



Modulation leakage vulnerability in continuous-variable quantum key distribution

Jain, Nitin; Derkach, Ivan; Chin, Hou Man; Filip, Radim; Andersen, Ulrik L.; Usenko, Vladyslav C.; Gehring, Tobias

Published in:
Quantum Science and Technology

Link to article, DOI:
[10.1088/2058-9565/ac0d4c](https://doi.org/10.1088/2058-9565/ac0d4c)

Publication date:
2021

Document Version
Early version, also known as pre-print

[Link back to DTU Orbit](#)

Citation (APA):
Jain, N., Derkach, I., Chin, H. M., Filip, R., Andersen, U. L., Usenko, V. C., & Gehring, T. (2021). Modulation leakage vulnerability in continuous-variable quantum key distribution. *Quantum Science and Technology*, 6(4), Article 045001. <https://doi.org/10.1088/2058-9565/ac0d4c>

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal

If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Modulation leakage vulnerability in continuous-variable quantum key distribution

NITIN JAIN,^{1,*} IVAN DERKACH,^{2,‡} HOU-MAN CHIN,^{1,3} RADIM FILIP,²
ULRIK L. ANDERSEN,¹ VLADYSLAV C. USENKO,² AND
TOBIAS GEHRING^{1,†}

¹Center for Macroscopic Quantum States (*bigQ*), Department of Physics, Technical University of Denmark, 2800 Lyngby, Denmark

²Department of Optics, Faculty of Science, Palacky University, 17. listopadu 50, 772 07 Olomouc, Czech Republic

³Department of Photonics, Technical University of Denmark, 2800 Lyngby, Denmark

*nitin.jain@fysik.dtu.dk

‡ivan.derkach@upol.cz

†tobias.gehring@fysik.dtu.dk

Abstract: Flaws in the process of modulation, or encoding of key bits in the quadratures of the electromagnetic light field, can make continuous-variable quantum key distribution systems susceptible to leakage of secret information. Here, we report such a modulation leakage vulnerability in a system that uses an optical in-phase and quadrature modulator to implement a single sideband encoding scheme. The leakage arises from the limited suppression of a quantum-information-carrying sideband during modulation. Based on the results from a proof-of-concept experiment, we theoretically analyse the impact of this vulnerability. Our results indicate that the leakage reduces the range over which a positive secret key can be obtained, and can even lead to a security breach if not properly taken into account. We also study the effectiveness of additional trusted noise as a countermeasure to this vulnerability.

© 2021 Optical Society of America under the terms of the [OSA Open Access Publishing Agreement](#)

1. Introduction

Quadrature modulation played a significant role in the revival of classical optical communication and the inception of continuous-variable (CV) quantum optical communication at the turn of this century [1–4]. Information encoded in the amplitude and phase quadratures of the electric field, usually denoted by I and Q in classical communication or x and p in quantum communication, is decoded using coherent detection. The main difference between quantum and classical communication using optical modulation is that in the former, the signal states are typically much weaker than in the latter. Any two such quantum states are then non-orthogonal in practice, i.e., they exhibit an overlap in phase space. This property of non-orthogonality, together with the no-cloning theorem and Heisenberg’s uncertainty principle, forms the bedrocks of quantum key distribution (QKD), a cryptographic method that facilitates secure communication [5–8].

An optical coherent state CVQKD transmitter randomly modulates the output of a coherent laser source along the x and/or p quadratures. In the so-called sideband encoding approach [9], the information carried by the light beam leaving the transmitter can be described in the form of modulation sidebands: coherent states are generated as a result of weak modulation applied at frequency (side-)bands shifted away from the optical carrier [10]. After being exposed to loss and noise on the quantum channel, the sidebands are measured by the CVQKD receiver using a local oscillator (LO) assisted coherent detector to decode the information in the quadrature(s).

These steps are performed as a part of a ‘CVQKD protocol’ that allows the transmitter (Alice) and receiver (Bob) to share correlated bitstreams, which are used as secret keys for encryption after some classical data processing [7, 8]. Security of the key is assessed by evaluating a lower

bound on the final key length, which characterizes the information advantage of Alice and Bob over an eavesdropper (Eve), assumed to control the quantum channel. A non-zero key length assures Alice and Bob that Eve possesses at most an insignificant knowledge of the key, while a zero value implies the channel to be too unsafe for exchanging confidential messages.

Realistic cryptographic systems, whether quantum or classical, are however vulnerable to side channels that lead to security loopholes in both design and implementation [8, 11]. Such loopholes can destroy the security assurance: in QKD systems, Eve obtains significant information about the shared key without leaving any footprints. CVQKD systems too have been known to be prone to attacks due to device imperfections and operational limitations [12–17].

Here, we experimentally demonstrate and theoretically analyze a vulnerability due to modulation leakage [18] in a CVQKD setup that implements an optical single sideband (OSSB) encoding scheme using an in-phase and quadrature (IQ) modulator. OSSB encoding is a technique where one of the two sidebands around the optical carrier is eliminated, effectively resulting in a single (modulated) sideband at the output of the transmitter. Apart from being spectrally efficient and immune to dispersion related issues [19], OSSB modulation potentially offers better noise performance for CVQKD systems by placement of sidebands in a manner that avoids the noisy carrier during modulation and the low-frequency noise region during detection [20].

However, any practical IQ modulator is capable of only finite sideband suppression, so information about the random modulation along x and/or p at the transmitter is leaked on the quantum channel through the suppressed band. Eve may be able to access this suppressed band without alerting the legitimate parties, and can thus obtain more information about the key than estimated. Through a proof-of-principle experiment and ensuing security analysis, we show that as we (intentionally) reduce the sideband suppression by 20 dB (starting with the best possible value of ~ 24 dB), the leakage of the secret key rises from 0.063 to 0.19 bits/symbol for reverse reconciliation (RR) and from 0.15 to 0.99 bits/symbol for direct reconciliation (DR) techniques. One way to address this security issue is to lower the bound on the secret key length, after having quantified the influence of the leakage on the Holevo information. We also investigate the conditions under which noise sources not controlled by Eve could reduce this penalty.

In the last 5 years, there has been a gradual shift in CVQKD setups to replace the discrete amplitude and phase modulators with an IQ modulator to prepare phase-shift keying or Gaussian constellations [21–24]. This move offers a compact design, potential cost benefits, and may also improve resilience to a Trojan-horse attack (through the reduction of a fiber connection) [15, 25]. However, poor sideband suppression, which could arise due to sub-optimal settings of the DC bias control of the IQ modulator or due to finite manufacturing tolerance and RF mismatch, can lead to insecure keys if Alice and Bob do not take the leakage into account. Although the demonstrated vulnerability affects CVQKD systems based on single-sideband encoding only, leakage can also occur due to production of higher-order sidebands (in the so-called ‘strong modulation’ regime), or more generally, due to multiple back-reflections inside Alice’s station [12, 15, 25].

The paper is organized as follows: we first develop a basic model of an IQ modulator and describe the conditions in which the leakage gets manifested. We then describe the attack model that treats the suppressed sidebands as excessive modulation. After detailing the experiment and the proof-of-concept implementation of Eve’s attack strategy, we present the measurement results. Following a discussion on the impact of the attack and countermeasures, we conclude this work.

2. Theoretical background

As shown in Fig. 1(a), the IQ modulator is essentially a Mach-Zehnder interferometer consisting of two nested Mach-Zehnder modulators (MZMs) and a phase modulator (PM). These modulators are characterized by V_π , the voltage at which the optical phase changes by π . For a MZM, this means going from maximum optical transmission to the minimum, or vice versa.

In the so-called optical single sideband modulation with carrier suppression (OSSB-CS)

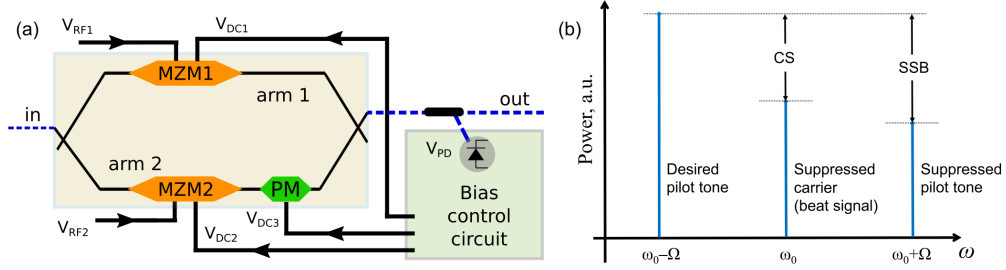


Fig. 1. Optical single sideband modulation with carrier suppression (OSSB-CS) from an IQ modulator. (a) The incoming light is split into two arms, and RF signals V_{RF1} and V_{RF2} with a phase difference of 90° drive Mach-Zehnder modulators (MZMs) operating on minima due to V_{DC1} and V_{DC2} . A relative phase of 90° , added by the phase modulator (PM) using V_{DC3} , then ensures OSSB-CS. The output is tapped to generate the photodiode signal V_{PD} used for feedback control of the bias voltages. (b) Theoretical spectrum depicting both SSB and CS; also see equation (3). The amount of SSB and CS can be improved, though not always independently, by tuning the parameters such as dither amplitude and feedback photodiode gain of the bias circuit.

mode [19, 26], both MZM1 and MZM2 are biased at the minimum transmission point, e.g., $V_{DC1} = V_{DC2} = -V_{\pi}^{\text{MZM}}$, while the PM voltage is e.g., $V_{DC3} = -V_{\pi/2}^{\text{PM}}$ to make the optical signals at the output beam-splitter combine in quadrature. If the RF waveforms to the two MZMs are sinusoids in quadrature, such as $V_{RF1}(t) = A_1 \sin(\Omega t)$ and $V_{RF2}(t) = A_2 \cos(\Omega t)$, the electric field obtained at the output of (an ideal) IQ modulator is

$$E_o(t) \propto [\sin(\mu_1 \sin(\Omega t)) + i \sin(\mu_2 \cos(\Omega t))] E_i(t), \quad (1)$$

given an electric field $E_i(t)$ at the input. Here, $\mu_j = \pi A_j / 2V_{\pi}^{\text{MZM}}$ captures the effective modulation depth in arm j , for $j = 1$ or 2 .

Using the (first two terms from) Jacobi-Anger expansion¹, we can rewrite Eq. (1) as

$$\begin{aligned} E_o(t) &\propto [J_1(\mu) (\cos(\Omega t) + i \sin(\Omega t)) - J_3(\mu) (\cos(3\Omega t) - i \sin(3\Omega t))] E_i(t) \\ &= J_1(\mu) e^{i(\omega_0 + \Omega)t} - J_3(\mu) e^{i(\omega_0 - 3\Omega)t}, \end{aligned} \quad (2)$$

given an input field $E_i(t) \propto e^{i\omega_0 t}$ and assuming $\mu_1 \approx \mu_2 = \mu$. Here J_k denotes a Bessel function of the first kind and order k . Note that a global phase of $\pi/2$ has been omitted in the above.

Eq. (2) illustrates a *complete* suppression of the lower sideband at a frequency offset $-\Omega$ from the carrier. Moreover, since CVQKD transmitters operate the IQ modulator at low modulation depths for preserving linearity, one can consider $J_3(\mu) \approx 0$ because $\mu \ll 1$. The output field is then a single optical line at frequency $\omega_0 + \Omega$, and exhibits perfect OSSB-CS.

In practice, such an infinite suppression of the carrier and a sideband is however impossible because of imprecise DC biasing, finite manufacturing tolerance, RF mismatch, etc. In the above example, one can thereby anticipate the presence of a suppressed carrier at frequency ω_0 and a suppressed sideband at $\omega_0 - \Omega$ in the output field. Under the low modulation depth condition in

¹ $\sin(z \sin \theta) = 2 \sum_{n=1}^{\infty} J_{2n-1}(z) \sin[(2n-1)\theta]$ and $\sin(z \cos \theta) = -2 \sum_{n=1}^{\infty} (-1)^n J_{2n-1}(z) \cos[(2n-1)\theta]$.

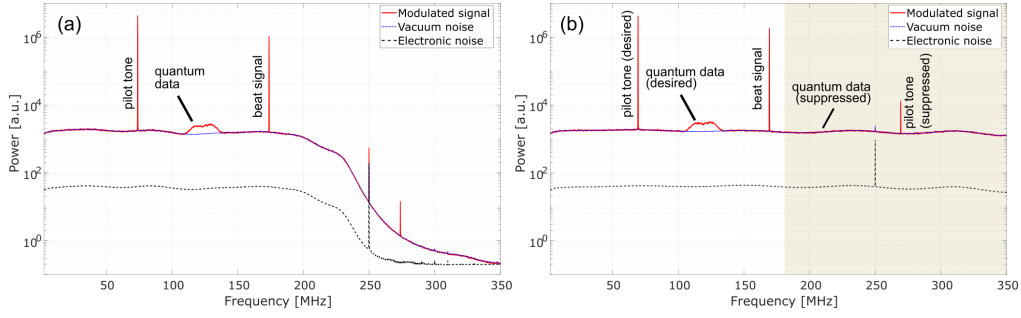


Fig. 2. Heterodyne spectra of frequency-multiplexed quantum data sideband and pilot tone (and other signals relevant to CVQKD measurements). (a) A low pass filter (LPF) with cutoff frequency of 200 MHz, used primarily for reducing out-of-band noise, also hides the suppressed sidebands quite well. (b) Once the 200 MHz LPF is removed, the suppressed pilot tone becomes much more apparent. The vulnerability arises if Alice and Bob do not take into account the leakage from the suppressed components (in the shaded region), as they are obviously present in the actual optical signal transmitted by Alice on the quantum channel, and thus fully accessible to Eve.

Eq. (2) but with $\mu - \delta = \mu_1 \neq \mu_2 = \mu + \delta$, one obtains

$$\begin{aligned}
 E_o(t) &\propto [J_1(\mu_2) \cos(\Omega t) + iJ_1(\mu_1) \sin(\Omega t) + \sin(\Delta_2) + i \sin(\Delta_1)] E_i(t) \\
 &\approx \frac{1}{2} [(\mu + \delta) \cos(\Omega t) + i(\mu - \delta) \sin(\Omega t) + \Delta_2 + i\Delta_1] E_i(t) \\
 &= \frac{\mu}{2} e^{i(\omega_0 + \Omega)t} + \frac{\delta}{2} e^{i(\omega_0 - \Omega)t} + \Delta e^{i\omega_0 t}
 \end{aligned} \tag{3}$$

on expanding the Bessel functions, with Δ_j denoting small deviations in the DC biases on the MZMs and $\Delta = \Delta_2 + i\Delta_1$ (by invoking $\sin(\Delta_j) \approx \Delta_j$). Figure 1(b) illustrates a power spectrum that may represent the optical field in Eq. (3). The two sidebands, namely, the desired pilot tone and suppressed pilot tone, are located symmetrically around the suppressed beat signal.

Leakage during state preparation

Coherent detection of the quantum data signal in CVQKD systems is performed by Bob, who now generally employs a locally generated ‘real’ LO instead of using the ‘transmitted’ LO from Alice. The sharing of phase reference across Alice and Bob is then done by so-called reference pulses (for pulsed systems) or pilot tones (for continuous-wave systems) [20–24, 27]. We focus on the latter type, where a broadband signal is frequency multiplexed to the pilot tone, and then attenuated to yield the quantum data signal with a comparably bright pilot.

Figure 2 shows various spectra measured with a RF heterodyne detector in our CVQKD setup. We measure the detector electronic noise (dashed-black trace) when both the signal laser and LO are off, while with the signal laser off but LO on, we obtain vacuum noise (dotted-blue trace). With both light sources on and with the IQ modulator operating in OSSB-CS mode due to the DC bias control; see Fig. 1(a), we observe the suppressed carrier / beat signal in the heterodyne spectra. On applying RF modulation, we obtain the modulated signal (solid-red trace) spectra that shows the two main sidebands on the left to the beat signal.

In normal operation, we use a low pass filter (LPF) with cutoff around 200 MHz to limit Bob’s detection bandwidth, as all relevant frequency components needed for carrier and phase recovery are present within this bandwidth [20]. The LPF is conspicuous by its absence in Fig. 2(b): the suppressed pilot tone (SP) is fairly distinct in the spectra here. While the suppressed quantum band (SQB) signal may seem buried in the vacuum noise, it carries correlations with the signal

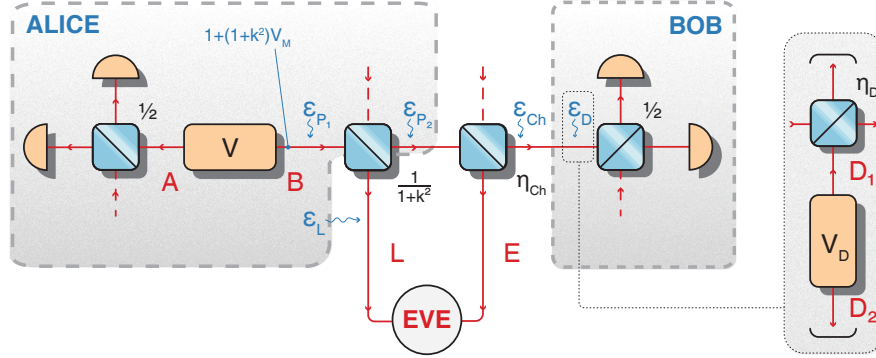


Fig. 3. Purification scheme used for security analysis. EPR source V radiates states with quadrature variance $1 + (1 + k^2)V_M$ in each of modes A and B . We model the modulation leakage as a linear interaction of the signal (B) and leakage (L) modes on a beamsplitter with transmittance $1/(1 + k^2)$. The signal is exposed to losses η_{Ch} and excess noise with variance ε_{Ch} in the untrusted channel. Eve obtains the information about the transmitted key from the output of the leakage mode (L) and from an auxiliary channel mode (E). Detection efficiency and trusted noise are modeled as a coupling with ratio η_D of the signal mode entering Bob and mode D_1 of an entangled state with variance $V_D = 1 + \varepsilon_D/(1 - \eta_D)$, where ε_D is the variance of added detection noise. Possible infusion points of trusted preparation noise $\varepsilon_{P_1, P_2, L}$ are also shown. Trusted preparation noise is also modeled as a result of unbalanced coupling between the signal and an EPR source with appropriate variance.

in the desired quantum band (DQB) and can also be used for decoding the information by anyone having access to that sideband, albeit with some penalty.

Note that such a leakage does not affect the security of intradyne or phase-diverse CVQKD systems [10, 21, 24, 27] because Bob effectively measures both sidebands. However, even in such systems, the vulnerability can be present in case higher-order sidebands, produced, for example, due to a large modulation depth, lie outside the detection bandwidth of Bob. This may indeed happen in pulsed CVQKD transmitters that actually implement polar modulation [12].

Attack model

Modulation leakage in the coherent-state protocol can be considered as a Trojan-horse attack [28], where the vacuum state injected by Eve receives a fraction of the signal modulation. Such an attack is equivalent to the setup without the side channel leakage, but with the altered values of higher signal modulation $V'_M = (k^2 + 1)V_M$, and lower transmittance of the quantum channel $\eta' = \eta/(k^2 + 1)$, where $k^2 = V_{ML}/V_M$ is the ratio between variances of the leakage mode modulation and the signal (with $k \geq 0$), and the input of the leakage mode is assumed to be vacuum. The covariance matrix describing the effective two-mode state is [28]:

$$\gamma_{AB} = \begin{pmatrix} [1 + (k^2 + 1)V_M]\mathbf{1} & \sqrt{\eta_{Ch}V_M[2 + (k^2 + 1)V_M]}\mathbf{P}_3 \\ \sqrt{\eta_{Ch}V_M[2 + (k^2 + 1)V_M]}\mathbf{P}_3 & [1 + \eta_{Ch}V_M + \varepsilon_{Ch}]\mathbf{1} \end{pmatrix}, \quad (4)$$

where $\mathbf{1}$ is a 2×2 identity matrix, $\mathbf{P}_3 = \text{diag}[1, 0, 0, -1]$ is the Pauli matrix, and loss η_{Ch} and excess noise with variance ε_{Ch} characterize the untrusted channel.

Figure 3 shows the overall purification scheme for the attack model, with the entire state in 4 trusted modes A, B, D_1 and D_2 , and Eve's modes E and L . The signal is subjected to trusted loss

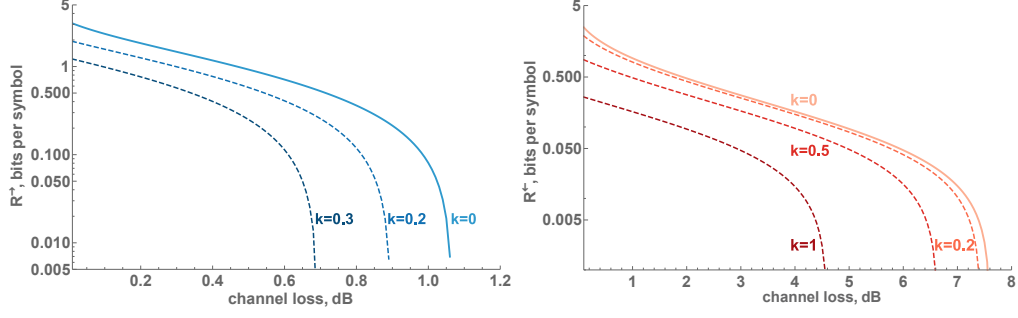


Fig. 4. Lower bound on the secure key fraction (in bits per symbol) versus the channel loss (dB) for DR (left) and RR (right). Solid lines show the expected security in the absence of leakage, dashed lines show the influence of the modulation leakage with $k = 0.2$ (-7.0 dB), 0.3 (-5.2 dB) for DR, and $k = 0.2$ (-7.0 dB), 0.5 (-3.0 dB), 1 (0.0 dB) for RR. Reconciliation efficiency $\beta = 0.96$, modulation variance V_M is optimized, assumed untrusted excess noise at the channel output $\varepsilon_{Ch} = 0.02$ SNU.

η_D and trusted noise ε_D stemming from the receiver, that are purified by an Einstein-Podolsky-Rosen (EPR) source radiating entangled states with variance $V_D = 1 + \varepsilon_D/(1 - \eta_D)$ in modes $D_{1,2}$. Likewise, potential trusted preparation noise ε_i ($i = P_1, P_2, L$) can be purified using a two-mode squeezed-vacuum source with variance $V_i = 1 + \varepsilon_i/(1 - \eta_i)$ coupled to the signal on a strongly unbalanced beamsplitter $\eta_i \rightarrow 1$. Such noise can be applied either to the signal and leaked along with the modulation (ε_{P_1}), or to the signal only (ε_{P_2}). In practice, Eve's measurement of the leakage mode may be susceptible to limited detection efficiency and detection noise, limiting the channel advantage for Eve. We adopt a pessimistic approach and assume that during the experiment Eve could retrieve the leaked information with perfect efficiency, and purify and eliminate the noise at her side. Nevertheless, we discuss the influence of all possible types of noise [29], including ε_L associated to the leakage mode L , on the security in Sec. 4.

Since Eve is assumed to hold a purification of the state shared between the trusted parties, one can use the equivalence between entropies of the state in Eve's mode and states in Alice and Bob modes [30]. Hence a four-mode covariance matrix $\gamma_{ABD_{1,2}}$ is sufficient to evaluate the Holevo bound on the information accessible to Eve:

$$\chi_E^{\text{DR}} = S(ABD_{1,2}) - S(BD_{1,2}|A), \quad \chi_E^{\text{RR}} = S(ABD_{1,2}) - S(AD_{1,2}|B), \quad (5)$$

where $S(ABD_{1,2})$, $S(AD_{1,2}|B)$ and $S(BD_{1,2}|A)$ are the (conditional) Von Neumann entropies that are calculated based on the symplectic eigenvalues of respective covariance matrices $\gamma_{ABD_{1,2}}$, $\gamma_{AD_{1,2}|B}$ and $\gamma_{BD_{1,2}|A}$. The secret key fraction, in bits/symbol, for direct (DR, \rightarrow) and reverse (RR, \leftarrow) reconciliation is given by Ref. [31]:

$$R^{\rightarrow(\leftarrow)} = \beta I'_{AB} - \chi_E^{\text{DR(RR)}}, \quad (6)$$

where $\beta \in [0, 1]$ is the efficiency of the reconciliation algorithm, and I'_{AB} is the mutual information² modified according to the scheme depicted in Fig. 3. For further details of the security estimation see Ref. [32].

Figure 4 shows the resulting lower bounds of the secure key fraction of Eq. (6) as a function of the channel loss. As expected, CVQKD protocols adopting DR are very sensitive to modulation leakage and are not able to establish a secure key when the leakage ratio reaches $k = 1$ [18]. Protocols with RR are less susceptible in comparison, however, with a diminished range of

²In the absence of trusted noise, $I_{AB} = I_{AB}^x + I_{AB}^p = \log_2 [(1 + \eta_{Ch} V_M)/(2 + \varepsilon_{Ch})]$ for heterodyne detection.

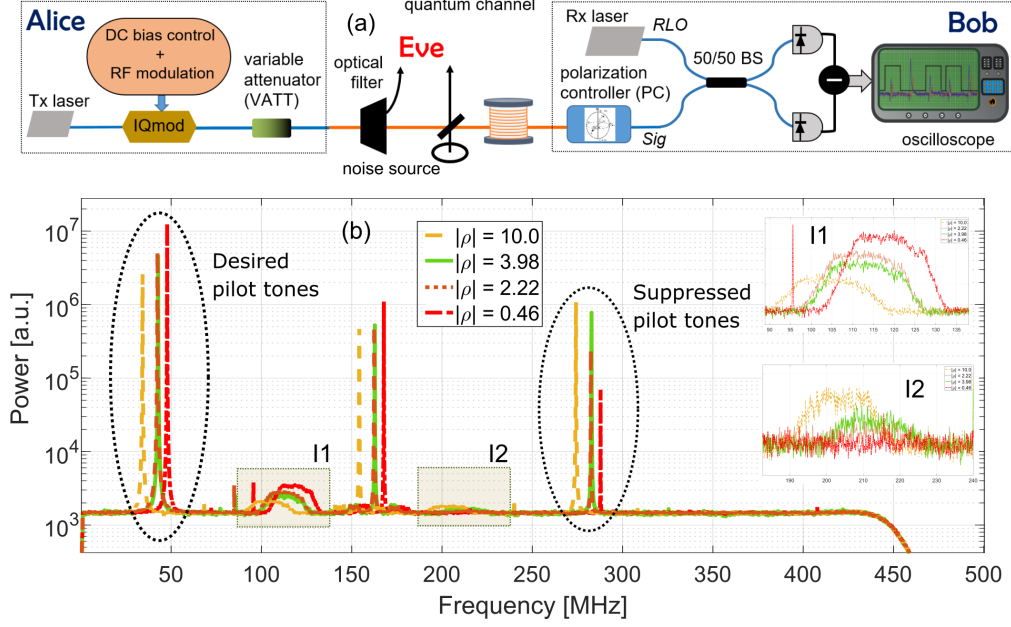


Fig. 5. Schematic of the experiment exposing the leakage vulnerability and measured heterodyne output spectra at varying degrees of sideband suppression. (a) Alice and Bob perform regular QKD measurements while Eve launches the attack illustrated in Fig. 3 from the quantum channel. (b) Both the suppressed pilot and quantum data clearly become more apparent with the departure of the scaling ρ from 0 dB. The insets I1 and I2 show the zoomed desired and suppressed quantum data bands, respectively.

channel loss for secure operation [18, 28]. For typical sideband suppression (> 20 dB) in bulk modulators, the performance impact is rather small. However, we note that if not taken properly into account, the leakage results in a wrong evaluation of the lower bound on secure key fraction, and can lead to security breach at large channel loss.

3. Experiment and Eve's attack strategy

Figure 5(a) shows a simplified scheme of the prepare-and-measure CVQKD setup used for the experiment. We use a commercial off-the-shelf IQ modulator in the transmitter and a home-made broadband balanced detector in the receiver. The output of the transmitter (Tx) laser is modulated using RF waveforms prepared using an arbitrary waveform generator (not shown in the figure). The DC biases to the IQ modulator (IQmod) are controlled using a commercial automatic bias controller to obtain OSSB-CS. The modulated output is attenuated so that the quantum data band contains a few photons when it travels over the quantum channel to Bob.

Using a manual polarization controller, we optimize the received signal's polarization for RF heterodyne detection with a real LO, generated by the receiver (Rx) laser. An oscilloscope samples and acquires the balanced detector output. The acquired data is used to reconstruct Alice's data using various digital signal processing methods, in particular, a machine learning framework based on Bayesian inference, for highly accurate phase estimation and compensation [20].

Since information is (also) encoded in the suppressed sidebands, Eve can use an optical filter, such as an optical add-drop multiplexer (OADM) as exhibited in Fig. 1(a), to divert a part of the spectrum to herself, while transmitting the rest to Bob. If Eve intercepts the SQB (shaded region I2 in Fig. 1(b)) and if Alice and Bob do not take this into account, then the security of the final

key can be compromised.

In the experiment, we connected Alice and Bob without any channel, i.e., in a back-to-back (B2B) configuration. From the acquired data, we processed the desired and suppressed quantum data bands (see Fig. 2(b)) *independently* of each other. The sharing of phase reference, i.e., phase corrections to the quantum data, can be performed using either the desired or the suppressed pilot tone. resulting in the following possible measurement strategies for Eve:

- SQB-SP: Suppressed quantum band processed using suppressed pilot tone, and
- SQB-DP: Suppressed quantum band processed using desired pilot tone,

while Bob’s measurement involves processing of the desired quantum band using the desired pilot tone (DQB-DP). Eve’s second strategy can be justified on the basis that DP is a classical signal, and therefore, Eve can manipulate – intercept, utilize, prepare afresh and re-send – it without any eventual penalty.

To highlight the vulnerability, we performed regular CVQKD measurements while varying the amount of sideband suppression by scaling the two RF output voltage levels that drive the IQ modulator with respect to each other; see Fig. 1(a). Eve is assumed to access the relevant parts of the spectrum using a perfect OADM, as illustrated in Fig. 5(a). The RF scaling factor, given by $\rho = 10 \log \frac{\max(V_{RF1}(t))}{\max(V_{RF2}(t))}$, is expressed in dB. We processed the acquired data from the heterodyne detector on a frame-to-frame basis, with each frame consisting of 10^7 samples from the oscilloscope. We acquired 20 frames per value of ρ for statistics.

Figure 5(b) shows the spectra from modulated frames acquired at four different values of ρ . The averaged frequency response obtained from the power spectra of the measured vacuum noise (see the dotted-blue trace in Fig. 2(b) for example), was inverted to create a ‘whitening’ filter. Applying this filter to the acquired data frames results in the flat response from near DC to > 400 MHz. To process the signal of interest, we performed carrier recovery with the help of a machine learning framework that employs an Unscented Kalman Filter (UKF) [20].

4. Results and Discussion

Figure 6(i) shows the total excess noise $\varepsilon_{Ch} + \varepsilon_D$ versus the RF scaling factor ρ for the 3 different data processing strategies mentioned before. Here, negative [positive] ρ values correspond to varying the peak-to-peak voltage of the applied waveform on arm 1 [arm 2] while keeping the peak-to-peak voltage on arm 2 [arm 1] constant; see Fig. 1(a). For poor sideband suppression ($|\rho| > 4$ dB), the average value of $\varepsilon_{Ch} < 0.06$ SNU, regardless of whichever pilot tone is used by the UKF for the purpose of phase recovery. For $|\rho| < 4$ dB, the suppressed pilot tone power is not large enough to provide enough SNR for a proper carrier recovery: consequently, the excess noise increases rapidly. Note that the green curve is above the orange curve because the modulation variance is higher for DQB compared to the SQB.

The pilot tone SNR values available to UKF are plotted in Fig. 6(ii); for $\text{SNR} < 10$, we could not obtain a sufficient number of processed frames with decent correlations for a reasonable estimation of the excess noise. Nonetheless, we note that in our experiment, we use much less powerful pilot tones compared to most other CVQKD setups [22–24]. So in general, there is a good likelihood that even the suppressed pilot tones provide a reasonable SNR for successful reconstruction. Finally, the slight asymmetry across the $|\rho| = 0$ dB vertical line stems from experimental imperfections, e.g., the mismatch in the electrical-to-optical response at the two MZMs in the IQ modulator.

Evaluating Bob’s (DQB-DP) and Eve’s (SQB-DP) data, we obtained a map between ρ and the modulation variance $V_M(\rho)$ and the leakage parameter $k(\rho)$. These two parameters are depicted in Fig. 6(iii) and (iv), respectively, and along with the upper bound estimates of $\varepsilon_{Ch}(\rho)$ and $\eta_{Ch}(\rho)$, are used to construct the covariance matrix $\gamma_{ABD_{1,2}}(\rho)$ and assess the lower bound

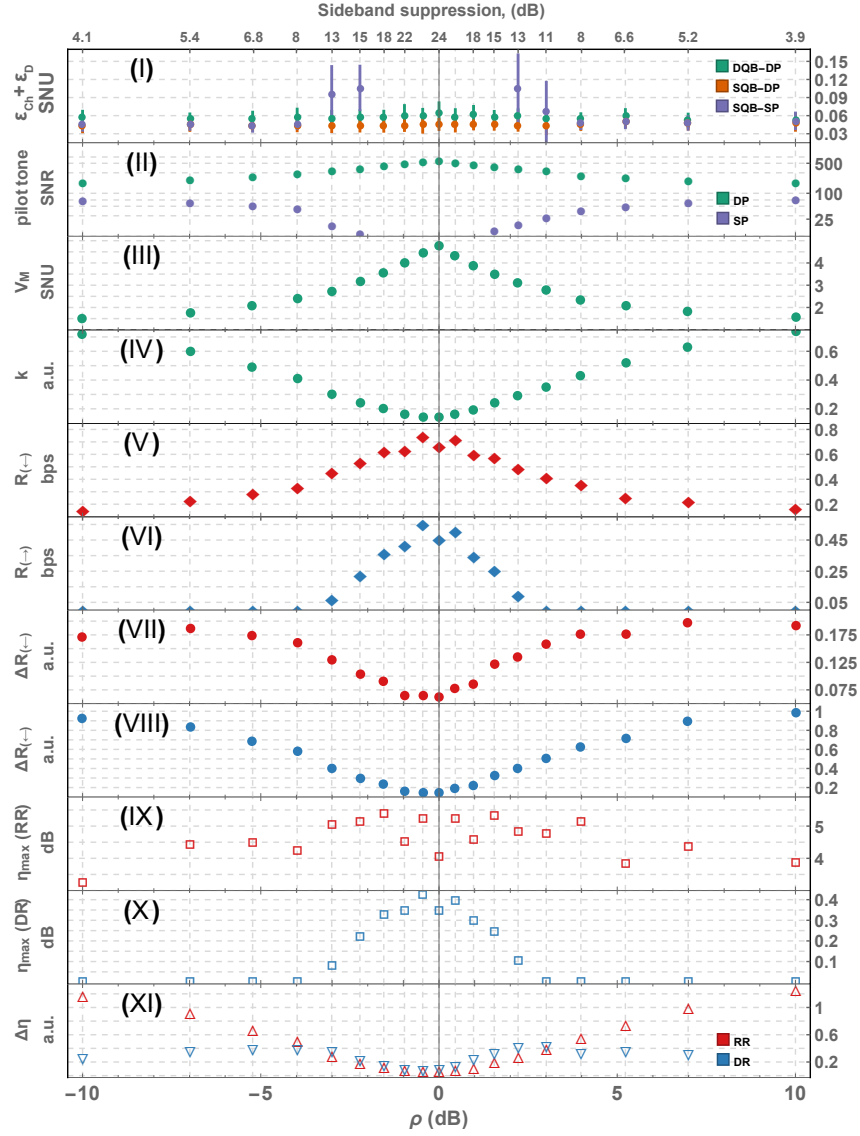


Fig. 6. Values of the estimated parameters (i-iv) and security analysis results (v-xi) as a function of the RF scaling ρ (bottom X axis). The corresponding sideband suppression values, estimated as the ratio of desired to suppressed pilot tone powers, are presented on the top X axis. From top to bottom: (i) the estimated total excess noise in shot noise units (SNU) from the processing of the SQB and DQB; (ii) signal-to-noise ratio (SNR) of desired and suppressed pilot tones; (iii) modulation variance V_M obtained from DQB; and (iv) leakage parameter k . The security analysis provides a lower bound on the key fraction in bits per symbol (bps) with RR (v) and DR (vi); difference of secure key fraction ΔR without leakage and with side channel leakage $k \neq 0$ for RR (vii) and DR (viii) techniques; maximal tolerable additional channel loss η_{max} in dB for RR and DR (ix) and (x) respectively; (xi) difference between maximal tolerable additional channel loss provided trusted parties are ignorant about modulation leakage ($k = 0$) and if the leakage is taken into account $\Delta\eta$ for RR (red) and DR (blue) techniques.

on the key fraction in Eq. (6) subsequently. The secure key fractions in B2B configuration for RR (red) and DR (blue) obtained with a reconciliation efficiency $\beta = 96\%$ and finite-size effects for a block size of 10^7 [33] are shown in Fig. 6 (v) and (vi), respectively. Evidently, the best sideband suppression yields the highest values of signal modulation variance V_M and lowest amount of leakage k , which consequently translates into higher levels of achievable secret key. Note that k never reaches zero due to the experimental inability to completely eliminate the suppressed components. The protocol based on DR is as expected very sensitive to the modulation leakage [18] and cannot deliver a secret key with poor sideband suppression, i.e. $|\rho| > 3$ dB. The RR technique, on the other hand, can tolerate more leakage and can securely operate regardless of the sideband suppression, although with significantly reduced key fraction.

The sensitivity of the CVQKD system to leakage is also highlighted in Fig. 6(vii) and (viii), where Eve's information advantage, i.e., the difference $\Delta R = R(k=0) - R(k \neq 0)$ between the secret key fractions, is shown for RR and DR, respectively. One way to interpret this would be, if Alice and Bob are ignorant of the side channel leakage they would be generating a key at rate ΔR higher than what is actually secure.

As the main sources of loss and noise are taken into account, we assess the maximal tolerable additional loss $\eta_{max}^{(\rightarrow, \leftarrow)}$ of the untrusted channel, i.e., the total loss is given by $\eta_{Ch}\eta_{max}^{(\rightarrow, \leftarrow)}$. The results are shown in Fig. 6(ix) for RR and (x) for DR techniques. For RR $\eta_{max}^{(\leftarrow)}$ is largely influenced by the noise encountered by Bob and Eve; see Fig. 6(i), while for DR, this additional loss is again determined by the amount of information leakage k . By ignoring the leakage, trusted parties might assume secure operation with up to $\eta_{max}^{(\rightarrow, \leftarrow)}(k=0)$ of additional channel loss, however the actual maximal loss, as shown in Fig. 6(ix) and (x), is lower. This is highlighted in Fig. 6(xi). Here $\Delta\eta = \eta_{max}^{(\rightarrow, \leftarrow)}(k=0) - \eta_{max}^{(\rightarrow, \leftarrow)}(k \neq 0)$ shows the regime where ignorant Alice and Bob would assume secure key distribution, while in fact the RR (red) or DR (blue) based CVQKD protocol is not secure anymore.

A possible approach to improve the secure key length under modulation leakage involves injection of trusted noise to the reference side [29, 34]. In our experiment, preparation noise was not characterized and was thus attributed to the untrusted channel, whereas detection noise was accurately identified. Such trusted noise on either side can be controlled and optimized in order to improve or even recover the security of CVQKD protocol in a noisy untrusted channel. However, it is important to recognize and characterize the trusted noise and identify where it is referred to, as it can affect only the signal or both the signal and leaked modulation (see Fig. 3) and carry different repercussions for security.

We identify the conditions under which trusted noise can be used to improve the key rate and summarize the results in Table 1. Firstly, any trusted noise ε_L in the leakage mode L will

Trusted noise:	DR	RR
Signal & leakage ε_{P_1}	✓	✗
Signal only ε_{P_2}	✓	✗
Leakage ε_L	✓	✓
Detection ε_D	✗	✓

Table 1. Viability of positive influence of trusted noise on the security of the coherent-state CVQKD protocol with modulation leakage.

translate into improved secure key fraction. As the DR technique is more sensitive to leakage (compared to RR) it will also benefit more from the respective noise, especially for stronger

leakage. Secondly, the effect of trusted detection noise ε_D is not altered by the leakage mode, and can be defensively used during RR only [34]. Lastly, overall influence of preparation noise remains similar to conventional CVQKD operation without the leakage. For DR, any preparation noise (ε_{P_1} or ε_{P_2}) can be used to the advantage of Alice and Bob. Although, if the noise is leaked along with the signal (ε_{P_1}) it can also directly hinder the effect of the leakage. For RR, trusted preparation noise can actually be harmful, even though ε_{P_1} seemingly curtails the usefulness of that leakage to Eve.

5. Conclusion

Optical single sideband (OSSB) encoding is a well-known technique in classical optical communication. It also has the potential to revolutionize broadband continuous-variable quantum key distribution (CVQKD) protocols by offering very low excess noise performance. OSSB modulation requires the suppression of a sideband, which can readily be implemented using an optical in-phase and quadrature (IQ) modulator. However, the amount of suppression is limited in practice, and as we have shown here, this can lead to the modulation leakage vulnerability in CVQKD systems. We have also presented a theoretical framework that analyses the insecurity resulting from this vulnerability: While the reverse reconciliation strategy suffers a reduction of the secret key length that becomes significant at higher leakages, the direct reconciliation strategy cannot produce a secret key even at moderate leakages. As a countermeasure, we have shown that depending on the type of reconciliation adopted, the trusted parties performing the CVQKD protocol could use preparation or detection noise, which is not in control of the adversary, to reduce the severity of the leakage. Finally, we note that such a leakage is much more likely in (future) photonic integrated circuit based modulators compared to bulk modulators. With IQ modulators poised to become the workhorses of CVQKD systems, we therefore believe this study is timely and can help protecting future CVQKD implementations against this vulnerability.

Acknowledgements

We acknowledge financial support from European Union’s Horizon 2020 research and innovation programmes CiViQ (grant agreement no. 820466), OPENQKD (grant agreement no. 857156), and CSA Twinning NONGAUSS (grant agreement no. 951737). NJ, HMC, ULA, and TG acknowledge support from Innovation Fund Denmark (CryptQ project, grant agreement no. 0175-00018A) and the Danish National Research Foundation, Center for Macroscopic Quantum States (bigQ, DNRF142). ID and VCU acknowledge support from the project 19-23739S of the Czech Science Foundation. RF acknowledges support of Horizon 2020 Framework Programme (731473, project 8C20002 ShoQC).

References

1. R. Griffin and A. Carter, “Optical differential quadrature phase-shift key (odqpsk) for high capacity optical transmission,” in *Optical Fiber Communications Conference*, (Optical Society of America, 2002), p. WX6.
2. K. Kikuchi, “Coherent Optical Communications: Historical Perspectives and Future Directions,” in *Electrical Engineering*, M. Nakazawa, K. Kikuchi, and T. Miyazaki, eds. (Springer, Berlin, Heidelberg, 2010).
3. T. C. Ralph, “Continuous variable quantum cryptography,” *Phys. Rev. A* **61**, 010303 (1999).
4. F. Grosshans and P. Grangier, “Continuous variable quantum cryptography using coherent states,” *Phys. Rev. Lett.* **88**, 057902 (2002).
5. C. H. Bennett and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, (Bangalore, India, 1984), pp. 175–179.
6. 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**, 1301–1350 (2009).
7. E. Diamanti and A. Leverrier, “Distributing secret keys with quantum continuous variables: Principle, security and implementations,” *Entropy* **17**, 6072–6092 (2015).

8. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," *Adv. Opt. Photon.* **12**, 1012–1236 (2020).
9. H. Bachor and T. Ralph, *A Guide to Experiments in Quantum Optics* (Wiley, 2019).
10. A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, "No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light," *Phys. Rev. Lett.* **95**, 180503 (2005).
11. N. Jain, B. Stiller, I. Khan, D. Elser, C. Marquardt, and G. Leuchs, "Attacks on practical quantum key distribution systems (and how to prevent them)," *Contemp. Phys.* **57**, 366–387 (2016).
12. P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," *Phys. Rev. A* **86**, 1–9 (2012).
13. 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**, 1–7 (2013).
14. 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**, 1–6 (2013).
15. B. Stiller, I. Khan, N. Jain, P. Jouguet, S. Kunz-Jacques, E. Diamanti, C. Marquardt, and G. Leuchs, "Quantum hacking of continuous-variable quantum key distribution systems: Realtime Trojan-horse attacks," in *Conference on Lasers and Electro-Optics (CLEO)*, (2015), pp. 1–2.
16. H. Qin, R. Kumar, and R. Alléaume, "Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution," *Phys. Rev. A* **94**, 012325 (2016).
17. Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu, and H. Guo, "Polarization attack on continuous-variable quantum key distribution," *J. Phys. B: At. Mol. Opt. Phys.* **52** (2019).
18. I. Derkach, V. C. Usenko, and R. Filip, "Continuous-variable quantum key distribution with a leakage from state preparation," *Phys. Rev. A* **96**, 062309 (2017).
19. G. Smith, D. Novak, and Z. Ahmed, "Technique for optical SSB generation to overcome dispersion penalties in fibre-radio systems," *Electron. Lett.* **33**, 74 (1997).
20. H.-M. Chin, N. Jain, D. Zibar, U. L. Andersen, and T. Gehring, "Machine learning aided carrier recovery in continuous-variable quantum key distribution," *npj Quantum Inf.* **7**, 20 (2021).
21. Z. Qu, I. B. Djordjevic, and M. A. Neifeld, "RF-subcarrier-assisted four-state continuous-variable QKD based on coherent detection," *Opt. Lett.* **41**, 5507 (2016).
22. 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**, 1588–1591 (2017).
23. H. H. Brunner, L. C. Comandar, F. Karinou, S. Bettelli, D. Hillerkuss, F. Fung, D. Wang, S. Mikroulis, M. Kuschnerov, A. Poppe, C. Xie, and M. Peev, "Low-noise, low-complexity CV-QKD architecture," in *QCrypt 2017*, (Cambridge, 2017), pp. 2–4.
24. 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**, 193 (2019).
25. 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. on Sel. Top. Quantum Electron.* **21**, 1077–260X (2014).
26. M. Xue, S. Pan, and Y. Zhao, "Optical single-sideband modulation based on a dual-drive MZM and a 120° hybrid coupler," *J. Light. Technol.* **32**, 3317–3323 (2014).
27. D. B. S. Soh, C. Brif, P. J. Coles, N. Luetkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, "Self-referenced continuous-variable quantum key distribution protocol," *Phys. Rev. X* **5**, 1–15 (2015).
28. J. Pereira and S. Pirandola, "Hacking Alice's box in continuous-variable quantum key distribution," *Phys. Rev. A* **98**, 062319 (2018).
29. V. C. Usenko and R. Filip, "Feasibility of continuous-variable quantum key distribution with noisy coherent states," *Phys. Rev. A* **81**, 022318 (2010).
30. S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables," *Rev. Mod. Phys.* **77**, 513 (2005).
31. A. S. Holevo and R. F. Werner, "Evaluating capacities of bosonic gaussian channels," *Phys. Rev. A* **63**, 032312 (2001).
32. C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," *Rev. Mod. Phys.* **84**, 621 (2012).
33. A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Phys. Rev. A* **81**, 062343 (2010).
34. V. C. Usenko and R. Filip, "Trusted noise in continuous-variable quantum key distribution: A threat and a defense," *Entropy* **18** (2016).