



UNIVERSIDADE ESTADUAL DE CAMPINAS
SISTEMA DE BIBLIOTECAS DA UNICAMP
REPOSITÓRIO DA PRODUÇÃO CIENTÍFICA E INTELLECTUAL DA UNICAMP

Versão do arquivo anexado / Version of attached file:

Versão do Editor / Published Version

Mais informações no site da editora / Further information on publisher's website:

<https://link.springer.com/article/10.1007/s11128-015-1193-8>

DOI: 10.1007/s11128-015-1193-8

Direitos autorais / Publisher's copyright statement:

©2016 by Springer. All rights reserved.

DIRETORIA DE TRATAMENTO DA INFORMAÇÃO

Cidade Universitária Zeferino Vaz Barão Geraldo

CEP 13083-970 – Campinas SP

Fone: (19) 3521-6493

<http://www.repositorio.unicamp.br>

Quantum key distribution using continuous-variable non-Gaussian states

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

Received: 3 September 2014 / Accepted: 14 November 2015 / Published online: 30 November 2015
© Springer Science+Business Media New York 2015

Abstract In this work, we present a quantum key distribution protocol using continuous-variable non-Gaussian states, homodyne detection and post-selection. The employed signal states are the photon added then subtracted coherent states (PASCS) in which one photon is added and subsequently one photon is subtracted from the field. We analyze the performance of our protocol, compared with a coherent state-based protocol, for two different attacks that could be carried out by the eavesdropper (Eve). We calculate the secret key rate transmission in a lossy line for a superior channel (beam-splitter) attack, and we show that we may increase the secret key generation rate by using the non-Gaussian PASCS rather than coherent states. We also consider the simultaneous quadrature measurement (intercept-resend) attack, and we show that the efficiency of Eve’s attack is substantially reduced if PASCS are used as signal states.

Keywords Quantum cryptography · Continuous variables · Non-Gaussian states

1 Introduction

The first quantum key distribution (QKD) protocol, conceived in 1984 (BB84) [1], is an inherently discrete protocol; it not only requires (discrete) single-photon sources, but the modulation of the signals is also discrete. Although the ideal BB84 has been

✉ A. Vidiella-Barranco
vidiella@ifi.unicamp.br

L. F. M. Borelli
borelli@ifi.unicamp.br

¹ Instituto de Física “Gleb Wataghin”, Universidade Estadual de Campinas,
Campinas, São Paulo 13083-859, Brazil

proved unconditionally secure [2,3], there are still practical shortcomings: Reliable single-photon sources (used by Alice, the sender) are hard to build, and photon counters (used by Bob, the receiver) limit the key generation rate. Notwithstanding fully discrete-variable protocols have been successfully accomplished over distances of more than 250 km in ultra-low loss fibers [4]. Meanwhile, several alternative QKD protocols using other (continuous-variable) light sources have been proposed employing, for instance, squeezed states [5–8] or coherent states [5,9–11]. In such continuous-variable protocols, the key may be encoded by Alice in the quadrature variables, and Bob will be allowed to employ photomultipliers (which are faster than single-photon detectors) to read the signals via homodyne detection. Continuous-variable protocols may be classified as: (1) all continuous protocols [9,10], for which Alice prepares, for instance, Gaussian states such as coherent states, with random amplitudes drawn from a continuous Gaussian distribution, or (2) hybrid protocols [8,12–14]. In the hybrid protocols, Alice uses light prepared in continuous-variable light signals, but the encoding is made using a discrete set of states (e.g., four states). At the same time, we are witnessing considerable advances concerning the implementation of QKD in real-world conditions [15,16] which usually requires long-distance communication. The all continuous-variable protocols are mostly based on coherent states, which are easier to generate than other quantum states of light. However, coherent state-based protocols are normally more effective in shorter ranges, due to poor performance in low signal-to-noise ratio conditions. Recently, though, a record of 80 km has been established for an improved version [17] of the GG02 continuous-variable protocol [9]. In spite of those advances, it would be interesting to seek other possibilities for long-distance QKD. A viable alternative are the hybrid continuous/discrete protocols, which may employ either Gaussian or non-Gaussian states. We would like to remark that continuous-variable non-Gaussian states (contrary to Gaussian states) may allow the use of quantum repeaters in order to increase the transmission range of a practical QKD system [18].

In this paper, we propose a protocol for QKD based on continuous-variable non-Gaussian states, viz., photon added then subtracted coherent states (PASCs). The PASCs may be generated in a relatively straightforward way departing from a Gaussian (coherent) state [19]. We may then formulate a protocol similar to already existing continuous-variable protocols [8,13] employing homodyne detection and post-selection [20]. We encode bits 0 and 1 in two pairs of PASCs (each pair containing states with opposite phases), which are randomly prepared by Alice. Alice sends light signals to Bob through a lossy line, who will perform homodyne detections on them. In order to demonstrate the robustness of our protocol against eavesdropping, we calculate the transmitted secret bit rate, (S_{AB}) [21] for a beam-splitter attack (superior channel attack), as well as for a kind of intercept-resend attack (simultaneous measurement quadrature attack). That analysis will allow us to assess the security of the protocol using two different attacks as well as to establish a comparison with the performance of other protocols. Our paper is organized as follows. In Sect. 2, we briefly introduce the PASCs. In Sect. 3, we review the basic structure of the protocol. In Sect. 4, we analyze the performance of our PASCs-based protocol under the superior channel attack: We calculate the secret key rate of our protocol and compare the results with those obtained using a similar protocol using coherent states. In Sect. 5, we

consider a intercept–resend attack: the simultaneous measurement quadrature attack. We evaluate the eavesdropper success rate for both the PASCs and the coherent states. In Sect. 6, we discuss the results and present our conclusions.

2 Photon added then subtracted coherent states

It is possible to perform quantum-state engineering, via conditional measurements by adding and/or subtracting photons of a quantized light field, as discussed in [22]. Earlier in the 1990s, there were envisaged the photon-added coherent states (PACS) [23], which were successfully generated a few years ago [24]. Subsequently, the combination of photon adding and photon subtracting in the electromagnetic field has also been experimentally explored [19]. In general, the operation of firstly adding k photons and then subtracting l photons from a coherent state $|\alpha\rangle$ results in the following state (PASCs) [25]:

$$|k, l, \alpha\rangle = [N_{k,l}(\alpha)]^{-1/2} \hat{a}^l \hat{a}^{\dagger k} |\alpha\rangle, \tag{1}$$

with normalizing constant

$$N_{k,l}(\alpha) = \sum_{m=0}^l \frac{(l!)^2 (l+k-m)!}{(-1)^m m! [(l-m)!]^2} L_{l+k-m}(-|\alpha|^2), \tag{2}$$

and where L_{l+k-m} is the Laguerre polynomial of order $(l+k-m)$.

Of particular interest for our purposes are the PACS and the PASCs having just one photon added and one photon subtracted ($k = l = 1$). Thus, from an initial coherent state $|\alpha\rangle$, we first add one photon to it or $|\phi_A\rangle \propto \hat{a}^\dagger |\alpha\rangle$ and then subtract one photon from the resulting state, obtaining the PASCs $|1, 1, \alpha\rangle \equiv \alpha \hat{a} |\phi_A\rangle$. An interesting feature of the state $|1, 1, \alpha\rangle$ is that it may be written as a superposition of a coherent state and a photon-added coherent state (PACS), i.e., $|1, 1, \alpha\rangle \propto \hat{a} \hat{a}^\dagger |\alpha\rangle \propto (1 + \hat{a}^\dagger \hat{a}) |\alpha\rangle \propto |\alpha\rangle + \alpha |\phi_A\rangle$. In other words, this specific PASCs may be written as a superposition of a Gaussian state (coherent state) with a non-Gaussian component (PACS) weighted by α .

A useful and well-known representation of the field states is the Wigner function— a quasiprobability distribution in phase space [26,27]. For a density operator $\hat{\rho}$, the Wigner function may be expressed as a series expansion:

$$W(\zeta) = \frac{2}{\pi} \sum_{n=0}^{\infty} (-1)^n \langle n | \hat{D}^{-1}(\zeta) \hat{\rho} \hat{D}(\zeta) | n \rangle, \tag{3}$$

where $\zeta = \zeta_r + i\zeta_i$, being (ζ_r, ζ_i) the phase space coordinates, and \hat{D} is Glauber’s displacement operator, $\hat{D}(\zeta) = \exp(\zeta \hat{a}^\dagger - \zeta^* \hat{a})$. For the PASCs, $\hat{\rho} = |k, l, \alpha\rangle \langle k, l, \alpha|$, the corresponding Wigner function reads [25]

$$W^{k,l}(\zeta; \alpha) = \frac{2e^{(-2|\alpha-\zeta|^2)}}{\pi N_{k,l}(\alpha)} \sum_{n=0}^k \frac{(-1)^n (k!)^2}{n! ((k-n)!)^2} |H_{k-n,l}[i(2\zeta - \alpha), i\alpha^*]|^2, \tag{4}$$

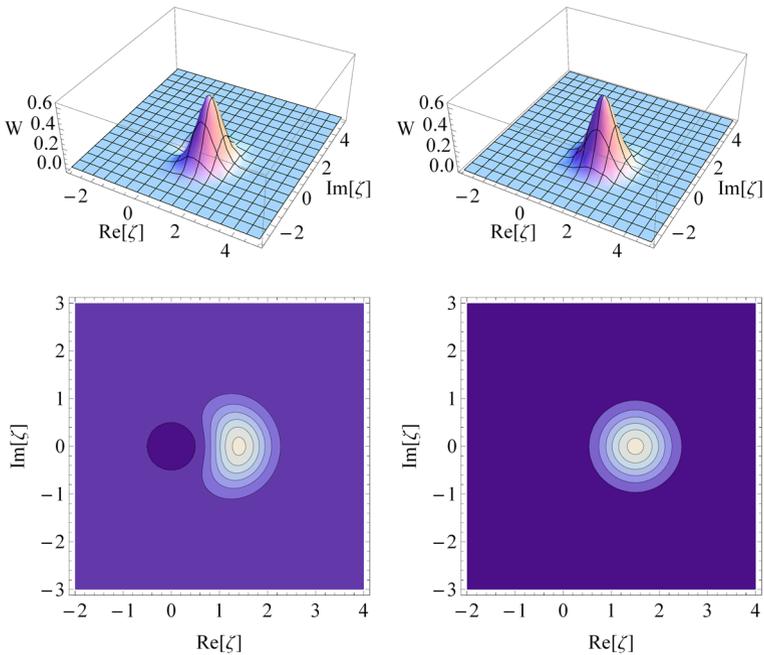


Fig. 1 Wigner function and contour plots of: PASCs (left) with one photon added and one photon subtracted from a coherent state having $\alpha = 1$ and a coherent state (right) having $\alpha' = 1.5$

being $H_{k-n,l}$ the bivariate Hermite polynomials

$$H_{p,q}(\epsilon, \varepsilon) = \sum_{r=0}^{\min(p,q)} \frac{(-1)^r p!q!}{r!(p-r)!(q-r)!} \epsilon^{p-r} \varepsilon^{q-r}. \tag{5}$$

For comparison, we have plotted in Fig. 1 the Wigner function of the PASCs having just one photon added and one photon subtracted [Eq. (4) with $k = l = 1$], together with the Wigner function of the coherent state $|\alpha\rangle$, given by $W(\zeta; \alpha) = \frac{2}{\pi} \exp(-2|\alpha - \zeta|^2)$. The Wigner function of a coherent state is exactly a Gaussian function, while the PASCs’s Wigner function has a slight deformation as well as a negative part, a clear indication of the non-classicality of the state. Apart from being useful for identifying some features of quantum states, the Wigner function may also be used to analyze the security of our protocol, as we are going to show below.

3 The protocol

The protocol works as follows: Firstly, Alice randomly chooses one of the four PASCs (for α real): either $|\psi_{AS+}\rangle \equiv |1, 1, \alpha\rangle$ and $|\psi_{AS+i}\rangle \equiv |1, 1, i\alpha\rangle$ (representing bit 1), or $|\psi_{AS-}\rangle \equiv |1, 1, -\alpha\rangle$ and $|\psi_{AS-i}\rangle \equiv |1, 1, -i\alpha\rangle$, (representing bit 0) in the horizontal and vertical bases, respectively. The plots of the Wigner functions corresponding to

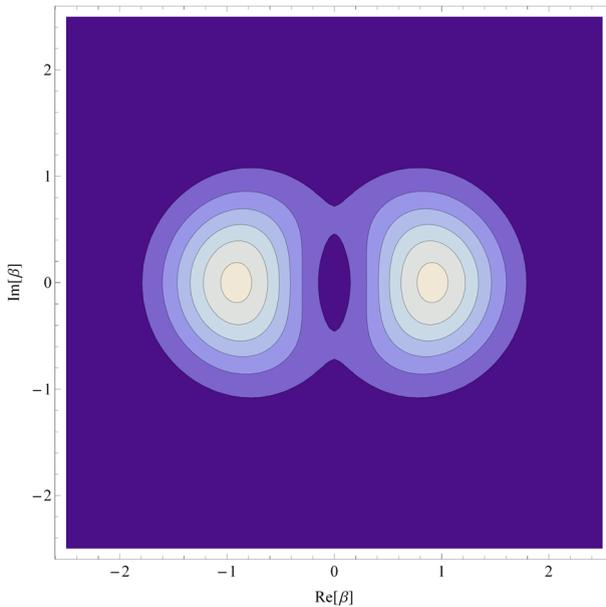


Fig. 2 Contour plots of the PASCs with one photon added and one photon subtracted from a coherent state having $\alpha = 0.55$, ($|\psi_{AS+}\rangle$) and $\alpha = -0.55$ ($|\psi_{AS-}\rangle$)

$|\psi_{AS-}\rangle$ and $|\psi_{AS+}\rangle$ in Fig. 2 give a clear picture of their distinguishability in phase space. In a second step, Alice sends a light signal prepared in the chosen state to Bob, who randomly selects either the horizontal or the vertical basis and performs a homodyne detection on the received signal. We now denote $\beta = \beta_r + i\beta_i$ the (complex) measurement variable corresponding to Bob's measurement. If Bob chooses, say, the vertical basis for his measurement, this corresponds to measure the real part of β (β_r); if he chooses the horizontal basis, it corresponds to measure the imaginary part of β (β_i). Bob also fixes a value for the post-selection threshold, β_c , obtained via an optimization procedure as we will discuss in what follows. If in a given measurement, he finds $\beta_{r,i} < -\beta_c$, Bob assigns value 0 the bit; if he finds $\beta_{r,i} > \beta_c$, he assigns value 1 to the bit. Otherwise, Bob tells Alice to neglect the corresponding bit.

4 Beam-splitter attack: superior channel attack

Due to the transmission line losses (imperfect channel), it is possible for an eavesdropper (Eve) to intercept a fraction of the signal without being noticed by the legitimate users. To do that, Eve uses an asymmetric beam splitter of transmissivity T and reflectivity R , with $T^2 + R^2 = 1$. She keeps the reflected part of the beam (the transmitted part is sent to Bob via a lossless channel) stored in a quantum memory and waits for the announcement of the measurement basis used by Bob. For simplicity, in this security analysis we consider just the case in which the horizontal basis is announced, as the discussion is analogous for the vertical basis due to symmetry. To estimate the amount

of gain of secret information per transmitted pulse S_{AB} , it is necessary to derive an upper bound of the information leaked to Eve when she splits the beam, as discussed in [21,30]. A relevant quantity in the following derivation is the joint measurement probability, $P(\beta_r, \epsilon_r)$, of Bob obtaining the result β_r and Eve obtaining ϵ_r ,

$$P_{\pm}(\beta_r, \epsilon_r) = \int \tilde{W}_{\pm}(\beta, \epsilon) d\beta_i d\epsilon_i, \tag{6}$$

where $\tilde{W}_{\pm}(\beta, \epsilon)$ is the (two-mode) Wigner function of the beam-splitter output [8,28,29],

$$\tilde{W}_{\pm}(\beta, \epsilon) = W_{\psi_{AS\pm}}^{1,1}(T\beta - R\epsilon, \alpha) W_{\text{vac}}(R\beta + T\epsilon). \tag{7}$$

The \pm signs refer to the pair of states we are considering for the security analysis, namely $|\psi_{AS+}\rangle$ and $|\psi_{AS-}\rangle$. In the expression above, $W_{\psi_{AS\pm}}^{1,1}(T\beta - R\epsilon, \alpha)$ is the (single mode) Wigner function [Eq. (4)] of the PASCs resulting from the addition of only one photon to a coherent state $|\alpha\rangle$ and subtraction of one photon from the resulting state. In the other port of the beam splitter, we have the vacuum as input state, with Wigner function $W_{\text{vac}}(R\beta + T\epsilon)$.

Because the PASCs is not a coherent state, the two emerging beams from the beam splitter are normally in an entangled state. Thus, the joint probability distribution does not factorize, and the results of measurements made by Bob, β_r , and Eve, ϵ_r , will be somehow correlated, as shown in Fig. 3. This means that if Bob measures a relatively large value for his quadrature (β_r), Eve is likely to measure a small value for hers (ϵ_r). For instance, as shown in Fig. 3, The maximum of $P_+(\beta_r, \epsilon_r)$ occurs for $\beta_r = 1.2$,

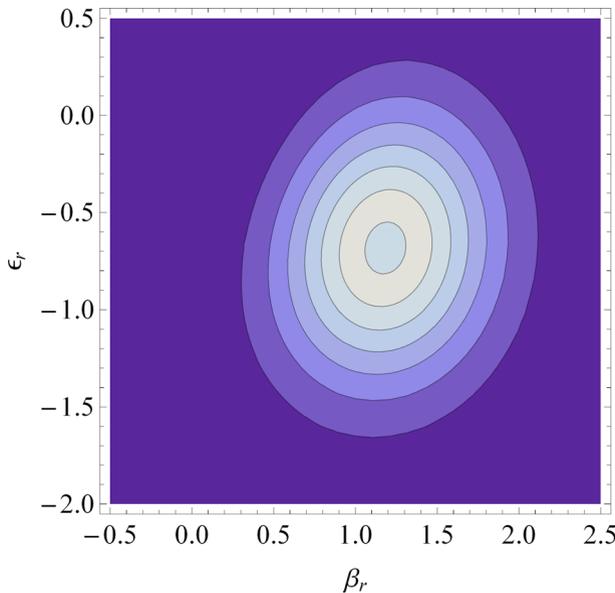


Fig. 3 Contour plot of the joint probability distribution, $P_+(\beta_r, \epsilon_r)$, for $\alpha = 1$ and $T^2 = 0.75$

while $\epsilon_r = -0.70$. Thus, if we increase the value of the post-selection threshold, the bit error rate on Eve's side will also be increased.

After performing an ideal error correction and privacy amplification, we may obtain a lower bound for the gain of secret information per transmitted pulse, S_{AB} as discussed in [8, 21, 30, 31]. Firstly, we define r_{acc} , the fraction of accepted bits as $r_{acc} = [P(0) + P(1)]/2$, with

$$P(1) = \int_{\beta_c}^{\infty} P'_+(\beta_r) d\beta_r \tag{8}$$

$$P(0) = \int_{-\infty}^{-\beta_c} P'_+(\beta_r) d\beta_r, \tag{9}$$

and

$$P'_\pm(\beta_r) = \int \tilde{W}_\pm(\beta, \epsilon) d\beta_i d\epsilon_i d\epsilon_r. \tag{10}$$

The Shannon information I_{AB} is defined as

$$I_{AB} = \int_{\beta_c}^{\infty} d\beta_r \frac{P'_+(\beta_r) + P'_+(-\beta_r)}{P(0) + P(1)} \times \{1 + \delta(\beta_r) \log_2 \delta(\beta_r) + [1 - \delta(\beta_r)] \log_2 [1 - \delta(\beta_r)]\}, \tag{11}$$

with

$$\delta(\beta_r) = \frac{P'_+(-\beta_r)}{P'_+(\beta_r) + P'_+(-\beta_r)}. \tag{12}$$

The amount of reduction of the raw key during the privacy amplification may be written as $\tau = 1 + \log_2(P_c)$, where P_c is the collision probability [8]

$$P_c = \frac{1}{2} \int \frac{\mathcal{P}_+^2(\epsilon_r | \beta_c < |\beta_r|) + \mathcal{P}_-^2(\epsilon_r | \beta_c < |\beta_r|)}{\mathcal{P}_+(\epsilon_r | \beta_c < |\beta_r|) + \mathcal{P}_-(\epsilon_r | \beta_c < |\beta_r|)} d\epsilon_r, \tag{13}$$

and where

$$\mathcal{P}_\pm(\epsilon_r | \beta_c < |\beta_r|) = \int_{\beta_c < |\beta_r|} \frac{P_\pm(\beta_r, \epsilon_r)}{P(0) + P(1)} d\beta_r \tag{14}$$

is Eve's probability distribution conditioned to the fact that a pulse \pm was sent and that Bob accepted the bit in his post-selection. The collision probability plays a crucial role in the generation of the secret key, indicating by which amount the raw key must be reduced in order to eliminate Eve's knowledge about it. The secret information S_{AB} is thus given by

$$S_{AB} = r_{acc} (I_{AB} - \tau). \tag{15}$$

The results are shown in Fig. 4. We have that the maximum of the surface representing the secret information is $S_{AB}^{max} \approx 0.140$ for the coherent state, while $S_{AB}^{max} \approx 0.167$ for the PASCs, i.e., a percent improvement of about 19% if the PASCs are used in place of coherent states. Moreover, we note that the PASCs-based protocol is more efficient for smaller values of the amplitude α of the transmitted pulse, compared

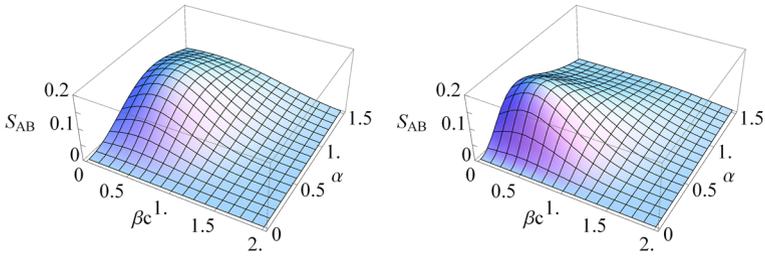


Fig. 4 Secret key rate S_{AB} versus the coherent state amplitude (α) and the post-selection threshold (β_c) for a coherent state (*left*) and for a PASCs having just one photon added and one photon subtracted (*right*). The channel transmission is $T^2 = 0.75$

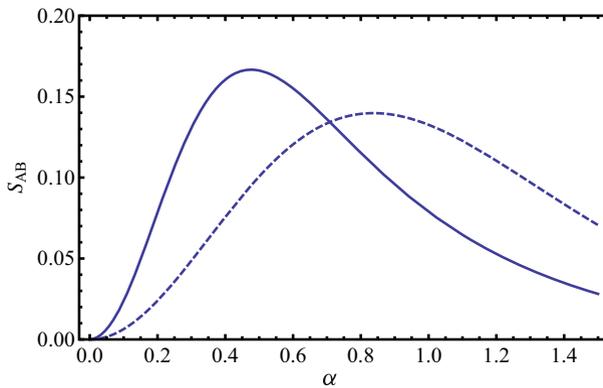


Fig. 5 Secret key rate S_{AB} as a function of α for the PASCs (*solid blue line*) and coherent state (*dashed blue line*); cross section of the surface plots in Fig. 4 for $\beta_c = 0.350$ (Color figure online)

with the coherent state case, as shown in Fig. 4. For the coherent state protocol, the peak of S_{AB} occurs for $\alpha = 0.838$ and $\beta_c = 0.377$, while for the PASCs protocol, $\alpha = 0.476$ and $\beta_c = 0.350$. In Figs 5 and 6, we have plotted cross sections of the surface plots in Fig. 4 to make easier a comparison of both cases. We remind that the PASCs (having just one photon added and one photon subtracted) may be written as a superposition of the coherent state $|\alpha\rangle$ with a PACS, or $|\psi_{AS}\rangle \propto |\alpha\rangle + \alpha|\phi_A\rangle$; thus, for small α the contribution of the PACS (non-Gaussian state) will also be very small, and the PASCs will be close to a coherent (Gaussian) state. Nevertheless, it will still generate an entangled state after crossing the beam splitter. This will introduce anti-correlations between Bob’s and Eve’s measurements results (see Fig. 3), which favors the security of the PASCs-based protocol, given that Bob will be able to reduce Eve’s knowledge about the bits via post-selection. In Fig. 7, we have plotted the secret bit rate S_{AB} as a function of transmission distance in a standard optical fiber for protocols using PASCs and coherent states. We note that a PASCs-based protocol outperforms a protocol based solely on coherent states, in the sense that a secret key could be generated at higher rates for a given distance.

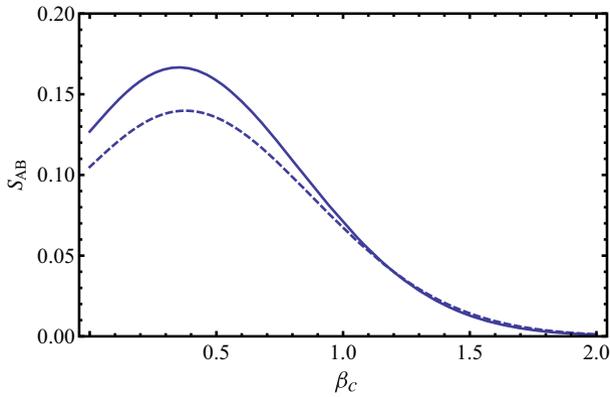


Fig. 6 Secret key rate S_{AB} as a function of (β_c) for the PASCs (solid blue line) and coherent state (dashed blue line); cross section of the surface plots in Fig. 4 for $\alpha = 0.476$ (Color figure online)

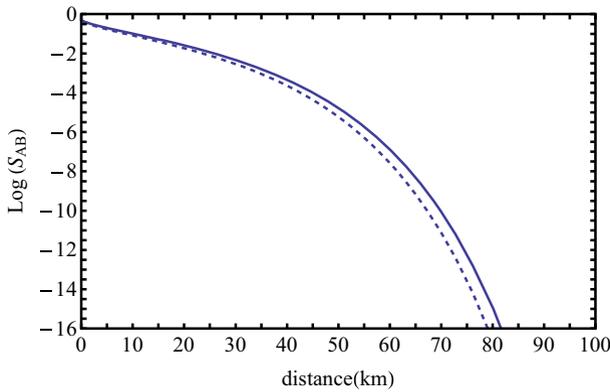


Fig. 7 Secret key rate S_{AB} versus distance for the: PASCs (solid line) and the coherent state (dashed line). We have considered an optical fiber loss coefficient 0.2 dB/km for a wavelength of 1.22 μm

5 Intercept-resend attack: simultaneous quadrature measurement attack

For complementarity, we discuss now a second (intercept-resend) attack performed by Eve in which she splits the incoming pulses of light in a 50:50 beam splitter and performs simultaneous quadrature measurements on the outgoing beams. She then tries to infer (with probability P_{corr}) the state of the signal sent by Alice. Here, we consider the preparation of four possible states by Alice, defined above as $|\psi_{AS\pm(i)}\rangle$. If Eve measures (β_r, ε_i) , she will choose the state of the signal for which the associated joint probability distribution $P_{\pm(i)}$ is maximum. For each state, we have a corresponding region in phase space (each one of area A_0), i.e., $\beta_r \geq |\varepsilon_i|$ for $|\psi_{AS+}\rangle$; $\varepsilon_i > |\beta_r|$ for $|\psi_{AS+i}\rangle$; $-\beta_r \geq |\varepsilon_i|$ for $|\psi_{AS-}\rangle$ and $-\varepsilon_i > |\beta_r|$ for $|\psi_{AS-i}\rangle$. Generally speaking, the associated probability distributions are given by

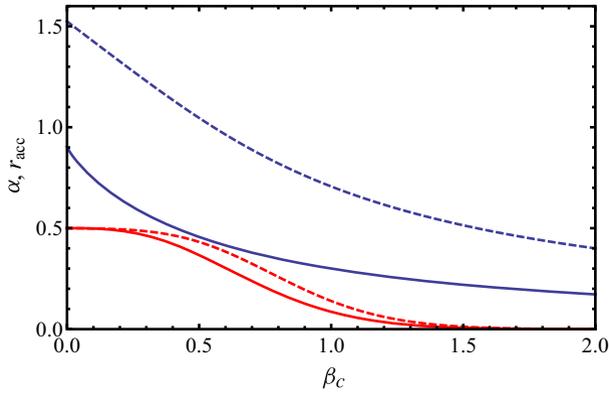


Fig. 8 Optimum α as a function of the post-selection threshold β_c (upper curves), for the PASCs (solid blue line) and coherent state (dashed blue line); fraction of accepted bits, r_{acc} as a function of β_c (lower curves), for the PASCs (solid red line) and coherent state (dashed red line) (Color figure online)

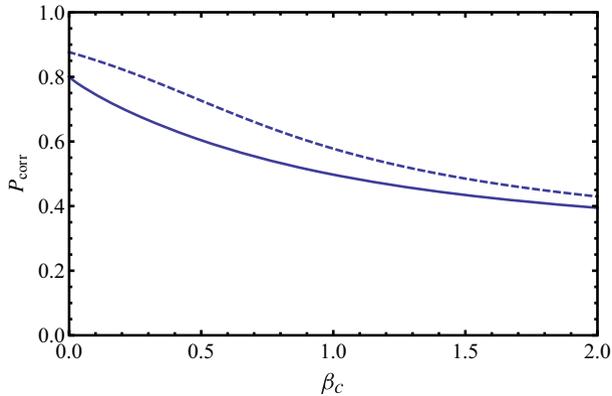


Fig. 9 Rate of Eve's success P_{corr} as a function of β_c , PASCs (solid line) and coherent state (dashed line)

$$P_{\pm(i)}(\beta_r, \epsilon_i) = \int \tilde{W}_{\pm(i)}(\beta, \epsilon) d\beta_i d\epsilon_r, \tag{16}$$

where $\tilde{W}_{\pm}(\beta, \epsilon)$ is the (two-mode) Wigner function of the beam-splitter output,

$$\tilde{W}_{\pm(i)}(\beta, \epsilon) = W_{\psi_{AS\pm(i)}}^{1,1}(T\beta - R\epsilon, \alpha) * W_{vac}(R\beta + T\epsilon). \tag{17}$$

As in reference [8], we may define Eve's success rate for the attack, P_{corr} . For instance, for a signal in the state $|\psi_{AS+}\rangle$, we have

$$P_{corr} = 2 \int_{A_0} P_+(\beta_r, \epsilon_i) d\beta_r d\epsilon_i. \tag{18}$$

The efficiency of such an attack may then be evaluated. Alice can make an optimization of the coherent amplitude α given a fixed error rate $\delta = 1.15 \times 10^{-3}$ for a lossless line and without the presence of Eve. In Fig. 8, we have the optimum α and the fraction of accepted bits, r_{acc} as a function of the post-selection threshold β_c , for both coherent state and the PASCs. We note that the value of optimum α (for each β_c) is in general smaller in the PASCs-based protocol, compared with the coherent state case. Thus, even though the rate of accepted bits is smaller for the PASCs, the probability of Eve obtaining the correct bit becomes also smaller in this case, given that the optimum value of α (for a given value of threshold β_c) is smaller for the PASCs. In Fig. 9, we have a plot of P_{corr} as a function of β_c , which clearly shows the advantage of the PASCs over coherent states in a simultaneous quadrature measurement attack.

6 Conclusions

We have shown that a continuous-variable protocol based on PASCs having just one photon added and one photon subtracted is more efficient than a coherent state-based protocol, both of them using homodyne detection and post-selection. We have performed a security analysis based on the superior channel attack and concluded that the PASCs-based protocol would allow the legitimate users (Alice and Bob) to build a secret key with transmission rates higher than the ones obtained from coherent state-based protocols. We have also analyzed the simultaneous quadrature measurement attack, and we have shown that Eve's success rate is smaller if PASCs are used in the place of coherent states. Having verified the better performance of PASCs (compared to coherent states) for two different attacks is a first step to assess the security of our protocol. Nevertheless, more general proofs of security are desirable, and we are going to consider them elsewhere. We are dealing with non-Gaussian, continuous-variable states, but, as we have already discussed, the PASCs having one added photon and one subtracted photon may be written as a quantum superposition of a coherent state $|\alpha\rangle$ and a PACS multiplied by the coherent amplitude α . This means that in the situation of small α we are considering here, the PASCs is very close to a coherent state, and a possible way to investigate collective attacks, for instance, could be done by following the methodology presented in [14, 32]. Our work is an attempt to explore the possibilities of utilization of non-Gaussian states for quantum key distribution purposes, and this may open up new directions for continuous-variable protocols.

Acknowledgments This work was partially supported by CNPq (Conselho Nacional de Desenvolvimento Científico e Tecnológico—INCT of Quantum Information), FAPESP (Fundação de Amparo à Pesquisa do Estado de São Paulo—CePOF of Optics and Photonics) and CAPES (Coordenação de Aperfeiçoamento de Pessoal de Ensino Superior), Brazil.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, pp. 175 (1984)
2. Scarani, V., et al.: The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009)

3. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000)
4. Stucki, D., et al.: High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New J. Phys.* **11**, 075003 (2009)
5. Ralph, T.C.: Continuous variable quantum cryptography. *Phys. Rev. A* **61**, 010303(R) (1999)
6. Hillery, M.: Quantum cryptography with squeezed states. *Phys. Rev. A* **61**, 022309 (2000)
7. Cerf, N.J., Lévy, M., Van Assche, G.: Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **63**, 052311 (2001)
8. Horak, P.: The role of squeezing in quantum key distribution based on homodyne detection and post-selection. *J. Mod. Opt.* **51**, 1249 (2004)
9. Grosshans, F., Grangier, P.: Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002)
10. Grosshans, F., et al.: Quantum key distribution using Gaussian-modulated coherent states. *Nature* **421**, 238 (2003)
11. Vidiella-Barranco, A., Borelli, L.F.M.: Continuous variable quantum key distribution using polarized coherent states. *Int. J. Mod. Phys. B* **20**, 1287 (2006)
12. Lorenz, S., Korolkova, N., Leuchs, G.: Continuous-variable quantum key distribution using polarization encoding and post selection. *Appl. Phys. B* **79**, 273 (2004)
13. Namiki, R., Hirano, T.: Security of quantum cryptography using balanced homodyne detection. *Phys. Rev. A* **67**, 022308 (2003)
14. Leverrier, A., Grangier, P.: Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev.* **102**, 180504 (2009)
15. Peev, M., et al.: The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009)
16. Sasaki, M., et al.: Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, 10387 (2011)
17. Jouguet, Paul, et al.: Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photon.* **7**, 378 (2013)
18. 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>
19. Parigi, 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. Silberhorn, C., Ralph, T.C., Lütkenhaus, N., Leuchs, G.: Continuous variable quantum cryptography: beating the 3 dB loss limit. *Phys. Rev. Lett.* **89**, 167901 (2002)
21. Lütkenhaus, N.: Security against eavesdropping in quantum cryptography. *Phys. Rev. A* **54**, 97 (1996)
22. Dakna, M., Knöll, L., Welsch, D.-G.: Quantum state engineering using conditional measurement on a beam splitter. *Eur. Phys. J. D* **3**, 295 (1998)
23. Agarwal, G.S., Tara, K.: Nonclassical properties of states generated by the excitations on a coherent state. *Phys. Rev. A* **43**, 492 (1991)
24. Zavatta, A., Viciani, S., Bellini, M.: Quantum-to-classical transition with single-photon-added coherent states of light. *Science* **306**, 660 (2004)
25. 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)
26. Wigner, E.: On the quantum correction for thermodynamic equilibrium. *Phys. Rev.* **40**, 749 (1932)
27. Hillery, M., et al.: Distribution functions in physics: fundamentals. *Phys. Rep.* **106**, 121 (1984)
28. Wu, J.W.: Violation of Bells inequalities and two-mode quantum-optical state measurement. *Phys. Rev. A* **61**, 022111 (2000)
29. Ou, Z.Y., Hong, C.K., Mandel, L.: Relation between input and output states for a beam splitter. *Opt. Commun.* **63**, 118 (1987)
30. Lütkenhaus, N.: Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A* **61**, 052304 (2000)
31. Shannon, C.E.: A Mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 379 (1948)
32. Becir, A., Wahiddin, M.R.: Phase coherent states for enhancing the performance of continuous variable quantum key distribution. *J. Phys. Soc. Jpn.* **81**, 034005 (2012)