Research Article | Vol. 28, No. 10 / 11 May 2020 / Optics Express 14547
Optics EXPRESS

Plug-and-play continuous-variable quantum key distribution for metropolitan networks

R. VALIVARTHI,[1,2,3,7] S. ETCHEVERRY,[1,4,7] J. ALDAMA,[1] F. ZWIEHOFF,[1,5] AND V. PRUNERI[1,6,*]

[1]ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, Castelldefels, Barcelona 08860, Spain
[2]Department of Physics, Mathematics and Astronomy, California Institute of Technology, California 91125, USA
[3]Alliance for Quantum Technologies, California Institute of Technology, Pasadena, California 91125, USA
[4]Department of Physics, Stockholm University, AlbaNova University Center, Stockholm, Sweden
[5]Institut de Física d'Altes Energies (IFAE), The Barcelona Institute of Science and Technology, Bellaterra, Barcelona 08193, Spain
[6]ICREA-Institucio Catalana de Recerca i Estudis Avançats, 08010 Barcelona, Spain
[7]These authors contributed equally to this work
[*]valerio.pruneri@icfo.eu

Abstract: We report a plug-and-play continuous variable quantum key distribution system (CV-QKD) with Gaussian modulated quadratures and a true local oscillator. The proposed configuration avoids the need for frequency locking two narrow line-width lasers. To minimize Rayleigh back-scattering, we utilize two independent fiber strands for the distribution of the laser and the transmission of the quantum signals. We further demonstrate the quantum-classical co-existing capability of our system by injecting high-power classical light in both fibers. A secret key rate up to 0.88 Mb/s is obtained by using two fiber links of 13 km and up to 0.3 Mb/s when adding 4 mW of classical light in the optical fiber used for transmitting the quantum signal. The reported performance indicates that the proposed QKD scheme has the potential to become an effective low-cost solution for metropolitan optical networks.

© 2020 Optical Society of America under the terms of the OSA Open Access Publishing Agreement

1. Introduction

Quantum key distribution (QKD) is one of the most mature quantum cryptography technologies [1–4]. QKD allows for the exchange of secure keys between two authenticated parties, commonly referred as Alice and Bob. QKD combined with one-time pad (OTP) provides a way for achieving information-theoretic security [5]. Two main QKD protocols have been pursued: discrete variable (DV) and continuous variable (CV) [6–8]. While DV-QKD heavily relies on single photon detector technology, CV-QKD provides security through shot-noise limited coherent detection. The strong resilience to incoherent background noise and independence of single photon detector technology have made CV-QKD an attractive solution to secure metropolitan scale networks [9–11]. Owing to the maturity of the security proofs, most of CV-QKD implementations perform the GG02 protocol, introduced by Grosshands and Grangier in 2002 [8], where the quadratures of coherent state of lights are modulated according to zero-centered Gaussian distribution. In the early demonstrations of CV-QKD, the local oscillator (i. e. reference signal needed for coherent detection) was transmitted along with the quantum signal [12–17]. These demonstrations have been shown to be vulnerable to several side-channel attacks based on manipulating the local oscillator by an eavesdropper [18–21]. Recently, CV-QKD with true local oscillator has been demonstrated where the local oscillator is generated at Bob, without being accessible to the eavesdropper [22–28]. Despite improving the security of practical CV-QKD, the experimental implementation of the true local oscillator scheme requires two narrow line-width lasers that are

#391491 https://doi.org/10.1364/OE.391491
Journal © 2020 Received 28 Feb 2020; revised 17 Apr 2020; accepted 17 Apr 2020; published 28 Apr 2020

Optics EXPRESS

frequency-locked, which increases the experimental complexity of the system. In addition, such locking is demanding to be maintained over time, preventing long term stability of the system [26–28].

To overcome this problem, plug-and-play CV-QKD with true local oscillator was proposed and implemented by Huang *et al.* [29]. A single laser was used both as a true local oscillator and as the source to prepare the modulated quadratures, avoiding the need of two frequency-locked lasers. The system reported by Huang *et al.* relies on two-way communication to implement a dual-phase modulated coherent state protocol (DPMCS) with homodyne detection, which is demonstrated to be equivalent to the GG02 protocol from a security perspective. Nevertheless, the reported plug-and-play CV-QKD suffers from Rayleigh back-scattering noise generated by the high power laser signal simultaneously transmitted with the quantum signal at the same wavelength and fiber channel. The Rayleigh back-scattering noise limits the performance and the maximum secure communication distance of the system compared to one-way CV-QKD protocols [29]. Rayleigh back-scattering noise in plug-and-play QKD, and its consequences on the secret key and maximum distance have been studied theoretically and experimentally for DV-QKD [30,31] and CV-QKD systems [29].

In this paper, we propose and demonstrate a plug-and-play CV-QKD system that minimizes the noise from Rayleigh back-scattering. This is done by relaying on two-way communication, where two different fiber strands are used, one to distribute the laser signal from Bob to Alice and the other one to send quantum states from Alice to Bob. To compensate for the phase fluctuations in the two independent fibers, we use a phase correction algorithm that relies on sending reference pulses interleaved between the quantum signals (LLO sequential design [25]). Contrary to previous work [29], the present design, besides minimizing the effect of Rayleigh back-scattering, allows for implementing a symmetric GG02 protocol with heterodyne detection, for which a general and composable security proof has been developed [32].

We note that in a real-world network, several fiber strands are present in a fiber bundle connecting different nodes, and the use of an additional fiber strand does not impose any additional overhead to the network. Moreover, we demonstrate co-existence of strong classical light in both fibers, removing the requirement of dark fibers which is not only considered an expensive solution but also an additional bottleneck for the deployment of QKD technology [33].

2. Experimental setup

Figure 1(a) shows a schematic of the experimental setup. A CW laser (1550 nm wavelength, 10 kHz line-width, 54 mW power) located at Bob is split in two parts by using a 90:10 beam splitter (BS1). The 90% of the laser is used as a true local oscillator for heterodyne detection, whereas the 10% is sent to Alice through a 13 km fiber spool (Corning SMF28 ULL fiber). At Alice, a polarization controller (PC1) and a polarizing beam splitter (PBS) are used to filter the polarization modes and optimize the performance of the subsequent electro-optic modulators.

According to the GG02 protocol [8], Alice generates coherent states of light (weak optical pulses) with X and P quadratures modulated according to zero-centered Gaussian random distributions. To this end, Alice uses an amplitude modulator (AM1) to create and modulate a train of optical pulses, and a phase modulator (PM) to encode phase information onto the pulses. Gaussian distributed quadratures are obtained by modulating the amplitude and the phase of the pulses according to a Rayleigh and a uniform random distribution, respectively [16]. As depicted in Fig. 1(b), pulses with constant amplitude and no encoded phase information (reference pulses) are interleaved between the modulated pulses (quantum signal pulses). The reference pulses allow Bob to compensate for phase drifts in the channel and retrieve the quadrature values sent by Alice [23]. The phase correction procedure is described in Section 3.2.

A second amplitude modulator (AM2) is used to increase the extinction ratio of the light pulses by modulating constant amplitude pulses that are overlapped to those generated by AM1. To

Optics EXPRESS

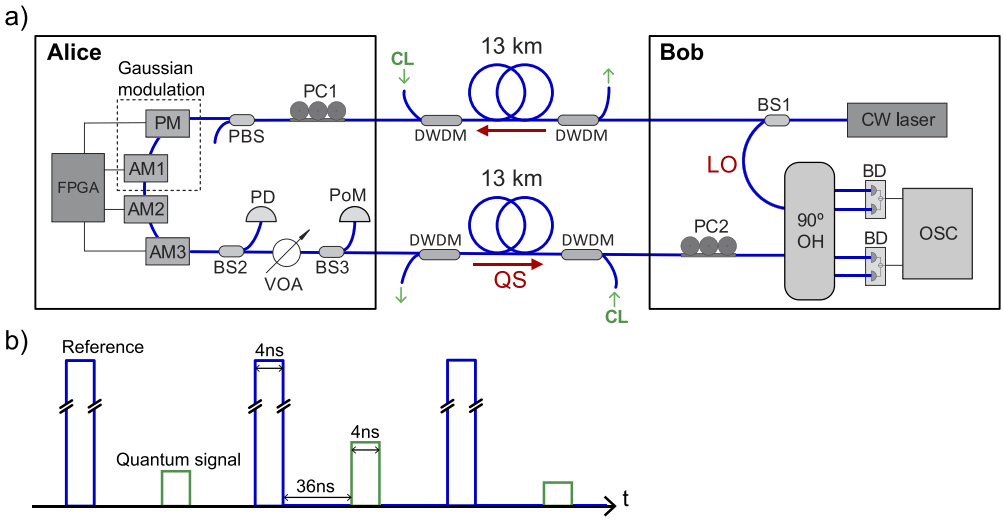

Fig. 1. (a) Experimental setup for the plug-and-play CV-QKD system. Alice prepares optical pulses with Gaussian modulated quadratures and Bob performs heterodyne detection. AM, amplitude modulator; PM, phase modulator; PD, photodiode; PoM, power meter; VOA, variable optical attenuator; PC, polarization controller; PBS, polarizing beam splitter; BS, beam splitter; 90° OH, 90° optical hybrid; OSC, oscilloscope; DWDM, dense wavelength division multiplexer; BD, balanced detector; LO, local oscillator; QS, quantum signal; CL, high power classical light. (b) Transmitted signal from Alice to Bob, where reference pulses are interleaved between the quantum pulses.

accurately recover the phase information of the pulses, the amplitude of the reference pulses has to be larger than the amplitude of the signal (e.g. 500 times in Ref. [24]). The ratio between the amplitude of the reference and signal pulses, R, is set by adjusting the bias set-point of a third amplitude modulator (AM3) that operates at half the clock frequency.

The electro-optic modulators are driven by RF signals generated by a field programmable gate array (FPGA) and a 1 GS/s digital to analog converter (DAC) unit. In the present CV-QKD system, the optical pulses have a width of 4 ns and a frequency of 25 MHz. The RF signals for AM1 and PM are obtained from two independent sequences of 2048 pseudo-random numbers that are constantly repeated. We note that in a final prototype, random numbers should be generated continuously by using, for instance, a quantum random number generator [34].

After the modulator AM3, a 50:50 beam splitter (BS2) and PIN photo detector (PD) are used to optimize the bias set-point of the modulators. A variable optical attenuator (VOA) is employed to set the appropriate modulation variance (V_{mod}) that maximize the secret key for a given channel transmittance. Subsequently, a 99:1 beam splitter (BS3) sends 99% of the light to a power meter (PoM) to measure the mean photon number $\langle n \rangle$ and Alice modulation variance, $V_{\mathrm{mod}} = 2\langle n \rangle$, which was set using the VOA. The modulation variance is known by the parties before the communication. The light from the 1% output of BS3 is sent to Bob through a second 13 km fiber spool (Corning SMF28 ULL fiber). At Bob, a polarization controller (PC2) is used to maximize the polarization overlap between the received pulses and the local oscillator for maximal interference. The incoming optical pulses are fed into a 90° Optical Hybrid (90°OH), where they interfere with the local oscillator. The four outputs of the 90° OH are detected by two balanced photodetectors (BDs), which provide measurements of X and P quadratures. The output from the BDs are digitized using a 2.5 GS/s oscilloscope, whose data is then collected and analyzed. The present design, Fig. 1(a), minimizes the noise from Rayleigh back-scattering, as

Optics EXPRESS

the Rayleigh back-scattered photons generated in the upper fiber spool will go through BS1 to the CW laser which has an integrated isolator and, therefore, will not reach the BDs.

We note that in the proposed plug-and-play system, most of the active components are located at Alice, and Bob only needs to compensate for polarization drifts, which can be done by maximizing the amplitude of the detected quadratures. Another possibility is to use a polarization-diversity 90° optical hybrid [27] at Bob, avoiding the need of active feedback mechanisms.

Finally, to demonstrate the co-existing capabilities of quantum and classical communication in the same fiber, we multiplex and de-multiplex strong classical light (from 0 to 11 mW input power) using dense wavelength division multiplexers (DWDMs) in both fiber spools as shown in Fig. 1. These DWDMs have a pass-band at (1550 ± 0.12) nm with a directivity of 50 dB and an isolation of 40 dB. The classical light is fed in both forward and backward directions with respect to the quantum light to analyse the effects of forward and backward Raman scattering processes on the performance of the system.

3. Analysis and results

3.1. Detector calibration

To achieve shot-noise limited detection with high sensitivity, the local oscillator power should be maximized within the linear operation range of the BDs. Figure 2(a) shows the shot noise variance as a function of the local oscillator power, where the electronic noise variance was subtracted from the measurements. The measurements were carried out by turning off the signal from Alice, having only the local oscillator activated. It can be seen that the detectors have a linear response even for powers up to 54 mW (maximum power of the laser). For the experimental results described below, a local oscillator power of 49 mW is used given the fact that, as mentioned above, 10% of the laser power is transmitted to Alice for quadrature modulation. Figure 2(b) shows the Fourier transform of the shot noise and electronic noise for a power of 49 mW. An average clearance (ratio between shot noise variance and electronic noise variance) of 15.8 dB is obtained over the full bandwidth of the detector (20 kHz-1 GHz). To increase the signal to noise ratio, a low-pass bandwidth filter of 200 MHz is employed at the input of the oscilloscope, which results in an average clearance of 16.8 dB.

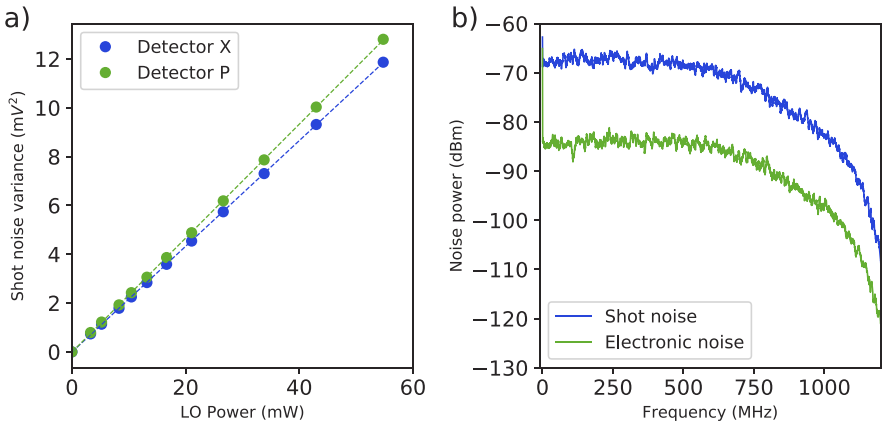

Fig. 2. Calibration of balanced detectors. (a) Shot noise variance as a function of LO power at the input of the optical hybrid. The electronic noise variance has been subtracted from the measurements. (b) Spectral response of the shot noise and electronic noise for a LO power of 49 mW.

Optics EXPRESS

In CV-QKD, the measured quadrature values are converted from voltage units to shot noise units [35]. To this end, a conversion factor is obtained by:

$$\phi = N_0 - N_{\text{det}} \tag{1}$$

where N_0 and N_{det} are respectively the shot noise and electronic noise variance in units of voltage square.

3.2. Phase correction

Since the local oscillator located at Bob and the signal pulses from Alice have not been interferometrically stabilized, the phase of the signal pulses drifts randomly and thereby the encoded information is scrambled. To overcome this, we employ the phase correction procedure described by Qi *et al.* [23]. As mentioned above, reference pulses are sent in close conjunction to the signal pulses. The phase information of the reference pulses is used to extract the encoded phase information onto the signal pulses. We note that in the present system the phase correction procedure should compensate for fluctuations in two independent fibers, which corresponds to an effective distance of twice the separation between Alice and Bob. As mentioned above, to reduce the phase recovery noise, the intensity of the reference pulses is typically much higher than that of the signal pulses. The measured quadrature X_{raw} and P_{raw} are divided into sets of reference pulse data (X_R, P_R) and signal pulse data (X_S, P_S), respectively. The phase of the i^{th} reference pulse, $\Phi_{R,i}$ is given by

$$\Phi_{R,i} = \arctan\left(\frac{P_{R,i}}{X_{R,i}}\right) \tag{2}$$

The phase of the i^{th} signal pulse (S_i) is calculated by using the reference pulses (R_i and R_{i+1}) and

$$\Phi_{S,i} = \frac{\Phi_{R,i} + \Phi_{R,i+1}}{2} \tag{3}$$

The quadratures are then remapped using the coordinate transformations:

$$\begin{aligned} X_{\text{corr},i} &= X_{S,i}\cos\left(\Phi_{S,i}\right) + P_{S,i}\sin\left(\Phi_{S,i}\right) \\ P_{\text{corr},i} &= -X_{S,i}\sin\left(\Phi_{S,i}\right) + P_{S,i}\cos\left(\Phi_{S,i}\right) \end{aligned} \tag{4}$$

Figure 3 shows an example of phase recovery. For simplicity, the quantum signal corresponds to optical pulses with constant amplitude and phase. The blue trace corresponds to the raw quadratures X_{raw} and P_{raw}, where the reference and signal quadratures correspond to the outer and inner ring, respectively. As expected, the phase of the raw signal and reference are randomly distributed from 0 to 2π. After phase correction, by using Eq. (4), the quadratures are centered at a given phase value, which was assigned by Alice. In the results presented in Section 3.5, the quadrature remapping procedure is applied to Gaussian modulated quadratures. The corrected quadratures are then further analysed to calculate the excess noise and the secret key rate as described below. In the following sections, we rename $X \equiv X_{\text{corr}}$ and $P \equiv P_{\text{corr}}$.

3.3. Estimation of excess noise and channel transmittance

Figure 4(a) shows a 4μs sample of the X quadrature for Alice and Bob. Bob's data corresponds to the output of the heterodyne detector after phase correction. Alice and Bob quadratures follow zero-centered Gaussian distributions, as it is shown in Fig. 4(b). The variance of Alice and Bob quadrature distributions, V_{mod} and V_B, are related by [35]

$$V_B = \frac{T\eta}{2}V_{\text{mod}} + \frac{\varepsilon}{2} + \nu_{\text{elec}} + 1 \tag{5}$$

where ε is excess noise measured at the channel output, ν_{elec} is the electronic noise, η is the detection efficiency, and T is the transmittance of the channel. The excess noise can be calculated

Optics EXPRESS

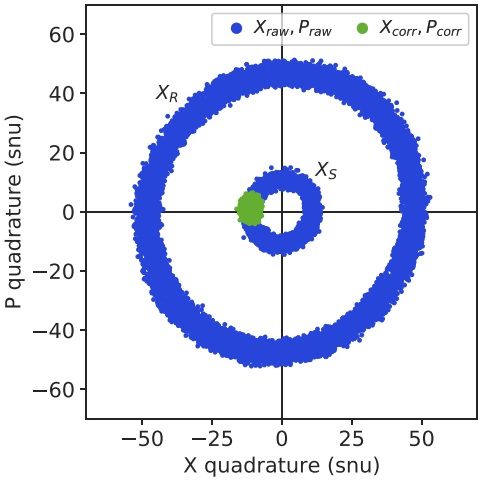

Fig. 3. Phase correction. The blue and green traces correspond to the raw quadratures (X_{raw}, P_{raw}) and corrected quadratures (X_{corr}, P_{corr}), respectively. The raw quadratures are divided into the reference (X_R) and signal (X_S) quadratures. To show the phase correction clearly, this measurement was carried out using high intensity signal pulses with constant amplitude and phase, and a ratio between reference and signal amplitude of R=17.

from

$$\varepsilon = 2\left(V_{B|A} - 1 - \nu_{\text{elec}}\right) \tag{6}$$

where $V_{B|A}$ is the conditional variance given by [35]

$$V_{B|A} = \text{var}\left(\sqrt{\frac{T\eta}{2}}q_A - q_B\right), \tag{7}$$

$q_A = \{X_{Ai}, P_{Ai}\}$ and $q_B = \{X_{Bi}, P_{Bi}\}$ are Alice and Bob quadrature data, respectively. The losses in the channel are assumed to be controlled by the eavesdropper (Eve), therefore, T has to be estimated by correlating Alice and Bob data,

$$T = \frac{2}{\eta}\left(\frac{\langle q_A q_B\rangle}{V_{\text{mod}}}\right)^2 \tag{8}$$

For the analysis of the experimental data we consider two scenarios, the "realistic scenario" [15,23] where the detection efficiency is trusted and calibrated, and the "paranoid scenario without electronic noise" [36,37] where the detection efficiency is not trusted and treated as losses in the channel. For both scenarios, the electronic noise is trusted and subtracted from the total excess noise.

It is important to note that in the asymptotic analysis presented here, the entire data set is used for parameter estimation to obtain accurate values of excess noise and channel transmittance. However, in a future prototype, finite-size effects [36] and key reconciliation [8] will be included to distil a secret key. This might reduce the key rate because part of the correlated data is sacrificed for parameter estimation, whereas the remaining data is used for secret key generation. However, recent results in CV-QKD have shown that the entire data set could be used for both parameter estimation and secret key generation [38].

Optics EXPRESS

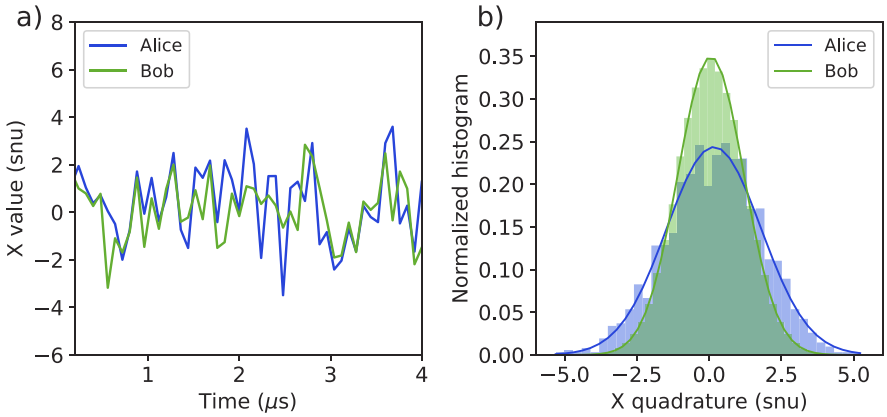

Fig. 4. Estimation of ε and T. (a) 4 μs sample of Alice (blue) and Bob (green) correlated data for the X quadrature. (b) Histogram of the X quadrature data for Alice (blue) and Bob (green).

3.4. Estimation of secret key rate

The secret key rate r, in bits per pulse, is given by [23,35]

$$r = fI_{AB} - \chi_{BE} \tag{9}$$

where f is the efficiency of the reconciliation algorithm, I_{AB} is the mutual information between Alice and Bob, and χ_{BE} is the Holevo bound. Considering reverse reconciliation [8], the Holevo bound corresponds the maximum accessible information that Eve could have on Bob data. The mutual information I_{AB} can be directly computed from the Shannon entropy and the experimental parameters,

$$I_{AB} = \log_2(1 + \mathrm{SNR}) \tag{10}$$

where the signal to noise ratio (SNR) is given by

$$\mathrm{SNR} = \frac{\eta T V_{\mathrm{mod}}}{2 + \varepsilon - 2\nu_{\mathrm{elec}}} \tag{11}$$

The calculation of the Holevo bound requires the computation of the co-variance matrix between Alice and Bob, which depends on the experimental parameters. A detailed description for the estimation of the Holevo bound is presented in Ref. [23,35]. Once Alice and Bob mutual information and Holevo bound are calculated, r is directly obtained from Eq. (9). The reconciliation efficiency f is considered to be 0.95 [13]. The secret key rate K in bits per second is obtained by multiplying r by the repetition rate of the signal pulses, 12.5 MHz.

3.5. Results

Figure 5(a) shows the excess noise ε, obtained using Eq. (6), as a function of Alice modulation variance V_{mod} for a ratio between reference signal and quantum signal amplitude of R=274. The electronic noise is $\nu_{\mathrm{elec}} = 0.022$ snu and the detection efficiency is $\eta = 0.38$. The detection efficiency was estimated from the quantum efficiency of the balanced detectors, losses at Bob, and the effect of the low-pass filter. Each point corresponds to ≈1.4 million signal samples, which are collected from the oscilloscope. The raw data is subjected to phase correction and then channel transmittance, excess noise, and secret key rate are calculated. Considering a linear

Optics EXPRESS

model for excess noise [26],

$$\varepsilon = \sigma V_{\text{mod}} + \varepsilon_{\text{rest}} \tag{12}$$

where the first term is the noise that depends on the modulation variance, such as the noise arising from imperfect phase correction [25]. The second term is the noise which is independent of the modulation variance, such as intensity noise of the local oscillator or CMRR-noise [35]. Fitting Eq. (12) to the experimental data, Fig. 5(a), we obtain $\sigma = 0.0067$, and $\varepsilon_{\text{rest}} = 0.0004$ snu. The value of K as a function of the modulation variance, for the realistic scenario, is shown in Fig. 5(b), where the solid line was obtained using Eq. (9) and Eq. (12). The value of V_{mod} that optimizes K for a distance of 13 km ($T = 0.6$) is approximately $V_{\text{mod}} = 2$ snu.

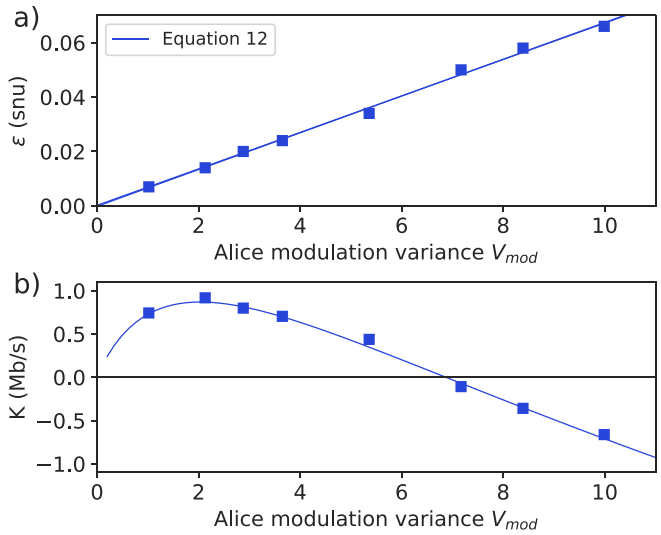

Fig. 5. (a) Excess noise versus modulation variance. (b) Secret key rate versus modulation variance for the realistic scenario. The experimental parameters are $\nu_{\text{elec}} = 0.022$ snu, $R = 274$, $\langle T\eta \rangle = 0.23$, and $\eta = 0.38$

Figure 6(a) shows the variation of the excess noise over 11 measurements taken during 90 minutes. The value of V_{mod} was set to 2.18 snu. The excess noise ε has a mean value of 0.016 snu and varies between 0.013 and 0.020 snu. The solid and dashed black lines correspond to the threshold after which K is zero, for the realistic (0.0375 snu) and paranoid (0.0250 snu) scenario, respectively. Figure 6(b) shows the value of K obtained for each measurement. For the realistic (paranoid) scenario, K fluctuates between 0.49 Mb/s (0.05 Mb/s) and 0.88 Mb/s (0.44 Mb/s) with an average value of 0.74 Mb/s (0.3 Mb/s). The fluctuations of ε and K mainly come from variations in the bias set-point of the electro-optic modulators and polarization changes in the fibers, which in turn affects V_{mod} and T, as can be seen in Fig. 6(c). Active feedback mechanism for polarization and modulator bias can improve the stability of the system and allows for field demonstrations.

Three contributions to ε can be identified. First, the noise $\varepsilon_{\text{drift}}$ coming from the error in the phase correction due to phase drift of the signal pulse compared to the reference pulse as they are generated at a time delay τ. For a plug-and-play system with only one laser, $\varepsilon_{\text{drift}}$ can be calculated as [25]

$$\varepsilon_{\text{drift}} = (4\pi\Delta\nu\tau)V_{\text{mod}}T\eta \tag{13}$$

where $\Delta\nu$ is the linewidth of the laser. Considering $\Delta\nu$=10 kHz and τ=40 ns, we obtain $\varepsilon_{\text{drift}} = 0.0024$ snu. The term $T\eta$ is added to scale to noise to the channel output. A second

Optics EXPRESS

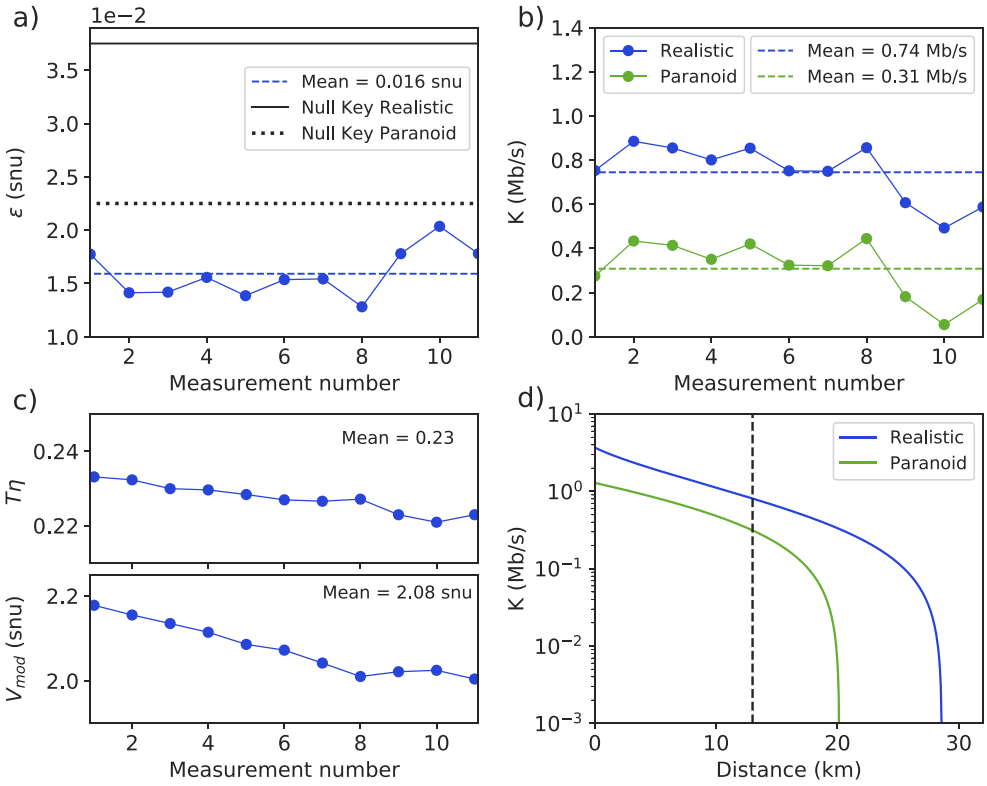

Fig. 6. 11 measurements obtained during 90 minutes. (a) Variation of the excess noise. The dashed and solid line represent the null secret key rate (K) threshold for the realistic and paranoid scenario. (b) K under the realistic and paranoid scenario. (c) Fluctuation of $T\eta$ (top) and modulation variance V_{mod} (bottom). (d) Simulation of K as a function of distance for the realistic and paranoid scenarios. The experimental parameters are $\nu_{\text{elec}} = 0.022$ snu, $R = 274$, $\langle T\eta \rangle = 0.23$, $\langle V_{\text{mod}} \rangle = 2.08$ snu, and $\eta = 0.38$

contribution to ε, which also affects the phase correction algorithm, comes from the error present on the reference pulses due to channel noise and shot noise,

$$\varepsilon_{\text{error}} = (1 + \chi)T\eta/R \tag{14}$$

where $\chi = 1/T - 1 + \varepsilon/(T\eta)$ is the total channel added noise. Considering the parameters of Fig. 6, we obtain $\varepsilon_{\text{error}} = 0.0013$. The value of $\varepsilon_{\text{error}}$ decreases when increasing R, as the noise on the reference pulses is less significant and the estimation of the signal phase is more accurate. A third contribution to ε arises from leak photons due to the finite dynamic range of the amplitude modulator (DR). This noise, referred to as ε_{AM}, contrary to $\varepsilon_{\text{error}}$, increases when increasing the amplitude of the reference pulse RV_{mod}. An estimation of ε_{AM} is given by

$$\varepsilon_{\text{AM}} = RV_{\text{mod}}10^{-DR/10}T\eta \tag{15}$$

The use of three amplitude modulators, as described in Section 2., allows for a high dynamic range and a large value of R, reducing ε_{AM} and $\varepsilon_{\text{error}}$. We achieve a dynamic range of $DR = 48$ dB which results in $\varepsilon_{\text{AM}} = 0.002$ snu. We note that ε_{AM} can be significantly reduced by replacing the second modulator (AM2) by a high extinction amplitude modulator >60dB [39]. A detailed description of additional source of noise can be found in Ref. [35]. Finally, Fig. 6(d) shows a

Optics EXPRESS

simulation of K versus distance for the realistic and paranoid scenarios. It can be seen that the present system may allow for operation over longer distances. For instance, a secret key of 0.12 Mb/s could be obtained at 25 km in the realistic scenario. We note that longer distances may reduce the accuracy of the phase correction algorithm and increase the excess noise, since the intensity of reference pulses drops due to channel losses, which in principle could be compensated by increasing the intensity of the reference pulses at Alice [26].

3.6. Estimation of Rayleigh back-scattering

As it is mentioned above, the proposed design minimizes the effects of Rayleigh back-scattering on the excess noise. To quantify the advantage of this, we estimate the extra excess noise that we would have from Rayleigh back-scattered photons ε_{RB}, considering the parameters of our system. This is done by using [29,30]

$$\varepsilon_{RB} = \frac{\beta_R \left[1 - 10^{(-2\alpha L/10)}\right] V_A R_{\text{rate}} \eta \delta t}{\eta_A T} \tag{16}$$

The parameter β_R is the Rayleigh back-scattering coefficient, −80 dB [29]. R_{rate} is the repetition rate, 25 MHz. δt is the detector integration time, 5 ns. α is the fiber attenuation coefficient, 0.17 dB/km, and η_A is the total losses at Alice, ≈45 dB. Equation (16) considers the case of minimum Rayleigh back-scattering, where the attenuator at Alice is fully opened and the light sent by Bob is minimized. Considering the values of Sec. 3.5 (L = 13 km, η = 0.38, T = 0.6, V_A = 2.11 snu), we estimate that the mean excess noise, Fig. 6(a), would be ≈50% higher in case of Rayleigh back-scattering reaching the detectors, and the secret key rate ≈40% lower. The Rayleigh back-scattering noise becomes higher at longer distances, and at 28 km, without considering any other source of noise, it would make the secret key rate equal to zero for the parameters of our system.

3.7. Coexistence with classical light

To demonstrate the coexistence capability between CV-QKD and transmission of classical signal, we input intense classical light (wavelength of 1542 nm) to both fibers strands and characterize the excess noise. Raman scattering from the fiber is the main source of noise when co-propagating intense signals with quantum signals at a different wavelength [9,33,40–42]. First, we added up to 12 mW of power in the fiber used for sharing the lasers between Alice and Bob, without seeing a significant effect on the excess noise. On the other hand, adding classical light to the fiber transmitting the quantum signals increases the excess noise, as depicted in Fig. 7. We study the backward Raman scattering effects, when the classical light and quantum light are propagating in the opposite directions Fig. 7(a), and the forward Raman scattering, when the quantum and classical light are in the same direction , Fig. 7(b). We see that the excess noise increases linearly with the power of the classical light [9]. A positive K can be obtained for power up to 8 mW in the backward or forward direction. For instance, K of 0.3 Mb/s is obtained for a classical light power of 4 mW. These results show that our system can coexist with high speed data communication. For instance, a 10Gb/s error-free communication channel at 50 km can be achieved with an input power of only 0.04 mW [43]. The experimental parameters considered for the measurements shown in Fig. 7 are $T\eta$ = 0.20, η = 0.33, and V_{mod} = 3.4 snu. The detection efficiency is lower compared to results showed in previous sections because of losses in Bob's DWDM. The results obtained for backward and forward Raman scattering configurations are similar, which is expected for a distance of 13 km [9]. Due to the fiber loss, forward Raman scattering increases with the distance and reaches a peak value at approximately 21 km, whereas backward Raman scattering increases up to approximately 40 km, where it saturates [9,33]. The Raman scattering at the distance of 13 km, used in this work, corresponds to approximately 80% and 60% of the maximum value for forward and backward directions, respectively.

Optics EXPRESS

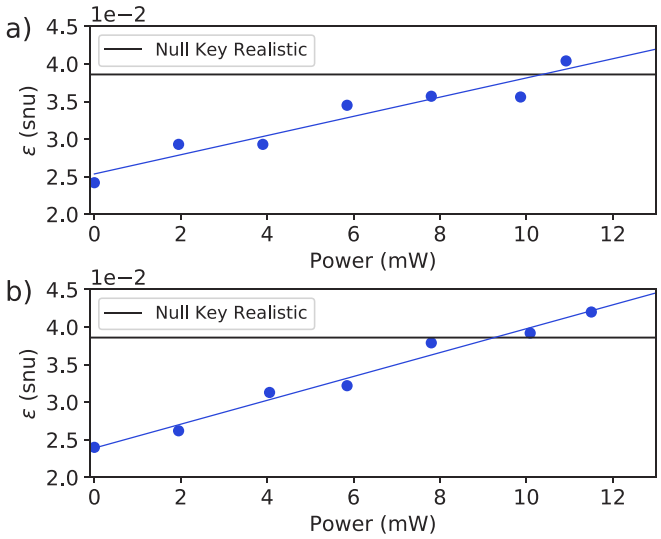

Fig. 7. Excess noise versus power of the classical channel for the (a) backward and (b) forward directions. The experimental parameters are $\langle T\eta \rangle = 0.20$, $\eta = 0.33$, and $\langle V_{\text{mod}} \rangle = 3.4$ snu.

We note that in the results showed in Fig. 7, the quantum signal is placed at a longer wavelength than the classical signal (quantum signal at 1550nm and classical signal at 1542 nm). This corresponds to the worst case scenario, since the Raman Stokes peak overlaps with the quantum signal, which is around 10% stronger that the Anti-Stokes peak [40].

3.8. *Side channel attacks and preparation noise*

Plug-and-play QKD has been traditionally shown to be vulnerable to Trojan horse attacks [44,45]. Recent investigations have proposed techniques to overcome these attacks. In plug-and-play QKD, it is important to have a watchdog detector at the Alice input to detect any unwanted optical signal. Also, the use of frequency filters at Alice input help preventing Eve from injecting optical signals at a frequency outside the bandwidth of the watchdog detector [44]. In our scheme, since the present plug-and-play system uses two fibers links, it is possible to add isolators at the input and output of Alice to avoid Trojan-horse attacks that could exploit reflected light from the modulators.

Contrary to one-way CV-QKD, plug-and-play systems give the eavesdropper access to the laser source [29]. However, there is no key information on the laser signal going from Bob to Alice, and the calibration of the system is performed locally at Bob. Therefore, if side-channel attacks are properly compensated, transmitting the laser source does not generate security problems. Nevertheless, the eavesdropper can manipulate the source to worsen the performance of the QKD session, for instance by adding phase noise to the laser. To overcome this, Alice can characterize the preparation noise of the signal, which may result in a significant improvement on the performance of the system [46,47].

4. Conclusions

CV-QKD with true local oscillator is known to be a promising solution for the integration of QKD into commercial optical networks. However, the requirement of two frequency stable lasers adds technological complexity to the system. It is also to be noted that, without proper feedback, the intrinsic frequency fluctuations between the lasers will prevent long term stable system

Optics EXPRESS

operation. With our work, we overcome these drawbacks by demonstrating a plug-and-play CV-QKD system where the same laser is used as true local oscillator and as the source to prepare Gaussian-modulated coherent states. In addition, we avoid the deterioration of the performance due to Rayleigh back-scattering by using a separate fiber to send the light from Bob to Alice. Finally, our system can co-exist with strong classical light, thereby showing that plug-and-play CV-QKD is an effective solution for securing short-reach metropolitan networks.

Funding

Horizon 2020 Framework Programme (820466); Ministerio de Economía y Competitividad (SEV-2015-0522); Fundación Privada Cellex; Fundació Mir-Puig; Generalitat de Catalunya (CERCA program); Vetenskapsrådet (International postdoc grant); Deutscher Akademischer Austauschdienst; European Regional Development Fund (ERDF Operational Program of Catalonia 2014-2020); H2020 Marie Skłodowska-Curie Actions (713729).

Acknowledgments

We thank Dan Nolan from Corning Inc. for providing the ultralow loss optical fibers used in this work.

Disclosures

The authors declare no conflicts of interest.

References

1. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing, *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* pp. 175–179 (1984).
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**(1), 145–195 (2002).
3. H. K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," Nat. Photonics **8**(8), 595–604 (2014).
4. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in Quantum Cryptography," arXiv:1906.01645 (2019).
5. C. E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J. **28**(4), 656–715 (1949).
6. T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**(1), 010303 (1999).
7. M. Hillery, "Quantum cryptography with squeezed states," Phys. Rev. A **61**(2), 022309 (2000).
8. F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**(6920), 238–241 (2003).
9. R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable QKD with intense DWDM classical channels," New J. Phys. **17**(4), 043027 (2015).
10. T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luas, M. Fujiwara, R. Namiki, Y. Awaji, M. Takeoka, N. Wada, and M. Sasaki, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 Tbit/s data channels," Commun. Phys. **2**(1), 9 (2019).
11. F. Karinou, H. H. Brunner, C.-H. F. Fung, L. C. Comandar, S. Bettelli, D. Hillerkuss, M. Kuschnerov, S. Mikroulis, D. Wang, and C. Xie, "Toward the integration of CV quantum key distribution in deployed optical networks," IEEE Photonics Technol. Lett. **30**(7), 650–653 (2018).
12. P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," Phys. Rev. A **87**(6), 062313 (2013).
13. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**(5), 378–381 (2013).
14. B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, C. Marquardt, and G. Leuchs, "Atmospheric continuous-variable quantum communication," New J. Phys. **16**(11), 113018 (2014).
15. S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, "Field test of a continuous-variable quantum key distribution prototype," New J. Phys. **11**(4), 045023 (2009).
16. C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng, "25 Mhz clock continuous-variable quantum key distribution system over 50 km fiber channel," Sci. Rep. **5**(1), 14607 (2015).
17. D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Rep. **6**(1), 19201 (2016).
18. X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol," Phys. Rev. A **87**(5), 052309 (2013).

Optics EXPRESS

19. J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," Phys. Rev. A **87**(6), 062329 (2013).
20. X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems," Phys. Rev. A **88**(2), 022339 (2013).
21. H. Häseler, T. Moroder, and N. Lütkenhaus, "Testing quantum devices: Practical entanglement verification in bipartite optical systems," Phys. Rev. A **77**(3), 032303 (2008).
22. D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," Opt. Lett. **40**(16), 3695–3698 (2015).
23. B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," Phys. Rev. X **5**(4), 041009 (2015).
24. D. B. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," Phys. Rev. X **5**(4), 041010 (2015).
25. A. Marie and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution," Phys. Rev. A **95**(1), 012316 (2017).
26. T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng, "High key rate continuous-variable quantum key distribution with a real local oscillator," Opt. Express **26**(3), 2794–2806 (2018).
27. F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, F. Karinou, A. Poppe, M. Peev, and H. Hübel, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," Quantum **3**, 193193 (2019).
28. S. Kleis, M. Rueckmann, and C. G. Schaeffer, "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals," Opt. Lett. **42**(8), 1588–1591 (2017).
29. D. Huang, P. Huang, T. Wang, H. Li, Y. Zhou, and G. Zeng, "Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol," Phys. Rev. A **94**(3), 032305 (2016).
30. D. Subacius, A. Zavriyev, and A. Trifonov, "Backscattering limitation for fiber-optic quantum key distribution systems," Appl. Phys. Lett. **86**(1), 011103 (2005).
31. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a plug&play system," New J. Phys. **4**, 34141 (2002).
32. A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Phys. Rev. Lett. **114**(7), 070501 (2015).
33. K. Patel, J. Dynes, I. Choi, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, "Coexistence of high-bit-rate quantum key distribution and data on optical fiber," Phys. Rev. X **2**(4), 041010 (2012).
34. M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, M. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," Opt. Express **19**(21), 20665–20672 (2011).
35. F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel, "Continuous-variable quantum key distribution with gaussian modulation - the theory of practical implementations," Adv. Quantum Technol. **1**(1), 1800011 (2018).
36. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**(6), 062343 (2010).
37. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**(3), 1301–1350 (2009).
38. C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandol, "Parameter Estimation with Almost No Public Communication for Continuous-Variable Quantum Key Distribution," Phys. Rev. Lett. **120**(22), 220505 (2018).
39. S. Liu, H. Cai, C. DeRose, P. Davids, A. Pomerene, A. Starbuck, D. Trotter, R. Camacho, J. Urayama, and A. Lentine, "High speed ultra-broadband amplitude modulators with ultrahigh extinction > 65 db," Opt. Express **25**(10), 11254–11264 (2017).
40. P. Eraerds, N. Walenta, M. Legré, N. Gisin, and H. Zbinden, "Quantum key distribution and 1 Gbps data encryption over a single fibre," New J. Phys. **12**(6), 063027 (2010).
41. B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," New J. Phys. **12**(10), 103042 (2010).
42. T. F. da Silva, G. B. Xavier, G. P. Temporao, and J. P. von der Weid, "Impact of Raman scattered noise from multiple telecom channels on fiber-optic quantum key distribution systems," J. Lightwave Technol. **32**(13), 2332–2339 (2014).
43. K. Patel, J. Dynes, M. Lucamarini, I. Choi, A. Sharpe, Z. Yuan, R. Penty, and A. Shields, "Quantum key distribution for 10 Gb/s dense wavelength division multiplexing networks," Appl. Phys. Lett. **104**(5), 051123 (2014).
44. N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, "Risk analysis of Trojan-horse attacks on practical quantum key distribution systems," IEEE J. Sel. Top. Quantum Electron. **21**(3), 168–177 (2015).
45. N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," Phys. Rev. A **73**(2), 022320 (2006).
46. V. C. Usenko and R. Filip, "Trusted noise in continuous-variable quantum key distribution: a threat and a defense," Entropy **18**(1), 20 (2016).
47. F. Laudenbach and C. Pacher, "Analysis of the Trusted-Device Scenario in Continuous-Variable Quantum Key Distribution," Adv. Quantum Technol. **2**(11), 1900055 (2019).

131.215.252.102 {ts '2020-06-25 12:44:45'}