of the protocol with the PASCS. In Sect. 3, we present the calculation of the lower bounds on the asymptotic key rate considering collective attacks. In Sect. 4, we analyse our
results, that is, the performance of the protocol using PASCS compared to the usual protocol with coherent states. In Sect. 5, we discuss and summarize our results.

2 Protocol with non-Gaussian (discrete) modulation

The protocol to be analysed here is based on the four-state CV-QKD protocol, with discrete modulation and homodyne detection using reverse reconciliation [10].

2.1 Four-state protocol with coherent states

The protocol, in its prepare-and-measure version, works as follows: firstly, Alice chooses one state from a set of four continuous variable states, say: states \( |\psi_+\rangle, |\psi_+i\rangle \) representing bit 1, and states \( |\psi_-\rangle, |\psi_-i\rangle \) representing bit 0. In a second step, Alice sends a light signal prepared in the chosen state to Bob with probability \( \frac{1}{4} \), who randomly measures either the quadrature \( X \) or the quadrature \( Y \) via homodyne detection on the received signal. We consider the reverse reconciliation procedure, in which Bob sends side information to Alice in order to complete the process of secret key generation. For instance, if Bob obtains the value \( X_i \) in his quadrature measurement, he will reveal the absolute value \( |X_i| \) to Alice via a public classical channel. At this stage, Alice and Bob share a string of correlated bits. They still need to exchange some more information, via the classical channel, to perform error correction and privacy amplification, so that they share a secret key at the end of the process. The protocol was originally conceived using as signal states the coherent states \( |\psi_\pm\rangle = |\pm \alpha\rangle, |\psi_{\pm i}\rangle = |\pm i\alpha\rangle \), \((\alpha > 0)\), which can be expressed in a compact form as \( |\alpha_k\rangle \), where \( \alpha_k = i^k\alpha \) and \( k \in \{0, 1, 2, 3\} \).

The security of the protocol against collective attacks can be proved as shown in Ref. [10]. The state received by Bob, represented by the density operator \( \rho_4 = \frac{1}{4} \sum_{k=0}^{3} |\alpha_k\rangle\langle\alpha_k| \) can be diagonalized, i.e., \( \rho_4 = \sum_{j=1}^{3} \lambda_j |\phi_j\rangle\langle\phi_j| \), and a particular purification of \( \rho_4 \) can be obtained via the Schmidt decomposition

\[
|\Phi_4\rangle = \sum_{k=0}^{3} \sqrt{\lambda_k} |\phi_k\rangle|\phi_k\rangle = \frac{1}{2} \sum_{k=0}^{3} |\psi_k\rangle|\alpha_k\rangle,
\]  

where

\[
|\psi_k\rangle = \frac{1}{2} \sum_{m=0}^{3} i^{km} |\phi_m\rangle.
\]  

Now we use the entanglement-based version of the protocol, in which Alice prepares the entangled state \( |\Phi_4\rangle \) and performs a projective measurement \( \Pi_k = |\psi_k\rangle\langle\psi_k| \) on her side, thus preparing the state \( |\alpha_k\rangle \), which is sent to Bob through a linear quantum channel. The covariance matrix corresponding to a bipartite state \( |\Phi_4\rangle \) is
\[ \Gamma_{AB} = \begin{pmatrix} \langle X_A^2 \rangle & \langle X_A X_B \rangle \sigma_Z \\ \langle X_A X_B \rangle \sigma_Z & \langle X_B^2 \rangle \end{pmatrix}, \quad (3) \]

where

\[ \langle X_A^2 \rangle = \langle \Phi_4 \rvert 1 + 2\hat{a}^\dagger \hat{a} \rvert \Phi_4 \rangle = 1 + V_A \]
\[ \langle X_B^2 \rangle = \langle \Phi_4 \rvert 1 + 2\hat{b}^\dagger \hat{b} \rvert \Phi_4 \rangle = 1 + V_A \]
\[ Z_4 = \langle X_A X_B \rangle = \langle \Phi_4 \rvert \hat{a} \hat{b} + \hat{a}^\dagger \hat{b}^\dagger \rvert \Phi_4 \rangle, \quad (4) \]

with \( V_A = 2\alpha^2 \), \( I_2 = \text{diag} \,(1,1) \), and \( \sigma_Z \) is the Pauli matrix \( \sigma_Z = \text{diag} \,(1,-1) \).

The functions \( V_A \) and \( Z_4 \) above are necessary for the calculation of the asymptotic key rates. One can also compare the correlation \( Z_4 \) between Alice and Bob for the discrete modulation protocol with the correlation \( (Z_{\text{Gauss}}) \) corresponding to the protocol with Gaussian modulation in order to assess the “proximity” between these two systems, in order to justify some of the Gaussianity assumptions made. The matrices corresponding to the actions of the linear channel and the subsequent homodyne detection can then be obtained, allowing the calculation of the mutual information between Alice and Bob, \( I_{AB} \) as well as the information accessed by Eve, the Holevo information \( S_{BE} \). The resulting lower bound for the secret key rate \( K \) is basically the difference between \( I_{AB} \) and \( S_{BE} \). If the reconciliation step between Alice and Bob is not ideal, we should introduce a reconciliation efficiency parameter, here denoted as \( \beta \). Thus, the key rate is given by

\[ K = \beta I_{AB} - S_{BE}. \quad (5) \]

The lines above are a summary of the similar procedure we will be adopting for the PASCS, as shown in detail in Sect. 3 below.

### 2.2 Four-state protocol with photon-added-then-subtracted coherent states (PASCS)

We are interested in using as signal states the continuous variable, photon-added-then-subtracted coherent states \([22, 23]\) having just one photon added and one photon subtracted. Thus, from an initial coherent state \( \rvert \xi \rangle \) having amplitude \( \xi \in \mathbb{C} \), we can first add one photon to it, i.e., \( \rvert \phi_A \rangle \propto \hat{a}^\dagger \rvert \xi \rangle \) and then subtract one photon from the resulting state, obtaining the PASCS: \( \rvert 1, 1, \xi \rangle \propto \hat{a} \rvert \phi_A \rangle \). This state can be written in the Fock basis as \([23]\)

\[ \rvert 1, 1, \xi \rangle = \sum_{k=0}^{\infty} \frac{e^{-|\xi|^2/2} \xi^k (k+1)!}{\sqrt{1 + 3|\xi|^2 + |\xi|^4(k!)^{3/2}}} \rvert k \rangle. \quad (6) \]

An interesting feature of the state \( \rvert 1, 1, \xi \rangle \) is that it can be expressed as a superposition of a coherent state and a photon added coherent state (PACS), or \( \rvert 1, 1, \xi \rangle \propto \hat{a} \hat{a}^\dagger \rvert \xi \rangle \propto (1 + \hat{a}^\dagger \hat{a}) \rvert \xi \rangle \propto \rvert \xi \rangle + \xi \rvert \phi_A \rangle \). In other words, this specific PASCS basically
consists as a superposition of a Gaussian state (coherent state) with a non-Gaussian component (PACS) weighted by the amplitude $\zeta$ [18]. We emphasize that this feature will be important in our security analysis to be presented further, as the smaller the $\zeta$, the closer the PACS will be of a (Gaussian) coherent state. Besides, the protocol is optimized, i.e., we obtain the maximum possible key generation rates precisely for $\zeta$ small.

We firstly assume that PACS are generated from an initial coherent state $|\alpha\rangle$ with amplitude $\alpha > 0$. In the prepare-and-measure version of the protocol, Alice randomly chooses one of the four states $\{ |\psi_{\pm}^i\rangle = |1, 1, \pm \alpha\rangle, |\psi_{\pm i}^i\rangle = |1, 1, \pm i\alpha\rangle \}$ sending it to Bob with probability $1/4$ via a linear quantum channel. Thus, the state received by Bob can be represented by the following density operator

$$\rho'_4 = \frac{1}{4} \sum_{k=0}^{3} |1, 1, \alpha_k\rangle\langle \alpha_k, 1, 1|, \quad \alpha = i^k \alpha, \quad k \in \{0, 1, 2, 3\}. \quad (7)$$

that is, a statistical mixture of four PACS.

3 Calculation of the asymptotic secret key rates

The calculation of the asymptotic secret key rates of our protocol with discrete modulation of PACS is analogous to what it is done in the protocol using coherent states [10], briefly discussed in Sect. 2.1 above. We should point out that the extremality property of Gaussian states assures the calculation of an upper bound of the information accessible to Eve while she executes Gaussian collective attacks [24, 25]. Yet, this is not the most general situation, given that Gaussian attacks may not be the optimal ones [15] in this case. However, as our main objective here is to make a comparison between the protocol using PACS and the equivalent protocol using coherent states under the same environmental conditions, the key rates calculated here are just appropriate for that purpose.

To calculate the secret key rates we use the entanglement-based version of the protocol [10, 11, 26]. We diagonalize the density operator in Eq. (7), $\rho'_4 = \sum_{i=1}^{3} \lambda'_i |\phi'_i\rangle\langle \phi'_i|$, using the purification

$$|\Phi'_4\rangle = \sum_{k=0}^{3} \sqrt{\lambda'_k} |\phi'_k\rangle |\phi'_k\rangle, \quad (8)$$

with corresponding eigenvalues

$$\begin{align*}
\lambda'_0 &= e^{-a^2} \frac{(3a^2(-\operatorname{sen}(a^2) + \operatorname{seh}(a^2)) - (-1 + a^4)\cos(a^2) + (1 + a^4)\cosh(a^2))}{2(1 + 3a^2 + a^4)} \quad (9) \\
\lambda'_1 &= e^{-a^2} \frac{(3a^2(+\cos(a^2) + \cosh(a^2)) - (-1 + a^4)\operatorname{sen}(a^2) + (1 + a^4)\operatorname{senh}(a^2))}{2(1 + 3a^2 + a^4)} \quad (10)
\end{align*}$$

 Springer
\[ \lambda'_2 = e^{-\alpha^2} (3\alpha^2 (\sin(\alpha^2) + \sinh(\alpha^2)) + (-1 + \alpha^4) \cos(\alpha^2) + (1 + \alpha^4) \cosh(\alpha^2)) \\
/ 2(1 + 3\alpha^2 + \alpha^4) \]  
\hspace{1cm} (11)\\
\[ \lambda'_3 = e^{-\alpha^2} (3\alpha^2 (-\cos(\alpha^2) + \cosh(\alpha^2)) + (-1 + \alpha^4) \sin(\alpha^2) + (1 + \alpha^4) \sinh(\alpha^2)) \\
/ 2(1 + 3\alpha^2 + \alpha^4) \]  
\hspace{1cm} (12)\\
and eigenvectors
\[ |\phi'_{k}\rangle = e^{-\alpha^2/2} \frac{\alpha^{4n+k} (1 + k + 4n)!}{((4n + k)!)^{3/2}} |4n + k\rangle, \]  
\hspace{1cm} (13)\\
where \( k \in \{0, 1, 2, 3\} \).

Now we should be able to obtain the covariance matrix between Alice and Bob. Firstly we can invoke the extremality property of the Gaussian states \([24]\), according to which upper bounds of the relevant quantities, e.g., the accessible information to Eve (Holevo information \( S'_{BE} \)) can be found via the covariance matrix of a Gaussian state having the same covariance matrix as that of our system. Also, for a protocol with Gaussian modulation of Gaussian states, it is straightforward to compute the covariance matrix from the data observed in the prepare-and-measure version of the protocol. On the other hand, this might not be possible to accomplish in the case of having non-Gaussian modulation of non-Gaussian states. However, we expect that by restricting Eve’s action to Gaussian attacks \([10]\), it is legitimate to employ the following covariance matrix \( \Gamma'_A B \) characteristic of a Gaussian state, which can obtained from the data observed, i.e.,
\[ \Gamma'_A B = \begin{pmatrix} \langle X'_A X'_A \rangle & \langle X'_A X'_B \rangle \sigma Z \\ \langle X'_A X'_B \rangle \sigma Z & \langle X'_B X'_B \rangle \end{pmatrix}. \]  
\hspace{1cm} (14)\\
Due to the symmetry of the state \( |\Phi'_4\rangle \), the matrix elements as well as Alice’s modulation variance \( V'_A \) can be directly calculated, resulting in
\[ \langle X'_A X'_A \rangle = \langle \Phi'_4 | 1 + 2a^\dagger a | \Phi'_4 \rangle = 1 + V'_A \] 
\[ \langle X'_B X'_B \rangle = \langle \Phi'_4 | 1 + 2b^\dagger b | \Phi'_4 \rangle = 1 + V'_A, \]  
\hspace{1cm} (15)\\
with
\[ V'_A(\alpha) = \frac{2\alpha^2 (\alpha^4 + 5\alpha^2 + 4)}{1 + 3\alpha^2 + \alpha^4}. \]  
\hspace{1cm} (16)\\
The correlation between Alice and Bob is given by:
\[ Z'_4 = \langle X'_A X'_B \rangle = \langle \Phi'_4 | (ab + a^\dagger b^\dagger) | \Phi'_4 \rangle, \]  
\hspace{1cm} (17)
\[ Z'_4(\alpha) = \frac{e^{-2\alpha^2 \alpha^2}}{2 \left( 1 + 3\alpha^2 + \alpha^4 \right)^2} \left( \frac{A^2}{\sqrt{\lambda'_0 \lambda'_1}} + \frac{B^2}{\sqrt{\lambda'_1 \lambda'_2}} + \frac{C^2}{\sqrt{\lambda'_2 \lambda'_3}} + \frac{D^2}{\sqrt{\lambda'_3 \lambda'_0}} \right), \tag{18} \]

where

\[
A = -\left( \alpha^4 - 2 \right) \cos(\alpha^2) + \left( \alpha^4 + 2 \right) \cosh(\alpha^2) + 4\alpha^2 \left( \sinh(\alpha^2) - \sin(\alpha^2) \right) \\
B = 4\alpha^2 \cos(\alpha^2) + 4\alpha^2 \cosh(\alpha^2) - \left( \alpha^4 - 2 \right) \sin(\alpha^2) + \left( \alpha^4 + 2 \right) \sinh(\alpha^2) \\
C = \left( \alpha^4 - 2 \right) \cos(\alpha^2) + \left( \alpha^4 + 2 \right) \cosh(\alpha^2) + 4\alpha^2 \left( \sin(\alpha^2) + \sinh(\alpha^2) \right) \\
D = -4\alpha^2 \cos(\alpha^2) + 4\alpha^2 \cosh(\alpha^2) + \left( \alpha^4 - 2 \right) \sin(\alpha^2) + \left( \alpha^4 + 2 \right) \sinh(\alpha^2). \tag{19} \]

We can estimate how close it is possible to get to a protocol with Gaussian modulation by making a direct comparison between the correlations \( Z'_4 \) and \( Z'_{\text{Gauss}} \), where

\[ Z'_{\text{Gauss}} = \sqrt{(1 + V'_A)^2 - 1}, \]

checking whether there is a range of amplitudes \( \alpha \) (modulation variances \( V'_A \)) for which \( Z'_4 \approx Z'_{\text{Gauss}} \). In Fig. 1 we have plotted the correlation curves as a function of the amplitude \( \alpha \) of the PASCS for the discrete-modulated four-state protocol compared to the Gaussian-modulated protocol. We have also included a plot of the two-state protocol to show that the four-state protocol is in fact advantageous. We note that for small values of the amplitude \( \alpha \) the curves \( Z'_4(\alpha) \) and \( Z'_{\text{Gauss}}(\alpha) \) are nearly indistinguishable. To be more accurate, we may expand the correlation functions up to the third order in \( \alpha \),

\[
Z'_4 \approx 4\alpha + 4 \left( 3\sqrt{2} - 4 \right) \alpha^3, \tag{20} \\
Z'_{\text{Gauss}} \approx 4\alpha + \frac{9}{2} \alpha^3. \tag{21} 
\]

We have that, for \( \alpha \approx 0.2 \) the relative difference between \( Z'_4 \) and \( Z'_{\text{Gauss}} \) is just about \( \approx 3\% \). Besides, the optimum value of the amplitude, \( \alpha_{\text{opt}} = 0.13 \) (maximizes the key generation rate for a low-noise line), lies within the appropriate range i.e.,

\[ Z'_4(\alpha = 0.13) \approx Z'_{\text{Gauss}}(\alpha = 0.13). \]

We may carry on the security analysis by assuming that the light signals are transmitted via a quantum channel characterized by transmittance \( T = \eta 10^{-0.02d} \) and excess noise \( \xi \), that is, a standard telecom fiber with losses of 0.2 dB/km. Here \( \eta \) is the quantum efficiency of the homodyne detection and \( d \) the distance between Alice and Bob. The covariance matrix \( \gamma_{AB} \) after the transmission reads

\[
\gamma_{AB} = \begin{pmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB} & \gamma_B \end{pmatrix}, \tag{22} 
\]
Fig. 1 Correlations between Alice and Bob modes for the PASCS-based protocol as a function of the amplitude $\alpha$. The solid line curve represents the Gaussian modulated protocol ($Z_{\text{Gauss}}'$), the dashed-dotted line curve the four-state protocol ($Z_4'$), and the dashed line curve the two-state protocol ($Z_2'$). For $\alpha \approx 0.2$ the relative difference between $Z_4'$ and $Z_{\text{Gauss}}'$ is $\approx 3\%$.

where

$$
\gamma_A = (1 + V'_A)\mathbb{I}_2 \\
\gamma_B = (TV'_A + 1 - T\xi)\mathbb{I}_2 \\
\sigma_{AB} = Z_4'\sqrt{T}\sigma_z.
$$

(23)

Following the transmission through the non-ideal linear quantum channel, Bob performs a homodyne detection on the received signal, represented by the transformations:

$$
\gamma_{A|B}^{\text{hom}} = \gamma_A - \sigma_{AB}(X\gamma_B X)^{MP}\sigma_{AB}^T,
$$

(24)

where $MP$ is the Moore–Penrose pseudo-inverse and $X = \text{diag}(1, 0)$.

The resulting (reduced) covariance matrix after Bob’s measurement is

$$
\gamma_{A|B}^{\text{hom}} = \begin{pmatrix}
V'_A + 1 - \frac{TZ_4'^2}{TV'_A + 1 - T\xi} & 0 \\
0 & V'_A + 1
\end{pmatrix}.
$$

(25)

We may now calculate $I'_{AB}$, the mutual information between Alice and Bob’s data. Our protocol comprises a discrete modulation of non-Gaussian states, for which there is no closed-form expression for $I'_{AB}$ [15]. However, for small values of the amplitude $\alpha$ (variance $V'_A$) we get very close to the fully Gaussian version of the protocol, and therefore we will assume that $I'_{AB}$ is well approximated by [27]

$$
I'_{AB} = \frac{1}{2} \log \left( \frac{V'_A}{V'_{A|B}} \right),
$$

(26)

where $V'_A$ is the modulation variance in Eq. (16), and $V'_{A|B}$ the conditional quadrature variance [28, 29], which is equal to the first diagonal element of the conditional matrix $\gamma_{A|B}^{\text{hom}}$. 

\( \odot \) Springer
\[ V_{A|B} = V_A' + 1 - \frac{T Z_4'^2}{TV_A' + 1 - T \xi}. \quad (27) \]

The upper bound on the information Eve can access by carrying out Gaussian collective attacks, the Holevo information \( S'_{BE} \), can be obtained from the covariance matrix \( \Gamma'_{AB} \) between Alice and Bob. For the PASCS, we have that

\[ S'_{BE} = G \left( \frac{v_1 - 1}{2} \right) + G \left( \frac{v_2 - 1}{2} \right) - G \left( \frac{v_3 - 1}{2} \right), \quad (28) \]

with

\[ G(x) = (x + 1) \log(x + 1) - (x) \log(x), \quad (29) \]

\[ v_1 = \sqrt{\frac{1}{2} \left( \Delta + \sqrt{\Delta^2 - 4 \delta} \right)}, \quad (30) \]

\[ v_2 = \sqrt{\frac{1}{2} \left( \Delta - \sqrt{\Delta^2 - 4 \delta} \right)}, \quad (31) \]

\[ v_3 = \sqrt{(V_A' + 1) \left[ (V_A' + 1) - \frac{T Z_4'^2}{\xi T + TV_A' + 1} \right]}, \quad (32) \]

\[ \Delta = \xi^2 T^2 + (T^2 + 1) V_A'^2 + 2V_A' (\xi T^2 + T + 1) + 2 \xi T - 2 T Z_4'^2 + 2, \quad (33) \]

and

\[ \delta = \left( TV_A'^2 + V_A' (\xi T + T + 1) + T (\xi - Z_4'^2) + 1 \right)^2. \quad (34) \]

If we use now the expressions in Eqs. (16), (27), (26) and (28), we obtain a lower bound for the asymptotic secret key rate \( K' \) under collective attacks, that is:

\[ K' = \beta I'_{AB} - S'_{BE}, \quad (35) \]

where \( \beta \) is the reconciliation efficiency of the protocol.

4 Results

Now we would like to present our results concerning the performance of a CV-QKD protocol using PASCS (key rates \( K' \) in Eq. (35)) and compare them to the protocol with coherent states (key rates \( K \) in Eq. (5)). We numerically evaluated optimal modulation amplitudes for each protocol, which are those that maximize the key rate corresponding to the smallest excess noise value used here (\( \xi = 0.002 \)). The optimum amplitudes
Fig. 2 Secret key rate of the PASCS-based four-state protocol with homodyne detection, photodetector quantum efficiency $\eta = 100\%$ and perfect reconciliation efficiency ($\beta = 100\%$). From right to left, the excess noise $\xi$ is 0.002, 0.004, 0.006, 0.008 and 0.01. The amplitude $\alpha_{\text{opt}} = 0.13$, which maximizes the key rate for $\xi = 0.002$, has been used in all plots.

Fig. 3 Secret key rate of the PASCS-based four-state protocol with homodyne detection, photodetector quantum efficiency $\eta = 60\%$ and imperfect reconciliation efficiency ($\beta = 80\%$). From right to left, the excess noise $\xi$ is 0.002, 0.004, 0.006, 0.008 and 0.01. The amplitude $\alpha_{\text{opt}} = 0.13$, which maximizes the key rate for $\xi = 0.002$, has been used in all plots.

obtained are $\alpha_{\text{opt}}^{(\text{PASCS})} \approx 0.13$ and $\alpha_{\text{opt}}^{(\text{coh})} \approx 0.35$ (modulation variance $V_A \approx 0.25$), for the PASCS and for the coherent states protocol, respectively.

In Fig. 2 it is shown the key generation rate for the ideal case regarding the detection stage, i.e., with Bob performing homodyne detection with efficiency $\eta = 100\%$ and a perfect reconciliation rate ($\beta = 100\%$). The graph shows the influence of excess noise on the key rate and transmission distance. We note that for very low values of excess noise, $\xi = 0.002$ and $\xi = 0.004$, we can have a secure key generation (at a rate $K \approx 10^{-10}$ bits/pulse) with a transmission range exceeding 400 km before saturation.

In Fig. 3 we analyse a more realistic case where we consider efficiencies of $\beta = 80\%$ for the reconciliation, and $\eta = 60\%$ for the photodetector. There is a drop in the transmission distance for a given key rate (as expected), and this gets worse for larger values of $\xi$ (excess noise), as can be clearly seen in the figure.

In what follows we directly compare the performance of the protocol using PASCS with the one using coherent states [10]. In Fig. 4 we have plotted the key rate as a function of the transmission distance for perfect reconciliation ($\beta = 100\%$) and photodetector efficiency $\eta = 100\%$. This is done for both low excess noise ($\xi = 0.002$) and higher excess noise ($\xi = 0.01$). Remarkably, the PASCS-based protocol has a significantly superior performance if the excess noise is higher, as shown in the two curves on the left in Fig. 4, although the curves in the low noise case (on the right) do not differ much. For the protocol with coherent states the key rate saturates at a transmission distance of $\approx 140$ km ($K \approx 10^{-5}$ bits/pulse), while for the PASCS this occurs at a transmission distance of $\approx 220$ km ($K \approx 10^{-7}$ bits/pulse).
Fig. 4 Comparison between the key generation rates from the protocol using PASCS with that of the protocol using coherent states. Both are four-state protocols with homodyne detection, photodetector quantum efficiency of 100% and perfect reconciliation efficiency ($\beta = 100\%$). From right to left, excess noise is 0.002 (solid line for the PASCS and dashed line for the coherent states) and 0.01 (dashed-dotted line PASCS and dotted line for the coherent states). The amplitudes used in the plots (maximize the key rates for $\xi = 0.002$), are $\alpha_{\text{opt}}^{(\text{PASCS})} = 0.13$ and $\alpha_{\text{opt}}^{(\text{coh})} = 0.35$, for the PASCS and coherent states, respectively.

Fig. 5 Comparison between the key generation rates from the protocol using PASCS with that of the protocol using coherent states. Both are four-state protocols with homodyne detection, photodetector quantum efficiency $\eta = 60\%$ and imperfect reconciliation efficiency ($\beta = 80\%$). From right to left, excess noise is 0.002 (solid line for the PASCS and dashed line for the coherent states) and 0.01 (dashed-dotted line PASCS and dotted line for the coherent states). The amplitudes used in the plots (maximize the key rates for $\xi = 0.002$), are $\alpha_{\text{opt}}^{(\text{PASCS})} = 0.13$ and $\alpha_{\text{opt}}^{(\text{coh})} = 0.35$, for the PASCS and coherent states, respectively.

If the conditions in Bob’s station are non-ideal, e.g., with a reconciliation coefficient $\beta = 80\%$ and photodetector efficiency $\eta = 60\%$, the performance of the protocols will be of course degraded. However, the use of PASCS in place of coherent states remains advantageous, as the former still allows for higher key generation rates and a longer transmission range especially for high excess noise, as shown in the two curves on the left in Fig. 5.

The performance of a CV-QKD protocol based on quadrature measurements depends on the noise distribution of the states in phase space. To illustrate the extent to which a Gaussian modulation can be approximated by a set of four states, we consider the Wigner functions of the quantum states, and compare the functions of
the coherent states with those of the PASCS. In Fig. 6a we have plots of the Wigner functions of the mixed state constituted by PASCS with amplitude $\alpha^{PASCS}_{opt} = 0.13$ and in Fig. 6b of coherent states with amplitude $\alpha^{coh}_{opt} = 0.35$, both optimized for excess noise $\xi = 0.002$. Firstly, we note that the contours of the PASCS Wigner function are “banana-shaped” [18], in contrast to the coherent state contours (circumferences). As a consequence, the region of phase-space covered by the Wigner functions in the PASCS case is slightly closer to a circumference (Gaussian modulation), than for the coherent states, as seen in Fig. 6. Also, in Fig. 7 we plotted the differences $\Delta S^{PASCS}_{BE} = S^{PASCS}_{BE} - S^{BE}_{Gauss}$ for the PASCS compared to $\Delta S^{coh}_{BE} = S^{coh}_{BE} - S^{BE}_{Gauss}$ for the coherent states, which shows that the PASCS-based protocol provides a tighter bound in Eve’s Holevo information.

5 Conclusion

We conducted an analysis of the performance of a CV-QKD protocol using photon-added-then-subtracted coherent states (PASCS) compared to the equivalent protocol using coherent states. Thus, in addition to having a non-Gaussian modulation of four states, the states themselves are non-Gaussian. The PASCS can be written as a quantum superposition of a coherent state $|\alpha\rangle$ and a photon-added coherent state multiplied by the amplitude $\alpha$. Hence, despite being non-Gaussian states, they become “close” to the coherent (Gaussian) states for small amplitudes $\alpha$ of the initial state, which brings us closer to the Gaussian domain. We therefore expect that with a sufficiently small $\alpha$ (small modulation variance $V_A'$), the system will remain close to Gaussian, allowing a reasonable estimate of the asymptotic secret key rate even considering the more restrictive Gaussian collective attacks. We should mention that the operation of photon addition followed by photon subtraction on weak coherent states acts roughly as a noiseless amplifier in the sense that an initial weak coherent state $|\zeta\rangle$ would become approximately the state $|2\zeta\rangle$ [30]. Indeed, noiseless amplification has been already proposed as a possible way of increasing the transmission distance in a CV-QKD protocol, as discussed in Refs. [31–33].

We concluded that, with regard to the estimates of the secret key rates we have obtained, the PASCS-based protocol outperforms the coherent state-based one in every scenario we studied. As shown in our numerical results, maximum transmission distances have been increased, i.e., the curves saturate at longer distances for the PASCS compared to the coherent state ones. Apart from that, the PASCS protocol is considerably more robust against excess noise than the coherent states protocol. This is particularly noticeable for noisier transmission lines (larger $\xi$), where we could verify that the key rate is considerably less degraded in the PASCS-based protocol, as seen in Figs. 4 and 5. We would also like to recall that the use of non-Gaussian states could allow the implementation of quantum repeaters, which would further increase the transmission distance of the secret key. Our work is a step towards the development of CV-QKD protocols using non-Gaussian states, aiming at the improvement of the efficiency of quantum cryptography systems.
Fig. 6 Contour plots of the Wigner functions of states: a $\rho_4'$ (4-PASCS), and b $\rho_4$ (4-coherent states). We have used the optimum modulation amplitudes in each case: $\alpha_{\text{opt}}^{(\text{PASCS})} = 0.13$ and $\alpha_{\text{opt}}^{(\text{coh})} = 0.35$, respectively. It is apparent that the PASCS case (left graph) brings us closer to the (perfect) Gaussian modulation than the coherent states (right graph).

Fig. 7 Differences between the Holevo information functions. The continuous blue curve corresponds to the PASCS, $\Delta S_{BE}^{(\text{PASCS})} = S_{BE}^{(\text{PASCS})} - S_{BE}^{(\text{Gauss})}$, and the dashed red curve to the coherent states, $\Delta S_{BE}^{(\text{coh})} = S_{BE}^{(\text{coh})} - S_{BE}^{(\text{Gauss})}$. It is shown that the PASCS protocol provides a tighter bound than the coherent states one.

Acknowledgements This work has been supported by Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq) Brazil, via the Instituto Nacional de Ciência e Tecnologia - Informação quântica (INCT-IQ), grant No 465469/2014-0.

Data availability The manuscript has no associated data.

References

1. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. Phys. Rev. Lett. 88, 057902 (2002)
2. Silberhorn, Ch., Ralph, T.C., Lütkenhaus, N., Leuchs, G.: Continuous variable quantum cryptography: beating the 3 dB loss limit. Phys. Rev. Lett. 89, 167901 (2002)
3. Grosshans, F., Grangier, P.: Reverse reconciliation protocols for quantum cryptography with continuous variables. arXiv preprint arXiv:quant-ph/0204127 (2002)
4. Grosshans, F., et al.: Quantum key distribution using Gaussian-modulated coherent states. Nature 421, 238 (2003)
5. Christandl, M., Renner, R., Ekert, A.: arXiv:quant-ph/0402131 (2004)
6. Grosshans, F.: Collective attacks and unconditional security in continuous variable quantum key distribution. Phys. Rev. Lett. 94, 020504 (2005)
7. Lodewyck, J., et al.: Quantum key distribution over 25 km with an all-fiber continuous-variable system. Phys. Rev. A 76, 042305 (2007)
8. Jouguet, P., et al.: Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat. Photonics 7, 378 (2013)
9. Namiki, R., Hirano, T.: Security of quantum cryptography using balanced homodyne detection. Phys. Rev. A 67, 022308 (2003)
10. Leverrier, A., Grangier, P.: Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys. Rev. Lett. 102, 180504 (2009)
11. Leverrier, A., Grangier, P.: Erratum: Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys. Rev. Lett. 106, 259902 (2011)
12. Leverrier, A., Grangier, P.: Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. Phys. Rev. A 83, 042312 (2011)
13. Ghorai, S., Grangier, P., Diamanti, E., Leverrier, A.: Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. Phys. Rev. X 9, 021059 (2019)
14. Denys, A., Brown, P., Leverrier, A.: Explicit asymptotic secret key rate of continuous variable quantum key distribution with an arbitrary modulation. Quantum 5, 540 (2021)
15. Leverrier, A. et al.: Quantum communications with Gaussian and non-Gaussian states of light In: International Conference on Quantum Information, OSA Technical Digest (CD) (Optical Society of America, 2011), paper QMF1. http://www.opticsinfobase.org/abstract.cfm?URI=ICQI-2011-QMF1
16. Borelli, L.F.M., Aguiar, L.S., Roversi, J.A., Vidiella-Barranco, A.: Quantum key distribution using continuous-variable non-Gaussian states. Quantum Inf. Process. 15, 893–904 (2016)
17. Srikara, S., Tapliyal, K., Pathak, A.: Continuous variable B92 quantum key distribution protocol using single photon added and subtracted coherent states. Quantum Inf. Process. 19, 371 (2020)
18. Li, F., Wang, Y., Liao, Q., Guo, Y.: Four-state continuous-variable quantum key distribution with photon subtraction. Int. J. Theor. Phys. 57, 2755 (2018)
19. Pariggi, V., Zavatta, A., Kim, M., Bellini, M.: Probing quantum commutation rules by addition and subtraction of single photons to/from a light field. Science 317, 1890 (2007)
20. Wang, Z., Yuan, H., Fan, H.: Nonclassicality of the photon addition-then-subtraction coherent state and its decoherence in the photon-loss channel. J. Opt. Soc. Am. B 28, 1964 (2011)
21. García-Patrón, R., Cerf, N.J.: Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys. Rev. Lett. 97, 190503 (2006)
22. Navascués, M., Grosshans, F., Acín, A.: Optimality of Gaussian attacks in continuous-variable quantum cryptography. Phys. Rev. Lett. 97, 190502 (2006)
23. Grosshans, F., et al.: Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quantum Inf. Comput. 3, 535–552 (2003)
24. Shannon, C.E.: A mathematical theory of communication. Bell Syst. Tech. J. 27, 379 (1948)
25. Zhao, W., et al.: Unidimensional continuous-variable quantum key distribution with discrete modulation. Phys. Lett. A 384, 126061 (2020)
26. Wang, X., et al.: Realistic rate-distance limit of continuous-variable quantum key distribution. Opt. Express 27, 13372 (2019)
27. Zavatta, A., Fiurášek, J., Bellini, M.: A high-fidelity noiseless amplifier for quantum light states. Nat. Photonics 5, 52 (2011)
28. Blandino, R., Leverrier, A., Barbieri, M., Etese, J., Grangier, P., Tuille-Brouri, R.: Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier. Phys. Rev. A 86, 012327 (2012)
29. Walk, N., Ralph, T.C., Symul, T., Lam, P.K.: Security of continuous-variable quantum cryptography with Gaussian postselection. Phys. Rev. A 87, 020303(R) (2013)
33. Fiurášek, J., Cerf, N.J.: Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. Phys. Rev. A 86, 060302(R) (2012)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Springer Nature or its licensor holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.