Hybrid quantum key distribution using coherent states and photon-number-resolving detectors

Marco Cattaneo,[1] Matteo G. A. Paris,[1,2] and Stefano Olivares[1,2,*]
[1]*Quantum Technology Laboratory, Dipartimento di Fisica "Aldo Pontremoli," Università degli Studi di Milano, I-20133 Milano, Italy*
[2]*INFN, Sezione di Milano, I-20133 Milano, Italy*

(Received 28 September 2017; published 30 July 2018)

We put forward a hybrid quantum key distribution protocol based on coherent states, Gaussian modulation, and photon-number-resolving (PNR) detectors, and show that it may enhance the secret key generation rate (KGR) compared to homodyne-based schemes. Improvement in the KGR may be traced back to the dependence of the two-dimensional discrete output variable on *both* the input quadratures, thus overcoming the limitations of the original protocol. When reverse reconciliation is considered, the scheme based on PNR detectors outperforms the homodyne one both for individual and collective attacks. In the presence of direct reconciliation, the PNR strategy is still the best one against individual attacks, but for the collective ones the homodyne-based scheme is still to be preferred as the channel transmissivity decreases.

DOI: 10.1103/PhysRevA.98.012333

I. INTRODUCTION

In the last decade, continuous-variable quantum key distribution (QKD) based on coherent states and homodyne detection (HD-QKD) gained much attention in the cryptographic community [1]. In particular, the compatibility with telecom techniques and the high detection efficiency makes HD-QKD of interest for practical implementations [2]. Moreover, the recent advances in establishing continuous-variable ground-satellite quantum channels [3,4] exploiting coherent states and homodyne detection has opened the way to the possibility of a global QKD network. Heterodyne-based protocols have been also suggested [5], and the secret key rate valid against individual attacks has been analyzed [6,7].

Usually, in HD-QKD an observable with a continuous spectrum is used to encode the information which will be used to extract the secret key. For example, in the original continuous-variable (CV) protocol based on coherent states [8,9], the information is encoded by Gaussian modulation of phase and amplitude of an input coherent state, whereas the secret key is retrieved by a slicing protocol processing the data from a homodyne detector.

Here we consider a CV-QKD protocol based on coherent states, but we substitute the homodyne detector with a scheme based on photon-number-resolving (PNR) detectors. While in a typical homodyne detection one measures the difference photocurrent from a couple of pin photodiodes [10] able to detect a macroscopic photocurrent proportional to the number of photons, here we consider a scenario in which the *number* of photons is measured at the two detectors. Recent theoretical [11,12] and experimental results [13,14] have shown that detection schemes aimed to measure the photon number statistics can be exploited in order to obtain some useful information about the field quadratures. Motivated by these results, we investigate whether, and to which extent, these PNR detection schemes can be employed in QKD protocols. Throughout the paper we will refer to this kind of protocol as PNR-QKD. More in detail, we will address the mutual information between sender, receiver, and eavesdropper, as a figure of merit to assess the performance of the PNR-based protocols [15].

The paper is structured as follows. In Sec. II we review the principles of the HD-QKD based on coherent states and evaluate the mutual information between sender and receiver, and between sender and eavesdropper, in order to assess the maximum key generation rate (KGR) [15]. Then, Sec. III illustrates our novel PNR-QKD: we show that the presence of two PNR detectors allows us to extract more information about the detected signals. In our analysis we consider the couple of numbers corresponding to the detected photons as a two-dimensional statistical variable. We find that there exists a threshold value on the LO energy above which PNR-QKD outperforms HD-QKD. In this regime, we investigate the performance of the PNR-QKD with respect to HD-QKD in the presence of individual and collective attacks and for direct and reverse reconciliation. Section IV closes the paper with some concluding remarks.

II. HD-QKD WITH COHERENT STATES

In HD-QKD (top panel of Fig. 1), Alice, the sender, draws two random real numbers, x and y, from a normal distribution $\mathcal{N}_{\mu,\sigma^2}(z)$, with mean value $\mu = 0$ and variance $\sigma^2 = \Sigma^2$. Then, Alice prepares the coherent state $|\alpha\rangle = |x + iy\rangle$, which is sent to Bob through a quantum channel. The receiver, Bob, performs homodyne detection by mixing the signal at a balanced beam splitter (BS) with a local oscillator (LO), i.e., a highly excited coherent state. Upon setting the LO phase at either $\phi = 0$ or $\phi = \pi/2$, Bob can detect the quadratures $\hat{x}$ or $\hat{y}$, respectively. In order to distribute a secret key, Bob chooses randomly to measure either one quadrature or the other on the signal received from Alice. After repeating this procedure several times, the partners share a string of (real) random variables whose correlations are quantified by the mutual information

*stefano.olivares@fisica.unimi.it

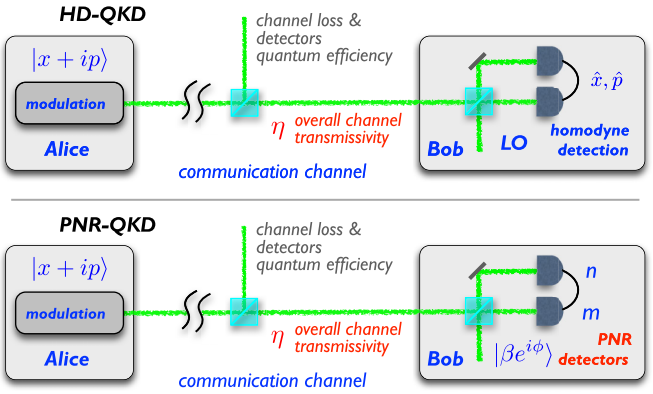

FIG. 1. (Top) Scheme of homodyne-detection-based QKD (HD-QKD). (Bottom) Scheme of PNR-based QKD, in which the two PNR detectors are used together with a low-intensity LO. The parameter η refers to the overall channel transmissivity. See the text for details.

$I(A;B)$, where A and B are the random variables of Alice and Bob, respectively, with joint distribution $P_{AB}(a,b)$ and marginal distributions $P_A(a)$ and $P_B(b)$.

In the ideal case of lossless channel, we have [8]

$$I(A;B) = H(A;B) - H(A|B) - H(B|A), \tag{1}$$

$$= \tfrac{1}{2}\log_2(1+4\Sigma^2), \tag{2}$$

where $H(A;B)$ is the joint (Shannon) entropy, and $H(A|B)$ and $H(B|A)$ are the conditional entropies of A and B.

Losses, including the quantum efficiency of the detectors, can be described by an *overall channel transmissivity* η, $0 \leqslant \eta \leqslant 1$ (see Fig. 1). In this case, the mutual information between the parties is unavoidably reduced and becomes

$$I(A;B) = \tfrac{1}{2}\log_2(1+4\eta\Sigma^2). \tag{3}$$

Starting from their shared correlated variables, Alice and Bob may distill a secret shared key using *reconciliation* [16] and *privacy amplification* [17], both making use of a classical channel. The presence of losses allows an eavesdropper, Eve, to obtain some information about Alice's random variable without being detected, upon hiding herself within the channel loss. In this case, the amount of information is limited by the no-cloning theorem [18,19]. More in details, the reconciliation stage requires a flow of information from Alice to Bob (direct reconciliation, DR) or vice versa (reverse reconciliation, RR) in order to correct the transmission errors and agree on a common bit string, which is thus partially known by the eavesdropper. In the first case (DR), Alice's data form the secret key, and therefore it is important to evaluate the information shared between Alice and Eve. In RR, the secret key is instead based on Bob's data and the information shared between Bob and Eve becomes the relevant player. The evaluation of the information shared between the parties requires one to understand also what is the kind of measurement performed. Here we focus on individual attacks (each pulse signal is measured individually) and collective attacks (the measurement involves all the sent pulses) [20]. In the following we assume that Eve also uses homodyne detection. This is a standard, feasible technique which mimics the detection system used by Bob but with a strong LO and pin photodiodes without photon-number resolving capabilities. (For a more general discussion on the optimality of Gaussian attacks, see Refs. [21] and [22].)

In the presence of individual attacks, the information shared by Eve and Alice is quantified by the corresponding mutual information $I(A;E) = \frac{1}{2}\log_2[1+4(1-\eta)\Sigma^2]$. Assuming DR, the secret KGR is given by [15]

$$\Delta I_{\rm D}^{(\rm ind)} = I(A;B) - I(A;E), \tag{4}$$

which is valid for *any* QKD scheme where classical communication is permitted. In particular, upon running the homodyne-based protocol proposed in Ref. [8], we have

$$\Delta I_{\rm D}^{(\rm ind)} = \frac{1}{2}\log_2\left[\frac{1+4\eta\Sigma^2}{1+4(1-\eta)\Sigma^2}\right], \tag{5}$$

which is positive if $\eta > 0.5$, that is, the overall losses should be less than 3 dB. This limit can be beaten using RR, obtaining the following KGR:

$$\Delta I_{\rm R}^{(\rm ind)} = I(A;B) - I(E;B), \tag{6}$$

$$= \frac{1}{2}\log_2\left[\frac{1+4\Sigma^2}{1+4(1-\eta)\Sigma^2}\right]. \tag{7}$$

When Eve can perform collective measurements (but Bob does not), we replace $I(A;E)$ and $I(B;E)$ with the Holevo information [23] in the previous formulas. The analytical results are quite cumbersome, but they can be obtained straightforwardly given the state of Eve conditioned to Bob's measurement outcome [24], as we will describe in the next section (see also Ref. [25] for further details).

III. PNR-QKD WITH COHERENT STATES

In this section we focus on the use of detectors able to discriminate the number of photons in order to investigate whether the KGR can be improved [1]. As we will see in the following, this provides additional information at the output which may be used to improve the secret KGR. In our scheme, the two photodiodes usually employed to build homodyne detection in HD-QKD are replaced by two PNR detectors. Furthermore, the high-intensity LO needed to implement homodyne detection is replaced with a relatively low-intensity (up to tens of photons) one, $|\beta e^{i\phi}\rangle$ with $\beta \in \mathbb{R}$ (see the bottom panel of Fig. 1).

In order to evaluate the statistics at the output, we recall that the output state of a balanced BS fed by coherent states is factorized, namely $U_{\rm BS}|\alpha\rangle|\beta e^{i\phi}\rangle = |(\alpha+\beta e^{i\phi})/\sqrt{2}\rangle|(\beta e^{i\phi}-\alpha)/\sqrt{2}\rangle$, $\alpha = x+iy$. The photon statistics measured by the two PNR detectors at the BS outputs are thus given by two Poisson distributions,

$$\mathscr{P}_k(n;\mu_k) = e^{-\mu_k}\mu_k^n/n!, \quad (k=1,2), \tag{8}$$

where the average numbers of photocounts $\mu_k \equiv \mu_k(x,y,\beta,\phi,\eta)$ read (we take into account the presence of the losses)

$$\mu_1 = \frac{\eta(x^2+y^2)+\beta^2}{2} + \sqrt{\eta}\beta(x\cos\phi + y\sin\phi), \tag{9a}$$

$$\mu_2 = \frac{\eta(x^2+y^2)+\beta^2}{2} - \sqrt{\eta}\beta(x\cos\phi + y\sin\phi). \tag{9b}$$

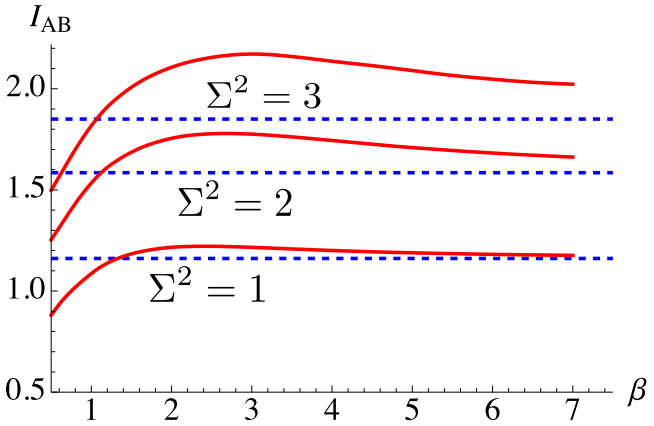

FIG. 2. Mutual information $I_{AB} = I(\mathbf{X};\mathbf{L})$ for a lossless channel as a function of β and for different values of Σ^2: from bottom to top $\Sigma^2 = 1$, 2, and 3. The red solid line refers to PNR-QKD and the blue dashed one to HD-QKD (the latter is independent of β). Notice the presence of a threshold of LO amplitude β above which PNR-QKD outperforms HD-QKD.

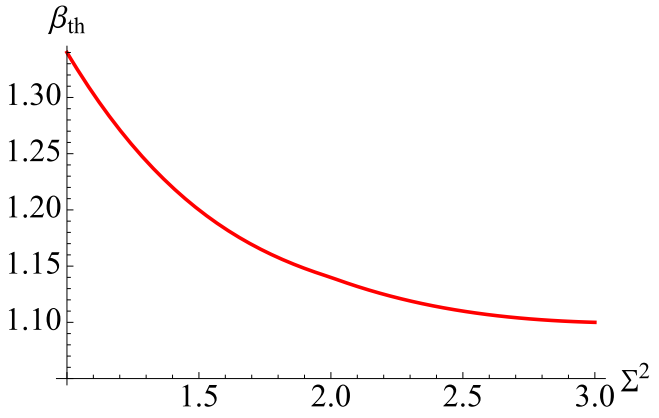

FIG. 3. Plot of the threshold value β_{th} as a function of Σ^2. For $\beta \geqslant \beta_{th}$, PNR-QKD outperforms HD-QKD.

It is worth noting that, since Eqs. (9) depend on both x and p, the PNR-QKD scheme may exploit the whole of Alice's input random variables $\mathbf{X} = (X, Y)$, while, using homodyne detection, the information about one of them is traced out at each run, due to Bob's measurement choice [8].

To investigate the performance of PNR-QKD with respect to the homodyne-based scheme, we consider the two-dimensional statistical variable corresponding to the two numbers of detected photons, namely, the two-dimensional discrete random variable $\mathbf{L} = (N, M)$, $N, M > 0$. The two variables N and M are distributed according to the Poisson distributions mentioned above. The joint distribution of the detected photons n and m is thus given by

$$P_{\mathbf{XL}}(x, y; n, m) = \mathcal{N}_{0,\Sigma^2}(x)\mathcal{N}_{0,\Sigma^2}(y)\mathcal{P}_1(n, \mu_1)\,\mathcal{P}_2(m, \mu_2). \tag{10}$$

Starting from the joint distribution, we can calculate the two marginals and evaluate the mutual information

$$I(\mathbf{X};\mathbf{L}) = H(\mathbf{X}, \mathbf{L}) - H(\mathbf{X}|\mathbf{L}) - H(\mathbf{L}|\mathbf{X}). \tag{11}$$

Without loss of generality, we set $\phi = 0$. The mutual information for an ideal channel, with neither eavesdroppers nor losses, i.e., $\eta = 1$, is reported in Fig. 2 as a function of β. We see that there is a threshold on the value of β above which the mutual information $I(\mathbf{X};\mathbf{L})$ for the PNR-QKD protocol is larger than the corresponding quantity for the HD-QKD.

Figure 3 shows the threshold β_{th} as a function of Σ^2. The monotone decreasing behavior of β_{th} can be understood as follows. If Σ^2 increases, we are "feeding" both the random variables X and Y in the PNR-QKD scheme, while only one of them in HD-QKD, i.e., we are accentuating the convenience of PNR-QKD with respect to HD-QKD.

A. Individual attacks

Let us now discuss the key generation rate in the presence of losses and of an eavesdropper, Eve, in the framework of individual attacks. In this case Eve performs a measurement in the same way on each state sent by Alice before the reconciliation stage and the key generation rate is given by Eq. (4) [20]. As we have seen above, the PNR-QKD protocol based on PNR is providing more information about the input alphabet compared to the homodyne case. Therefore, since we have to consider the best strategy for the eavesdropper, we assume that Eve employs the PNR scheme, if available. This leads us to compare two scenarios, the one in which both Bob and Eve employ homodyne detection and the one in which they both use PNR detectors. The mixed case, where Bob uses homodyne detection and Eve PNR one, has no practical meaning, since during the reconciliation protocol Alice and Bob will deal only with one random variable (say X) and thus Eve's information about the other random variable Y is completely irrelevant. This also means that Eve cannot use PNR detection in order to break the original homodyne protocol [8].

In Fig. 4 we show the key generation rate $\Delta I^{(\mathrm{ind})}$ as a function of the channel transmission η for HD-QKD and PNR-QKD in the case of DR (solid lines) and RR (dashed

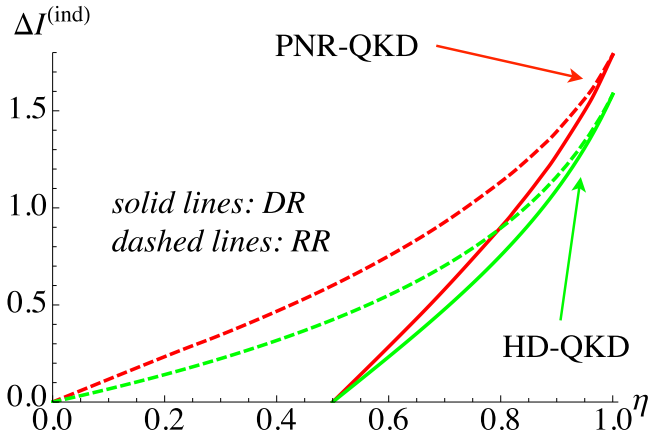

FIG. 4. KGR $\Delta I^{(\mathrm{ind})}$ as a function of channel transmissivity η in the presence of individual attacks for HD-QKD (green) or PNR-QKD (red), referring to the scenarios in which both Bob and Eve employ homodyne detection and the one in which they both use PNR detectors, respectively. We set $\beta = 2$ and $\Sigma^2 = 2$. In this case PNR-QKD outperforms HD-QKD in both cases of DR and RR.

lines): PNR-QKD turns out to be the best strategy in the presence of individual attacks. The enhancement may be traced back to the dependence of the output variable $\mathbf{L}$ on both the full Alice's alphabet $\mathbf{X}$ and not only on one of the components (either x or y), as it unavoidably happens for the original homodyne protocol. Since Bob's measurement is symmetric with respect to Eve's, the threshold $\eta = 0.5$ does not depend on Σ^2.

B. Collective attacks

To perform collective attacks Eve should store each quantum state sent by Alice and measure it only after the classical key distillation procedure. Now Eve can implement an optimal measurement, and therefore the new figure of merit for the KGR and DR is given by (as mentioned above, for a fair comparison with the PNR-QKD we assume that Bob does not perform a collective measurement) [20],

$$\Delta I_{\mathrm{D}}^{(\mathrm{coll})} = I(\mathbf{X};\mathbf{L}) - \chi(A;E), \tag{12}$$

where $\chi(A;E) = S[\rho_E] - \sum_{\mathbf{x}} p(\mathbf{x})\, S[\rho_{E|\mathbf{x}}]$ is the Holevo information between Alice and Eve. With $S[\rho] = -\mathrm{Tr}[\rho \log_2 \rho]$ being the von Neumann entropy of the state ρ, we are assuming that Eve receives the state $\rho_{E|\mathbf{x}}$ with probability $p(\mathbf{x})$ and, thus, $\rho_E = \sum_{\mathbf{x}} p(\mathbf{x})\, \rho_{E|\mathbf{x}}$. To calculate $\chi(A;E)$ we must distinguish HD-QKD from PNR-QKD, since in the first case the useful information is contained only in one single quadrature (say X), while in PNR-QKD it is contained in both X and Y (the difference appears essentially in the reconciliation stage). According to the protocol, in the case of HD-QKD Eve receives the mixed state (the information about the random variable y is lost)

$$\rho_{E|x} = \int_{\mathbb{R}} \mathcal{N}_{0,\Sigma^2}(y)\, |\sqrt{1-\eta}(x+iy)\rangle\langle\sqrt{1-\eta}(x+iy)|\, dy \tag{13}$$

with probability $\mathcal{N}_{0,\Sigma^2}(x)$ [25]. By contrast, in PNR-QKD Alice is sending information stored in both X and Y, and therefore Eve's conditional state is now the pure state

$$\rho_{E|(x,y)} = |\sqrt{1-\eta}(x+iy)\rangle\langle\sqrt{1-\eta}(x+iy)| \tag{14}$$

and $S[\rho_{E|(x,y)}] = 0$, while ρ_E is the same as in HD-QKD.

When RR is considered, we should substitute $\chi(E;B) = S[\rho_E] - \sum_{n,m} p(n,m)\, S[\rho_{E|(n,m)}]$ to $\chi(A;E)$ into Eq. (12). Here $p(n,m)$ is the marginal of $P_{\mathbf{XL}}(x,y;n,m)$ given in Eq. (10), i.e., the joint distribution for obtaining n and m number of photons at Bob's PNR detectors and $\rho_{E|(n,m)}$ is the corresponding conditional state received by Eve.

The KGR for collective attacks is depicted in Fig. 5 as a function of η in the case of HD-QKD and PNR-QKD for DR and RR. It is clear that in the framework of collective attacks and DR (solid lines), HD-QKD outperforms PNR-QKD (but for very high channel transmissivity!). Nevertheless, in the presence of RR we still find that PNR-QKD beats the scheme based on homodyne detection, though, as the channel transmissivity decreases, they exhibit almost the same performance.

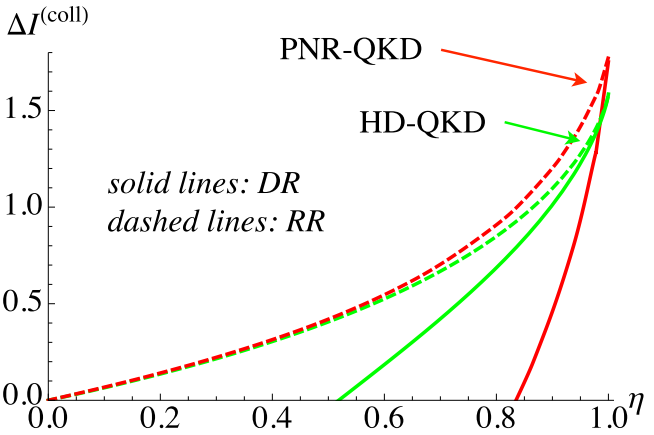

FIG. 5. KGR $\Delta I^{(\mathrm{coll})}$ as a function of channel transmissivity η in the presence of collective attacks for HD-QKD (green) or PNR-QKD (red). We set $\beta = 2$ and $\Sigma^2 = 2$. Now PNR-QKD beats HD-QKD for any value of η only in the case of RR, whereas if we use DR, PNR-QKD turns out to be the best strategy only for high values of the channel transmissivity.

IV. CONCLUDING REMARKS

In conclusion, we have shown that PNR detectors may be profitably employed to design a hybrid quantum key distribution protocol using coherent states. If we are restricted to individual attacks, when we exploit the full information at the output to implement PNR-QKD, the dependence of the two-dimensional discrete output variable on *both* the input quadratures provides enhancement of the secret KGR compared to HD-QKD, both for DR and RR. In the presence of collective attacks and RR the PNR-QKD still outperforms the homodyne-based strategy, though as the transmission of the channel decreases, the performance is almost the same as that of the HD-QKD. If we consider DR, the strategy based on PNR turns out to be the best choice only for very high values of the channel transmissivity. This is due to the conditional state received by Eve: in the case of HD-QKD it is a mixed state (the information about one quadrature is lost), whereas for PNR-QKD she receives pure states, having access to both the orthogonal quadratures, and thus leading to a clear increase of the overall gained information.

If we focus on the regimes where using PNR leads to greater ΔI, we can also note that PNR-QKD requires a lower value of η with respect to HD-QKD in order to obtain a given value of the KGR. This can be indeed an advantage, also considering that the state-of-the-art technology exploiting PNR detectors cannot achieve the overall quantum efficiency of homodyne detectors. In practice, homodyne setups may easily exhibit quantum efficiencies larger than 0.8, whereas customary PNR detectors are about 0.5 [14] or less. Nevertheless, there exist photon-number-resolving techniques based on transition-edge sensors which allow one to obtain a much higher efficiency, $\sim$0.9 or higher [26,27].

Further investigation is expected upon the design of a scheme for distilling a secret key after having run the

protocol and the investigation of performances for PNR-detector-based protocols involving not just simple homodyne detection at the receiver but also heterodyne detection [5–7,21,22]. In this view, our results pave the way for further developments in this promising field of quantum technology.

ACKNOWLEDGMENTS

We thank A. Allevi and M. Bondani for stimulating discussions, A. Leverrier for useful comments, and M. A. C. Rossi for assistance in the numerical calculations. This work has been supported by the University of Milan through the project CVQTIQP (Grant No. 15-6-643).

[1] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, Practical challenges in quantum key distribution, npj Quantum Inf. **2**, 16025 (2016).

[2] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, Ch. Pacher, R. F. Werner, and R. Schnabel, Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks, Nat. Commun. **6**, 8795 (2015).

[3] K. Günthner, I. Khan, D. Elser, B. Stiller, Ö. Bayraktar, C. R. Müller, K. Saucke, D. Tröndle, F. Heine, S. Seel, P. Greulich, H. Zech, B. Gütlich, S. Philipp-May, C. Marquardt, and G. Leuchs, Quantum-limited measurements of optical signals from a geostationary satellite, Optica **4**, 611 (2017).

[4] M. Lasota, R. Filip, and V. C. Usenko, Robustness of quantum key distribution with discrete and continuous variables to channel noise, Phys. Rev. A **95**, 062312 (2017).

[5] 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).

[6] J. Sudjana, L. Magnin, R. García-Patrón, and N. J. Cerf, Tight bounds on the eavesdropping of a continuous-variable quantum cryptographic protocol with no basis switching, Phys. Rev. A **76**, 052301 (2007).

[7] J. Lodewyck and P. Grangier, Tight bound on the coherent-state quantum key distribution with heterodyne detection, Phys. Rev. A **76**, 022332 (2007).

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

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

[10] S. Olivares, S. Cialdi, F. Castelli, and M. G. A. Paris, Homodyne detection as a near-optimum receiver for phase-shift keyed binary communication in the presence of phase diffusion, Phys. Rev. A **87**, 050303(R) (2013).

[11] W. Vogel and J. Grabow, Statistics of difference events in homodyne detection, Phys. Rev. A **47**, 4227 (1993).

[12] J. Sperling, W. Vogel, and G. S. Agarwal, Balanced homodyne detection with on-off detector systems: Observable nonclassicality criteria, Europhys. Lett. **109**, 34001 (2015).

[13] M. Bina, A. Allevi, M. Bondani, and S. Olivares, Homodyne-like detection for coherent state-discrimination in the presence of phase noise, Opt. Express **25**, 10685 (2017).

[14] M. Bina, A. Allevi, M. Bondani, and S. Olivares, Phase-reference monitoring in coherent-state discrimination assisted by a photon-number resolving detector, Sci. Rep. **6**, 26025 (2016).

[15] U. M. Maurer, Secret key agreement by public discussion from common information, IEEE Trans. Inf. Theory **39**, 733 (1993).

[16] G. Van Assche, J. Cardinal, and N. J. Cerf, Reconciliation of a quantum-distributed Gaussian key, IEEE Trans. Inf. Theory **50**, 394 (2004).

[17] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer, Generalized privacy amplification, IEEE Trans. Inf. Theory **41**, 1915 (1995).

[18] N. J. Cerf and S. Iblisdir, Optimal N-to-M cloning of conjugate quantum variables, Phys. Rev. A **62**, 040301(R) (2000).

[19] F. Grosshans and P. Grangier, Quantum cloning and teleportation criteria for continuous quantum variables, Phys. Rev. A **64**, 010301 (2001).

[20] F. Grosshans, A. Acín, and N. J. Cerf, in *Continuous-Variable Quantum Key Distribution* in *Quantum Information with Continuous Variables of Atoms and Light*, edited by N. J. Cerf, G. Leuchs, and E. S. Polzik (Imperial College Press, London, 2012).

[21] M. Navascués, F. Grosshans, and A. Acín, Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography, Phys. Rev. Lett. **97**, 190502 (2006).

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

[23] A. S. Holevo, The capacity of the quantum channel with general signal states, IEEE Trans. Inf. Theory **44**, 269 (1998).

[24] S. Olivares, Quantum optics in the phase space, Eur. Phys. J. Special Topics **203**, 3 (2012).

[25] F. Grosshans, Collective Attacks and Unconditional Security in Continuous Variable Quantum Key Distribution, Phys. Rev. Lett. **94**, 020504 (2005).

[26] D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, Noise-free high-efficiency photon-number-resolving detectors, Phys. Rev. A **71**, 061803(R) (2005).

[27] B. Calkins, P. L. Mennea, A. E. Lita, B. J. Metcalf, W. S. Kolthammer, A. Lamas-Linares, J. B. Spring, P. C. Humphreys, R. P. Mirin, J. C. Gates, P. G. R. Smith, I. A. Walmsley, T. Gerrits, and S. W. Nam, High quantum-efficiency photon-number-resolving detector for photonic on-chip information processing, Opt. Express **21**, 22657 (2013).