UNIVERSITY of York

This is a repository copy of *Hacking Alice's box in continuous-variable quantum key distribution*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/139154/

Version: Accepted Version

Article:
Pereira, Jason and Pirandola, Stefano orcid.org/0000-0001-6165-5615 (2018) Hacking Alice's box in continuous-variable quantum key distribution. Physical Review A. 062319. ISSN 1094-1622

https://doi.org/10.1103/PhysRevA.98.062319

Reuse
Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown
If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Hacking Alice's box in continuous variable quantum key distribution

Jason Pereira, Stefano Pirandola
Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK

Security analyses of quantum cryptographic protocols typically rely on certain conditions; one such condition is that the sender (Alice) and receiver (Bob) have isolated devices inaccessible to third parties. If an eavesdropper (Eve) has a side-channel into one of the devices, then the key rate may be sensibly reduced. In this paper, we consider an attack on a coherent-state protocol, where Eve not only taps the main communication channel but also hacks Alice's device. This is done by introducing a Trojan horse mode with low mean number of photons $\bar{n}$ which is then modulated in a similar way to the signal state. First we show that this strategy can be reduced to an attack without side-channels but with higher loss and noise in the main channel. Then we show how the key rate rapidly deteriorates for increasing photons $\bar{n}$, being halved at long distances each time $\bar{n}+1$ doubles. Our work suggests that Alice's device should also be equipped with sensing systems that are able to detect and estimate the total number of incoming and outgoing photons.

I. INTRODUCTION

Quantum information science [1–3] is advancing at a rapid pace. The progress of quantum computing [4] threatens to make current, classical cryptography insecure. Quantum key distribution (QKD) [5–7] is a possible solution to this problem, offering provable information security based on physical principles. It is possible to design QKD protocols that ensure that any eavesdropper can hold only an arbitrarily small amount of information about the message sent. This holds true regardless of how advanced the eavesdropper's technology is.

Security proofs for QKD protocols have a few assumptions that must hold in order for them to be valid [8]. The two trusted parties (Alice and Bob) must have isolated devices, which are inaccessible to the eavesdropper (Eve). The devices should be fully characterised, so that an adversary cannot exploit device imperfections to acquire information about the key or to alter the trusted parties' estimations of the quantum channel properties. The trusted parties must also have an authenticated (but not secure) classical channel; an eavesdropper can listen in to classical communications along this channel, but cannot alter them. If we relax any of these conditions, the secure key rate for a protocol may change.

Current commercial implementations of discrete variable (DV) protocols, such as BB84 [9] with decoy states [10, 11], have been shown to be vulnerable to a variety of attacks that exploit device imperfections, such as "side-channels" that leak information from the trusted parties' devices to Eve [12]. These attacks include detector blinding attacks [13], time-shift attacks [14] and Trojan horse attacks [15].

A variety of attacks on continuous variable (CV) protocols have been proposed. In experimental realisations of QKD, the local oscillator (which is used by Bob to carry out his measurements) is often sent down the quantum channel; this introduces a vulnerability that an eavesdropper can exploit. Häseler et al. [16] demonstrated that Eve could disguise an intercept and resend attack by replacing the signal state and the local oscillator with squeezed states. The wavelength-dependence of beamsplitters in Bob's setup can be exploited to engineer his measurement outcomes [17, 18]. Altering the shape of the local oscillator pulse can allow an eavesdropper to change Bob's estimation of the shot-noise [19, 20]. Saturation attacks [21, 22], which push Bob's detectors out of the linear mode of operation, have also been proposed.

One way of avoiding attacks that exploit device imperfections is to use device-independent QKD [8, 23]. This is a family of protocols that do not require Alice's and Bob's devices to be trusted. Such protocols are immune from many side-channel attacks, but have significantly lower key rates than protocols that require trusted devices. Measurement-device independent (MDI) QKD protocols have been formulated for both the DV [24, 25] and the CV [26] cases, and have much higher key rates than fully device-independent protocols. MDI-QKD removes threats from the detector's point of view, but still assumes that the state-preparation devices are completely trusted. Therefore, MDI-QKD is also subject to the quantum hacking described in this paper.

Here we consider a Trojan horse attack, where Eve sends extra photons into Alice's device, in order to gain information about the states being sent through the main quantum channel without disturbing the signal state. This type of attack was first considered in depth by Vakhitov et al. [27]. Such an attack may be used in DV protocols [28], in order to distinguish decoy states from signal states or to gain information about Alice's basis choice.

Gisin et al. [29] described how reflectometry could be used by Eve to gain information about Alice's phase modulator settings and analytically calculated the information leakage in terms of the photon number of the state received by Eve after the side-channel. They assumed attenuation of the side-channel mode by Alice and showed that the information leakage is reduced if Alice can randomise the phase of the side-channel mode.

Lucamarini et al. [30] calculated the secret key rate for BB84, with and without decoy states, in the presence of a Trojan horse side-channel, in terms of the photon number of the state received by Eve. They then bounded the

incoming photon number in terms of the Laser Induced Damage Threshold (LIDT) of the optical fibre and the time for which Alice's device gate is open, assuming that the Trojan horse photons are sent in via the main channel, whilst the gate is open. Based on this constraint, they designed an architecture to passively limit the photon number of the received state, and hence the information leakage.

Tamaki et al. [31] found general analytical expressions for the information leakage of DV protocols due to Trojan horse attacks, in terms of the actions of the phase and intensity modulators. This allows the secret key rate of a general DV protocol in the presence of a Trojan horse side-channel to be calculated, as long as the phase and intensity modulators are well-characterised.

Here we assume a CV protocol based on the modulation of coherent states [32], so that the attack is against the modulator. The experimental viability of carrying out a Trojan horse attack on the commercial CV system SeQureNet has previously been considered [33].

More precisely we assume that Eve is both hacking Alice's device with $\bar{n}$ mean photons per run and tapping the main quantum channel between Alice and Bob, which can be assumed to be a thermal-loss channel. This joint eavesdropping strategy can be reduced to a side-channel-free attack but where the main quantum channel has higher loss and noise. In this way we can compute the secret key rate and how it varies in terms of the mean photons $\bar{n}$. In particular, we show that, at long distances, the key rate is halved each time $\bar{n}+1$ doubles. This means that inserting just a few hacking photons into Alice's setup can seriously endanger the security of the protocol. As a result of our analysis, we conclude that the presence of these extra photons should be actively monitored in any practical implementation of CV QKD.

II. RESULTS

A. General scenario

We consider two parties, Alice and Bob, who are trying to establish a secret key, with a third party, Eve, trying to gain information about the secret key. Alice initiates a coherent state protocol [32, 34]. This involves her displacing a vacuum state by a Gaussian-distributed random (two-dimensional) variable, α. In real implementations, this displacement is generally carried out by independently modulating the phase and the intensity, so that the overall displacement has a Gaussian distribution. She then sends the displaced vacuum state (called the signal state) to Bob, via a quantum channel. Bob then carries out a heterodyne measurement on the signal state, to obtain a value β. This process is repeated several times. Alice and Bob compare some of their values via a classical communication channel in order to establish the transmittance, η, and excess noise, ϵ, of the channel. Bob and Alice then establish a secret key based on their shared knowledge of Bob's values (this is called reverse reconciliation).

Whilst the signal states are in the main quantum channel, we allow Eve to enact any unitary operation upon them. We assume that Eve can listen in on all classical communication between Alice and Bob (but cannot alter it). She can then store all states involved in the operation (except for the signal state) in a quantum memory and carry out an optimal measurement on them after all quantum and classical communication has been completed, in order to gain information about Bob's values. Alice and Bob therefore assume that all of the noise and loss of the channel has been caused by Eve's unitary operations and try to bound the maximum knowledge that Eve could have obtained about Bob's values. As long as Alice has more information about Bob's values than Eve, it is possible for Alice and Bob to obtain a secret key.

If Eve is only able to access the main channel and is not able to access Alice or Bob's devices in any way, the optimal attack on the signal state for a given attenuation and noise is an entangling cloner [35]. The secret key rate for this case has been calculated [36]. Here we instead consider the case where Eve also has access to part of Alice's device via a side-channel. Eve can send a Trojan horse mode into Alice's device, which will be displaced by α in the same way as the signal state. This side-channel mode contains an average number of photons $\bar{n}$, and we assume that Alice is able to monitor these photons and estimate their number. This will not be the case for most current CV-QKD implementations, especially since certain potential Trojan horse side-channels may not have been identified yet, so additional quantum metrological tools must be placed inside Alices box in order for this assumption to be met. To represent Eve's Trojan horse mode, we assume it is part of a two-mode squeezed vacuum (TMSV) state [34] with squeezing r, so that $\bar{n} = \sinh^2 r$. This is an active attack when $\bar{n} > 0$ and it is a passive one when $\bar{n} = 0$, meaning that we just have a leakage mode from Alice's device.

Recently, a side-channel on CV-QKD based on leakage from a multimode modulator was considered by Derkach et al. [37], building on their previous work [38]. These works considered leakage modes prior to and after modulation of the signal state, for both the coherent state and the squeezed state protocols. However, these authors did not consider side-channels that allow Eve to send photons into Alice's device (non-zero values of $\bar{n}$). They also considered homodyne, rather than heterodyne, measurements by the receiver. In this paper, we will consider a more general scenario, where the hacking of Alice's device is active, therefore involving the use of two-mode squeezing, so that $\bar{n} > 0$ photons enter the device. We analyse the security when the side-channel mode is modulated by α, exactly as the signal mode is (we later generalise to the case where its modulation is $m\alpha$). See Fig. 1 for an overview of the situation.

To find the secret key rate in reverse reconciliation, we need to calculate the mutual information between Alice

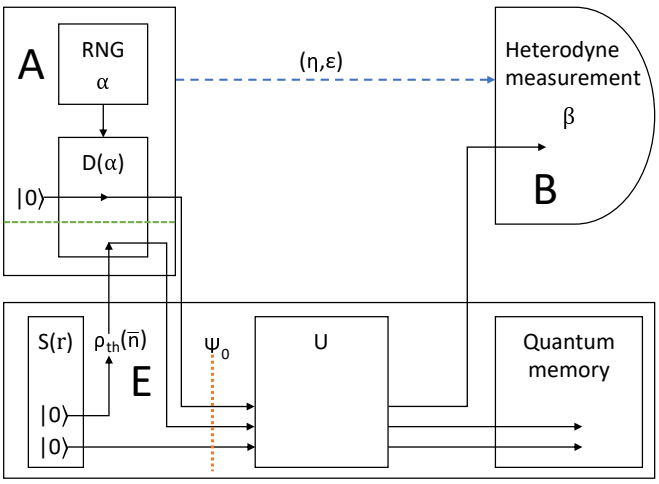

FIG. 1: The channel setup under consideration. A is Alice's device, B is Bob's device and E is Eve's device. The dashed green line marks the part of Alice's device that is accessible to Eve. Eve sends one mode of a TMSV state into Alice's device to be displaced by α in the same way as the signal state. Alice knows the average photon number, $\bar{n}$, of Eve's state. The (displaced) squeezed vacuum modes and the signal state form the state ψ_0. Eve enacts a unitary on this total state and any ancillary modes, then sends the signal state to Bob and stores the remaining modes in a quantum memory. Bob carries out a heterodyne measurement on the signal state, obtaining β. We find the key rate assuming that the main channel is a thermal channel, with transmittance η and excess noise ϵ, as represented by the blue dashed arrow.

and Bob $I(\alpha:\beta)$ and that between Eve and Bob. The latter is upper-bounded by the Holevo bound $I(E:\beta)$, which can be calculated as the reduction in entropy of Eve's output state when conditioned by Bob's value, β. We upper-bound Eve's knowledge of Bob's state by assuming that all noise and loss experienced by the signal state is due to Eve enacting unitary operations on the signal state and some ancillary modes, which are then stored in a quantum memory.

B. Reduction of the attack

If there are no side-channels, Eve's Holevo bound can be calculated by assuming that the signal state is entangled with some state held by Alice, and that α is the result of a heterodyne measurement on a TMSV state [35]. In the presence of our side-channel, the initial state held by Eve prior to her enacting the main channel is tripartite and composed of the signal mode and Eve's side-channel modes. Our first step must be to determine the first and second moments of this state ψ_0 (see Fig. 1). We label the initial first moment vector X_0 and the initial second moment (covariance) matrix V_0. For a fixed value of α, we have the conditional state $\psi_0|\alpha$ which is the tensor product of a coherent state $|\alpha\rangle\langle\alpha|$ and a TMSV state where one of the modes has also been displaced by α. The conditional moments are given by

$$X_0|\alpha = \begin{pmatrix}\alpha\\ \alpha\\ 0\end{pmatrix}, \quad V_0|\alpha = \begin{pmatrix}\mathbf{1} & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \cosh 2r\mathbf{1} & \sinh 2r\mathbb{Z}\\ \mathbf{0} & \sinh 2r\mathbb{Z} & \cosh 2r\mathbf{1}\end{pmatrix}, \quad (1)$$

where $\mathbf{1}$ is the one-mode identity matrix, $\mathbf{0}$ is the one-mode zero-matrix, and $\mathbb{Z}$ is the Pauli Z-matrix.

In order to find the elements of V_0, we add the expectation value of $X_0|\alpha \cdot X_0|\alpha^T$ to $V_0|\alpha$. Using $\langle\alpha\rangle = 0$ and $\langle\alpha^2\rangle = \mu$, we find

$$X_0 = \begin{pmatrix}0\\0\\0\end{pmatrix}, \; V_0 = \begin{pmatrix}(\mu+1)\mathbf{1} & \mu\mathbf{1} & \mathbf{0}\\ \mu\mathbf{1} & (\mu+\cosh 2r)\mathbf{1} & \sinh 2r\mathbb{Z}\\ \mathbf{0} & \sinh 2r\mathbb{Z} & \cosh 2r\mathbf{1}\end{pmatrix}. \quad (2)$$

From the covariance matrix V_0 we can compute the three symplectic eigenvalues [34]

$$v_1 = 1, \quad (3)$$

$$v_2 = \mu + \sqrt{1+\mu+\mu^2+\mu\cosh 2r}, \quad (4)$$

$$v_3 = -\mu + \sqrt{1+\mu+\mu^2+\mu\cosh 2r}, \quad (5)$$

and compute the entropy of the total state as [34] $S(\psi_0) = \sum_{k=1}^{3} g(v_k)$ where [40]

$$g(x) = \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2} \quad (6)$$

$$\overset{x\gg 1}{\to} \log_2\frac{ex}{2} + O(x^{-1}). \quad (7)$$

The fact that $v_1 = 1$ tells us that there is a symplectic transformation that reduces ψ_0 to a tensor product of a two-mode state and a vacuum state. We can build on this observation and reduce the number of modes. In fact, we may show the reduction to the setup in Fig. 2, which only involves the signal mode, modulated by $k_1\alpha$ (with $k_1 > 1$), and a single Trojan horse mode, modulated by $k_2\mathbb{Z}\alpha$ (with k_2 real). We can design a Gaussian unitary $\tilde{U}$ that converts the initial state ψ_0 from Fig. 1 into the initial state ψ_3 from Fig. 2. This unitary operation $\tilde{U}$ is the optical circuit shown in Fig. 3, where we have labelled the signal state as ψ_B, Eve's squeezed state that enters the side-channel as ψ_{E1} and Eve's idler state (the squeezed state that does not enter the side-channel) as ψ_{E2}.

To see how the circuit transforms the state, we examine it after each of the three optical components; we label the states after each component with the subscripts 1, 2 and 3. ψ_i has first moments vector X_i and covariance matrix V_i. The conditional state $\psi_i|\alpha$ is associated to $X_i|\alpha$ and $V_i|\alpha$. The symplectic matrix of the i^{th} component is S_i and it characterises the transformation of the state from ψ_{i-1} to ψ_i as follows: $V_i = S_i V_{i-1} S_i^T$ and $X_i = S_i X_{i-1}$.

The first component is a balanced beamsplitter, acting on the signal state and Eve's side-channel mode. This sets the quadratures for Eve's side-channel mode to 0. It

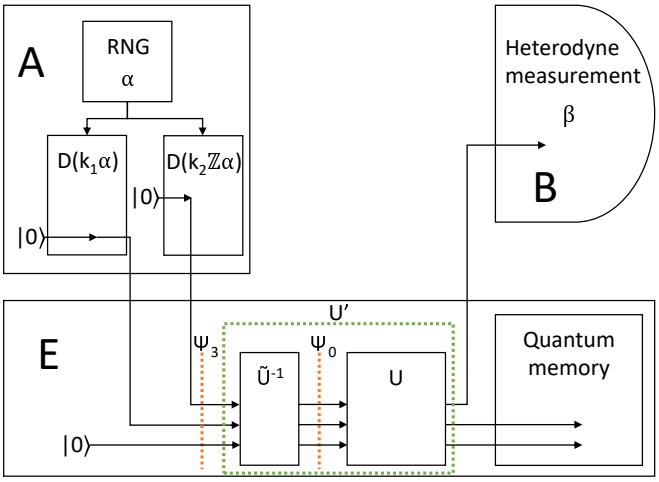

FIG. 2: An equivalent channel to the setup in Fig. 1. Alice draws a two-dimensional variable, α, from a Gaussian distribution then displaces one vacuum state by $k_1\alpha$ and another by $k_2\mathbb{Z}\alpha$. The first mode is sent through the main channel to Bob as the signal state and the second mode is leaked to Eve. The equivalence can be seen from the fact that Eve can get the initial state from Fig. 1, ψ_0, by enacting the unitary $\tilde{U}^{-1}$, and can then enact the same arbitrary unitary, U. We can regard this as Eve enacting a single combined unitary, U'.

has symplectic matrix

$$S_1 = \begin{pmatrix} \frac{1}{\sqrt{2}}\mathbf{1} & \frac{1}{\sqrt{2}}\mathbf{1} & \mathbf{0} \\ -\frac{1}{\sqrt{2}}\mathbf{1} & \frac{1}{\sqrt{2}}\mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{1} \end{pmatrix}, \tag{8}$$

and it results in the following moments for $\psi_1|\alpha$ and ψ_1

$$X_1|\alpha = \begin{pmatrix} \sqrt{2}\alpha \\ 0 \\ 0 \end{pmatrix}, \tag{9}$$

$$V_1|\alpha = \begin{pmatrix} \cosh^2 r\mathbf{1} & \sinh^2 r\mathbf{1} & \frac{\sinh 2r}{\sqrt{2}}\mathbb{Z} \\ \sinh^2 r\mathbf{1} & \cosh^2 r\mathbf{1} & \frac{\sinh 2r}{\sqrt{2}}\mathbb{Z} \\ \frac{\sinh 2r}{\sqrt{2}}\mathbb{Z} & \frac{\sinh 2r}{\sqrt{2}}\mathbb{Z} & \cosh 2r\mathbf{1} \end{pmatrix}, \tag{10}$$

$$V_1 = V_1|\alpha \oplus 2\mu \begin{pmatrix} \mathbf{1} & & \\ & \mathbf{0} & \\ & & \mathbf{0} \end{pmatrix}. \tag{11}$$

The second component is a two-mode squeezer, operating on Eve's modes such that one of them becomes a vacuum state. Its squeezing parameter is given by $r_2 = \log\left(\frac{\sqrt{2}\cosh r - \sinh r}{\sqrt{\cosh^2 r + 1}}\right)$, and it has symplectic matrix

$$S_2 = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \frac{\sqrt{2}\cosh r}{\sqrt{\cosh^2 r+1}}\mathbf{1} & -\frac{\sinh r}{\sqrt{\cosh^2 r+1}}\mathbb{Z} \\ \mathbf{0} & -\frac{\sinh r}{\sqrt{\cosh^2 r+1}}\mathbb{Z} & \frac{\sqrt{2}\cosh r}{\sqrt{\cosh^2 r+1}}\mathbf{1} \end{pmatrix}. \tag{12}$$

The moments of $\psi_2|\alpha$ and ψ_2 are given by

$$X_2|\alpha = \begin{pmatrix} \sqrt{2}\alpha \\ 0 \\ 0 \end{pmatrix}, \tag{13}$$

$$V_2|\alpha = \begin{pmatrix} \cosh^2 r\mathbf{1} & \mathbf{0} & \sqrt{\cosh^4 r - 1}\mathbb{Z} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ \sqrt{\cosh^4 r - 1}\mathbb{Z} & \mathbf{0} & \cosh^2 r\mathbf{1} \end{pmatrix}, \tag{14}$$

$$V_2 = V_2|\alpha \oplus 2\mu \begin{pmatrix} \mathbf{1} & & \\ & \mathbf{0} & \\ & & \mathbf{0} \end{pmatrix}. \tag{15}$$

Note that one of the modes has become a vacuum state. Henceforth, we neglect this mode and implicitly enact the identity operation on it. We now see that, for fixed α, the system is a displaced TMSV state. The third component undoes the squeezing, leaving us with two displaced vacuum states. Its squeezing parameter is given by $r_3 = -\operatorname{arcsinh}\left(\frac{\sinh r}{\sqrt{2}}\right)$ and it has symplectic matrix

$$S_3 = \begin{pmatrix} \frac{\sqrt{\cosh^2 r+1}}{\sqrt{2}}\mathbf{1} & -\frac{\sinh r}{\sqrt{2}}\mathbb{Z} \\ -\frac{\sinh r}{\sqrt{2}}\mathbb{Z} & \frac{\sqrt{\cosh^2 r+1}}{\sqrt{2}}\mathbf{1} \end{pmatrix}. \tag{16}$$

The moments of $\psi_3|\alpha$ and ψ_3 are

$$X_3|\alpha = \begin{pmatrix} k_1\alpha \\ k_2\mathbb{Z}\alpha \end{pmatrix}, \; V_3|\alpha = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}, \tag{17}$$

$$V_3 = \begin{pmatrix} (1+\mu(\cosh^2 r + 1))\mathbf{1} & -\mu\sqrt{\cosh^4 r - 1}\mathbb{Z} \\ -\mu\sqrt{\cosh^4 r - 1}\mathbb{Z} & (1+\mu\sinh^2 r)\mathbf{1} \end{pmatrix}, \tag{18}$$

where we have set

$$k_1 := \sqrt{\cosh^2 r + 1}, \; k_2 := -\sinh r. \tag{19}$$

This conclude the proof of equivalence between the setups in Fig. 1 and Fig. 2.

We note that the two components (quadratures) of α are uncorrelated with each other and have the same variance. Let us also assume that the two quadratures of Bob's outcome (β) are also uncorrelated with each other and have the same variance. This is certainly the case in the presence of a thermal-loss channel, characterised by a transmittance η and an excess noise ϵ, which is the most typical scenario in QKD. Next, we show that the setup in Fig. 2 has the same key rate as the setup in Fig. 4, in which the signal mode is modulated by $k_1\alpha$ and the side-channel mode is modulated by $k_2\alpha$ (rather than by $k_2\mathbb{Z}\alpha$). Note that in Fig. 4, we have also imposed that the general unitary results in a thermal-loss channel.

Since we assume that the main channel does not mix the quadratures, we can treat the two quadratures of α, which we denote as α_x and α_p, as independent variables that have been sent through the channel and measured to give the independent variables β_x and β_p respectively. Let I^x_{AB} (I^p_{AB}) denote the mutual information

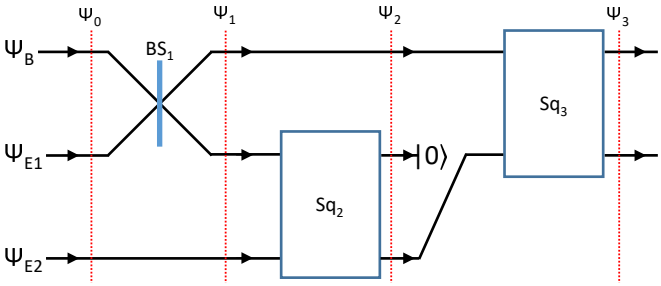

FIG. 3: A circuit that converts the initial (pre-main channel) state from the setup in Fig. 1 into the initial state from the setup in Fig. 2. This shows that the two channel setups have the same key rate, since Eve can enact any unitary operation and hence is able to convert one into the other. We label this entire circuit $\tilde{U}$. Eve can also enact the inverse, $\tilde{U}^{-1}$. ψ_B denotes the signal state, ψ_{E1} denotes Eve's squeezed state that enters the side-channel and ψ_{E2} denotes Eve's idler state. BS_1 is a balanced beamsplitter and Sq_2 and Sq_3 are two-mode squeezers. BS_1 moves all of the displacement onto the first mode, such that Eve's states are no longer displaced, Sq_2 unsqueezes Eve's states such that one of the modes becomes a pure vacuum state and Sq_3 unsqueezes the signal state and Eve's remaining mode such that they become pure displaced vacuum states.

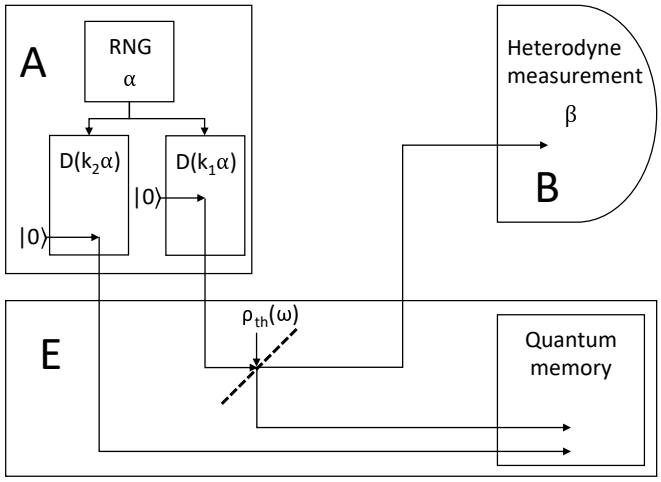

FIG. 4: An alternative channel setup that must give the same secret key rate as the setup in Fig. 2 assuming the presence of a thermal-loss channel. The difference between the two setups is that in Fig. 2, the x-quadrature of Eve's side-channel state is modulated by $k_2\alpha_x$ and the p-quadrature is modulated by $-k_2\alpha_p$; in this figure,the x-quadrature is still modulated by $k_2\alpha_x$ but the p-quadrature is modulated by $k_2\alpha_p$. Since the two quadratures encode independent variables and since the x-quadrature is not affected by the change, the mutual informations arising from the measurement of the x-quadrature, I^x_{AB} and I^x_{EB}, must be the same in each setup and hence the key rates must be the same. We assume that Eve beamsplits the signal state with some thermal state with variance ω. This specific representation of Eve's unitary is unique up to isometries on her output ancillas. In other words, if we fix the channel to be thermal-loss, then its dilation into a beamsplitter with an environmental thermal state is fixed up to unitaries acting over Eve's entire output Hilbert space [39].

between Alice and Bob arising from the measurement of the x-quadrature (p-quadrature) and let I^x_{EB} (I^p_{EB}) denote the maximum mutual information between Eve and Bob arising from the measurement of the x-quadrature (p-quadrature). Since the x and p quadratures of α and β are independent and identically distributed, I_{AB} and I_{EB} are double I^x_{AB} and I^x_{EB} respectively.

Let I'_{AB}, I'^x_{AB}, I'_{EB} and I'^x_{EB} be the counterparts of I_{AB}, I^x_{AB}, I_{EB} and I^x_{EB} respectively for the setup in Fig. 4. It is again true that I'_{AB} and I'_{EB} are double I'^x_{AB} and I'^x_{EB} respectively. Further, since the quadratures are independent and the x-quadratures of Eve's states are not affected by the change in setup (the only difference is that the p-quadrature of Eve's side-channel mode is modulated by $k_2\alpha_p$ rather than by $-k_2\alpha_p$), I^x_{AB} must be the same as I'^x_{AB}. This means that I_{AB} is the same as I'_{AB} and I_{EB} is the same as I'_{EB}. Note that this holds for all channels (not just thermal channels) that do not mix the quadratures and so the $\mathbb{Z}$ matrix in Fig. 2 can be neglected for any such channel.

Hence, the setup in Fig. 4 must give the same key rate as the setup in Fig. 2, and therefore the setup in Fig. 1. The setup in Fig. 4 is equivalent to a main channel setup with a higher initial modulation and a lower effective transmittance. The equivalent main channel attack is shown in Fig. 5. The signal state is modulated by $k\alpha$, where

$$k = \sqrt{k_1^2 + k_2^2} = \sqrt{2}\cosh r = \sqrt{2(\bar{n}+1)}, \tag{20}$$

and hence the modulation amplitude is $k^2\mu$. k is a function of $\bar{n}$, which characterises the side-channel. We note that k_1 and k_2 are functions only of $\bar{n}$. By choosing an appropriate parameter for the beamsplitter in Fig. 5, Eve can get the initial state of Fig. 4. We then effect a thermal channel by beamsplitting with the thermal state with parameter ω. We can reduce both operations to a single beamsplitter operation with some other thermal state ω' (see Fig. 6).

This allows us to calculate the key rate in the same way as a main channel attack but with a higher "effective modulation amplitude", μ', and a lower "effective transmittance", η'. These effective parameters (the channel parameters that the trusted parties would calculate for the setup in Fig. 5) are related to the measured values of μ and η by

$$\mu' = k^2\mu, \quad \eta' = \frac{\eta}{k^2}. \tag{21}$$

The effective transmittance accounts for both beamsplitters and is the transmittance that we would observe if, instead of a setup with a signal state modulated by μ and a side-channel (as seen in Fig. 1), we had a setup with a signal state modulated by μ' and no side-channel, with the same measured values of β (as seen in Fig. 5). This was found by multiplying the transmissions of the two beamsplitters in Fig. 5.

It is helpful to clarify the definition of the excess noise, ϵ. To do so, we introduce the random variable n: this is

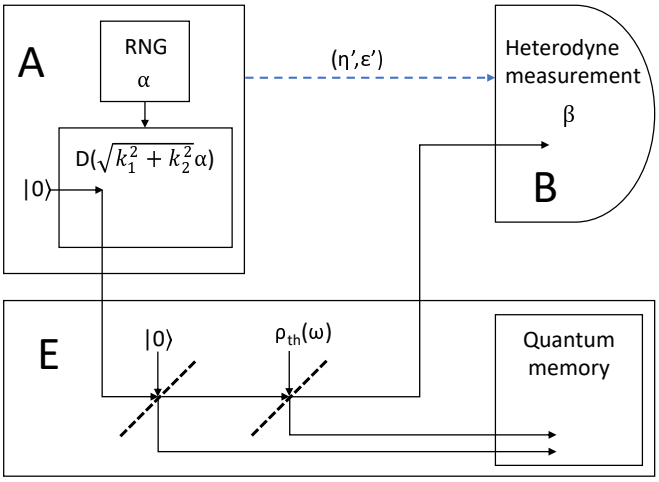

FIG. 5: This is a setup without a side-channel that must give the same secret key rate as the setup with the side-channel. The variance of Alice's variable in this setup is higher than the actual variance of α, and the channel transmittance for this setup is lower than the observed channel transmittance, η. The channel for this setup can be regarded as a thermal channel with parameters η' and ϵ' (represented by the blue, dashed arrow).

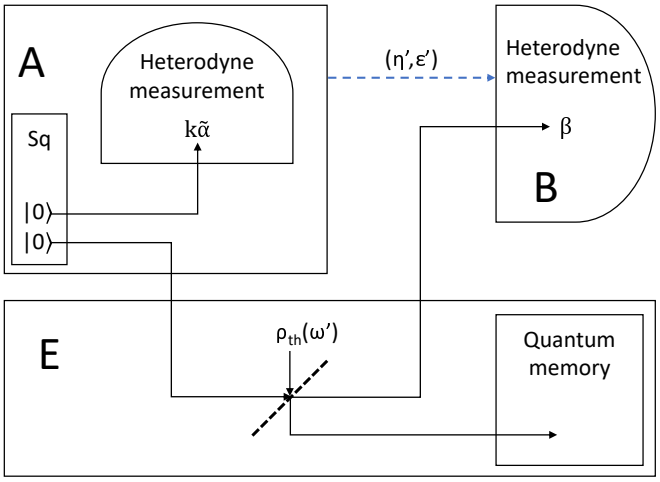

FIG. 6: This is the entanglement-based representation of the attack in Fig. 5. Alice heterodynes one half of a TMSV state to get the value $k\tilde{\alpha}$, which linearly corresponds to $k\alpha$ (the displacement of the signal state). The signal state enters the channel and is subject to some thermal noise due to beamsplitting with one mode of an entangling cloner (the thermal state ω'). It is then heterodyned by Bob, to obtain β. The resultant state of Alice, Bob and Eve is pure. The channel between Alice and Bob is a thermal channel, characterised by η' and ϵ'; this is represented by the blue, dashed arrow.

the total relative input noise of β around α, including the vacuum noise. We can describe β in terms of n as $\beta = \eta(\alpha + n)$. Here n is characterised by its second moment $\langle n^2 \rangle = 1 + (1-\eta)/\eta + \epsilon$. We now find the effective excess noise, ϵ' (as would be observed for the setup in Fig. 5), using the fact that we have the same measured β values in all representations. β can be expressed in terms of effective parameters as $\beta = \eta'(k\alpha + n')$, where the second moment of n' is now given by $\langle n'^2 \rangle = 1 + (1-\eta')/\eta' + \epsilon'$. We then substitute in the definition of η' and compare the expressions for β, and so solve for ϵ', i.e.,

$$\epsilon' = \frac{\eta}{\eta'}\epsilon = k^2\epsilon. \tag{22}$$

C. Computation of the key rate

To calculate the secret key rate for a main channel attack with a modulation amplitude of μ', a transmittance of η' and an excess noise of ϵ', we can use an entanglement-based representation (rather than a prepare and measure representation) [35]. This representation is shown in Fig. 6, and is valid as long as $\mu > 0$.

Alice heterodynes one mode of a TMSV state, obtaining the value $k\tilde{\alpha}$ (and hence also the value of α) and preparing the state $\rho(k\alpha)$. She then sends the prepared signal state through the channel to Bob, who heterodynes it to obtain β. In the channel, the signal state is beamsplit with the thermal state $\rho_{th}(\omega)$. The total state shared by Alice, Bob and Eve, which we denote ρ_{ABE}, is pure since Eve holds the purification of the channel. This means that the entropy of Eve's state, ρ_E, is equal to the entropy of the combined state of Alice and Bob, ρ_{AB}. The combined state of Alice and Eve conditioned by some value of β, $\rho_{AE}|\beta$, is also pure, so the entropy of Eve's state conditioned by β, $\rho_E|\beta$, is equal to the entropy of Alice's state conditioned by β, $\rho_A|\beta$.

The covariance matrix of ρ_{AB} is

$$V_{AB} = \begin{pmatrix} (\mu'+1)\mathbf{1} & \sqrt{\eta'\mu'(\mu'+2)}\mathbb{Z} \\ \sqrt{\eta'\mu'(\mu'+2)}\mathbb{Z} & (\eta'(\mu'+\epsilon')+1)\mathbf{1} \end{pmatrix}, \tag{23}$$

the covariance matrices of the conditional states $\rho_A|\beta$ and $\rho_B|\alpha$ are given by

$$V_A|\beta = \left(\mu' + 1 - \frac{\eta'\mu'(\mu'+2)}{\eta'(\mu'+\epsilon')+2}\right)\mathbf{1}, \tag{24}$$

$$V_B|\alpha = (\eta'\epsilon' + 1)\mathbf{1}. \tag{25}$$

We can calculate the symplectic eigenvalues of V_{AB} using the formula in [34]. The expressions for these eigenvalues can be simplified by taking the asymptotic limit in μ (the limit as $\mu \to \infty$). In this limit, $\mu' \to \infty$ and all other parameters stay the same. We assume that $\eta' \leq 1$, since realistically, Eve will not enact a main channel that causes gain rather than loss. We denote the two symplectic eigenvalues of V_{AB} in this limit as $v^{\infty}_{AB,1}$ and $v^{\infty}_{AB,2}$ and denote the symplectic eigenvalue of $V_A|\beta$ in

this limit as $v^{\infty}_{A|\beta}$. We find these to be:

$$v^{\infty}_{AB,1} = 1 + \frac{\epsilon'\eta'}{1-\eta'}, \tag{26}$$

$$v^{\infty}_{AB,2} = \mu'(1-\eta'), \tag{27}$$

$$v^{\infty}_{A|\beta} = \frac{2}{\eta'} + \epsilon' - 1. \tag{28}$$

We calculate the mutual information between Alice and Bob, $I(\alpha:\beta)$, as the reduction in (classical) entropy of β when conditioned with α. The asymptotic limit of this mutual information is equal to

$$I(\alpha:\beta)^{\infty} = H(V_\beta + 1) - H(V_\beta|\alpha + 1) \tag{29}$$

$$= \log_2 \frac{\eta'\mu'}{\eta'\epsilon' + 2}, \tag{30}$$

where H is the Shannon entropy [43] and V_β ($V_\beta|\alpha$) is the variance of Bob's outcome β (conditional outcome $\beta|\alpha$). We then calculate the Holevo bound between Eve and Bob in the asymptotic limit. We find:

$$I(E:\beta)^{\infty} = \log_2 \frac{e\, v^{\infty}_{AB,2}}{2} + S_{\text{const}}, \tag{31}$$

where

$$S_{\text{const}} = g(v^{\infty}_{AB,1}) - g(v^{\infty}_{A|\beta}) \tag{32}$$

is the entropy contribution that does not scale with μ. The first term of this expression comes from the asymptotic form of $g(v^{\infty}_{AB,2})$, as per Eq. (7). The asymptotic secret key rate is given by the difference

$$K^{\infty}(\bar{n},\eta,\epsilon) = I(\alpha:\beta)^{\infty} - I(E:\beta)^{\infty} \tag{33}$$

$$= \log_2 \frac{2\eta'}{e(1-\eta')(\eta'\epsilon'+2)} - S_{\text{const}}. \tag{34}$$

The extra information gained by Eve due to the side-channel is the difference between the key rate with the side-channel and the key rate without. In general, the asymptotic key rate decreases as the effective transmission decreases (either due to an increase in the average photon number of the side-channel mode or due to increased line loss) and as the channel noise increases. This is shown in the plots in Figs. 7 and 8.

The asymptotic secret key rate K^{∞} takes a particularly simple form if the channel does not add any noise (a pure-loss channel). In fact, it becomes

$$K^{\infty}_{\text{lossy}} = -\frac{\log_2(1-\eta')}{\eta'} - \log_2 e \tag{35}$$

$$= \frac{2(\bar{n}+1)}{\eta} \log_2\left[1 - \frac{\eta}{2(\bar{n}+1)}\right] - \log_2 e. \tag{36}$$

The rate $K^{\infty}_{\text{lossy}}$ is always positive and plotted in Fig. 7 for various mean photon numbers $\bar{n}$, where it is also compared with the ultimate point-to-point rate or PLOB bound $-\log_2(1-\eta)$ [41]. Each time $\bar{n}+1$ doubles (e.g. when $\bar{n}$ goes from 0 to 1, from 1 to 3 or from 3 to 7), the key rate $K^{\infty}_{\text{lossy}}$ decreases by approximately 3 dB.

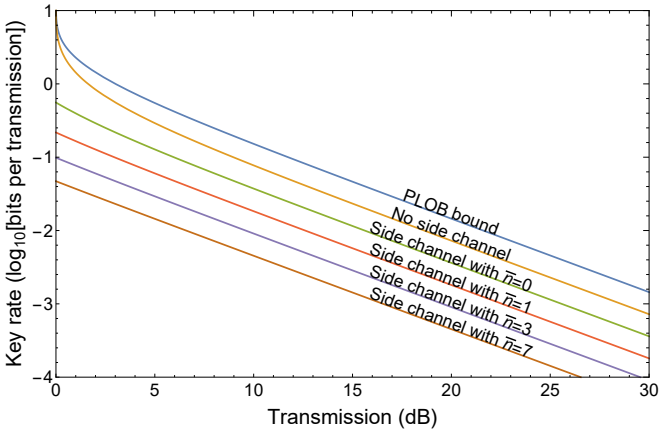

FIG. 7: Plots of the secret key rate (in logarithmic scale) versus channel transmission η of the main quantum channel, in the absence of excess noise (lossy channel rate). The top curve is the PLOB bound [41], which is the secret key capacity of the lossy channel, i.e., the maximum key rate achievable over this channel by any point-to-point QKD protocol in the absence of side-channels [42]. We then show the ideal rate of the coherent state protocol [32] with no side channels. Lower curves refer to the coherent state protocol in the presence of a side-channel with an increasing number of photons $\bar{n}$, ranging from the leakage mode case ($\bar{n}=0$) to more active hacking ($\bar{n}=1$, 3, 7). As we can see, the key rate is always positive (for any value of $\bar{n}$), but it quickly declines as $\bar{n}$ increases.

In the low transmission regime (i.e., long distances), it is known that the PLOB bound becomes roughly linear in η, and is approximately equal to $\eta/\ln 2 \simeq 1.44\eta$ bits per transmission. It is also known that, without side-channels, the coherent state protocol has a long-distance ideal rate of about $\eta/(2\ln 2) \simeq 0.72\eta$ bits per transmission, which is half the PLOB bound. The linearity also holds when we include the side channels. In fact, for low η, we find that the key rate of Eq. (36) becomes

$$K^{\infty}_{\text{lossy}} \simeq \frac{\eta}{4(\bar{n}+1)\ln 2} \simeq \frac{0.36}{\bar{n}+1}\eta\ . \tag{37}$$

Note that with the leakage mode ($\bar{n}=0$), this rate is half that of the coherent state protocol without side-channels. This rate keeps halving each time $(\bar{n}+1)$ doubles; this can also be seen in the constant decrease in intercept between each of the plots in Fig. 7.

We then calculate the threshold excess noise, $\epsilon_{\max}$, for a given channel transmission, η, and side-channel parameter, $\bar{n}$. This is the value of the excess noise up to which secret key distribution is possible. The threshold condition $\epsilon_{\max} = \epsilon(\eta,\bar{n})$ is given by solving $K^{\infty}(k,\eta,\epsilon) = 0$. In Fig. 8, we show the security threshold of the coherent state protocol [32] without side-channels and, then, in two cases with side-channel modes ($\bar{n}=0$ and 1). The shaded regions show the regions in which secret key distribution is possible for a given side-channel.

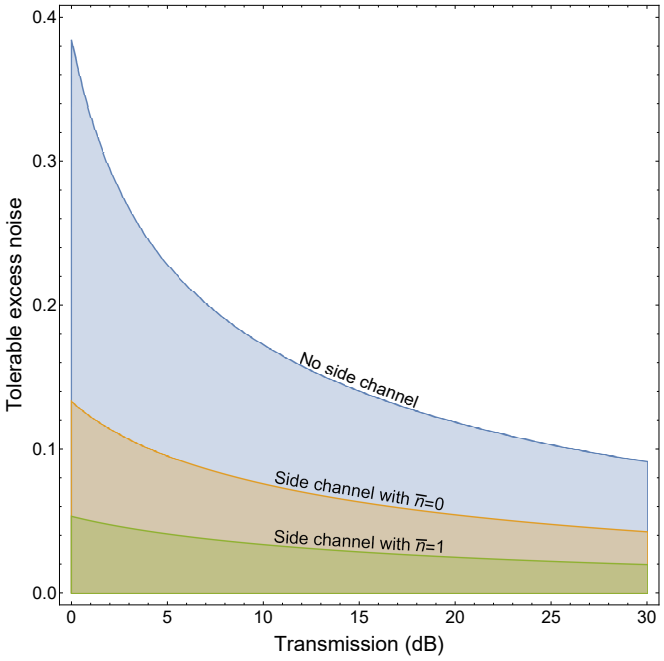

FIG. 8: Security thresholds in terms of maximally-tolerable excess noise versus channel transmission (in decibels). The shaded regions are the regions in which secret key distribution is possible for a given side-channel. The boundaries of the regions show the values of the excess noise at which secret key distribution becomes impossible for a given transmission and side-channel. Adding the leakage mode side-channel significantly decreases the tolerable excess noise for a given transmission, and increasing the average photon number $\bar{n}$ of the side-channel further decreases it.

The leakage mode case ($\bar{n} = 0$) has a significantly lower security threshold than the case with no side-channel, and increasing the average photon number further decreases the threshold, for fixed transmission. For instance, for channel transmission of 20 dB, the presence of leakage ($\bar{n} = 0$) decreases the tolerable excess noise by $\simeq 0.06$ (from about 0.12). For active hacking with $\bar{n} = 1$ photon, we have a further decrease of $\simeq 0.03$. In other words, a side-channel with $\bar{n} = 1$ gives a $\simeq 75\%$ decrease in tolerable excess noise at this distance. If $\bar{n}$ is increased, the attack becomes even more powerful. It is then important for Alice to be able to accurately measure $\bar{n}$, by characterising her devices as accurately as possible.

D. Generalisation of the side-channel

We can also consider a simple extension, in which Eve's side-channel mode is modulated by $m\alpha$, whilst Alice's signal state is modulated by α. m is a multiplicative factor on the displacement of the Trojan state; $m = 1$ gives the case that has already been considered. This setup is shown in Fig. 9. Without loss of generality, we assume that $m > 0$, since Eve can always apply a phase shift of π to her modes. Similarly to the original $m = 1$ case,

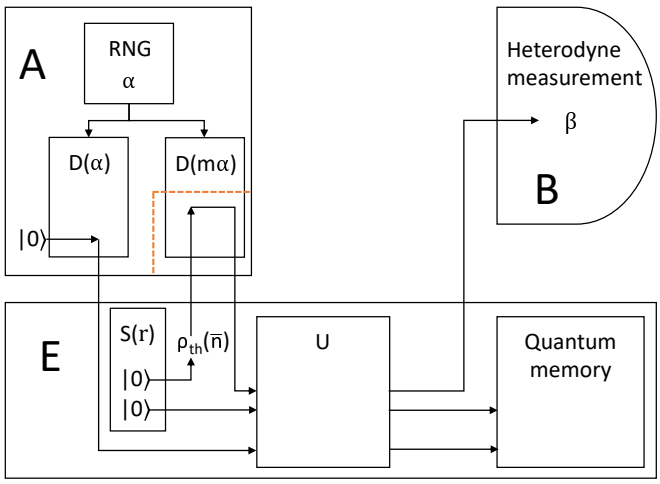

FIG. 9: This is an extension of the original setup (Fig. 1), in which both the average number of photons entering Alice's device, $\bar{n}$, and the modulation amplitude of the side-channel mode, m, are monitored. Unlike in the original case, m does not have to equal 1, and can take any real value. The dashed red line marks the part of Alice's device that is accessible to Eve. The key rate for this setup can be calculated similarly to the key rate for the original setup; the only difference is in the expression for the k parameter, which affects the "effective loss", the "effective excess noise" and "effective modulation amplitude". See text for more explanation.

we can show that this attack is equivalent to a standard attack against the main channel but with an "effective modulation amplitude", an "effective excess noise" and an "effective loss". As we show in the appendix, the original and effective parameters are related by the same Eqs. (21) and (22), but where k becomes the following function of both $\bar{n}$ and m [44]

$$k(\bar{n}, m) = \sqrt{m^2(2\bar{n} + 1) + 1}. \tag{38}$$

By monitoring both $\bar{n}$ and m, Alice can therefore fully quantify the effect of any single mode side-channel of this type. Alice can find $\bar{n}$ by monitoring the average photon number entering her device. There are a number of ways in which she could find m. For instance, she could monitor the total average outgoing photon number of her device across all modes.

III. CONCLUSIONS AND FURTHER DISCUSSIONS

In this work we have considered the effects of hacking Alice's box in one-way CV QKD, namely the coherent state protocol of Ref. [32], which is hacked while being implemented over a thermal-loss quantum communication channel. We have assumed that a Trojan horse side-channel mode is introduced in Alice's device and is modulated in the same way as the signal state. Under this condition, we have found how quickly the key rate of the

original protocol is deteriorated by increasing the mean number of photons $\bar{n}$ inserted in the device. Even the presence of a leakage mode ($\bar{n} = 0$) is able to halve the rate. Then, each time the value of $(\bar{n} + 1)$ doubles, the long-distance key rate is further halved.

Then we have also considered a direct generalisation of the basic side-channel attack where the Trojan horse mode is modulated at a different amplitude ($m\alpha$) than the signal state. If this modulation is inefficient ($m < 1$), then the attack is weaker than the basic one. However, if $m > 1$, then the attack becomes more deleterious. In order to deal with this situation, Alice should be able to estimate not only the mean number of extra photons $\bar{n}$ entering the device, but also the mean number of extra photons leaving the device, so that she can also evaluate m. Therefore, it seems that quantum metrological tools [45–51] are necessary inside Alice's box, unless Eve's hacking is mitigated by other means which suitably modify the original setup and protocol.

If the modulator can be surrounded by a passive attenuator, such that any photons not entering or leaving via the main channel are highly attenuated, the effects of any Trojan horse photons not entering via the main channel can be greatly mitigated. The attenuator can be modelled as a beamsplitting operation with a vacuum mode. The effects on the information gained by Eve are twofold: the first quadrature of her side-channel mode is scaled down by the attenuation and the correlations between Eve's Trojan horse mode and her idler mode are reduced. The conditional state $\psi_{E1,E2}|\alpha$ received by Eve after the side-channel (conditioned on Alice's value), will be a TMSV state with a lower photon number than the incoming state and classical Gaussian noise added to the idler state. If we denote the covariance matrix of this state $V_{E1,E2}|\alpha$,

$$V_{E1,E2}|\alpha = \begin{pmatrix} \bar{n'}\mathbf{1} & \sqrt{\bar{n'}-1}\mathbb{Z} \\ \sqrt{\bar{n'}-1}\mathbb{Z} & \bar{n}\mathbf{1} \end{pmatrix} \tag{39}$$

$$= \begin{pmatrix} \bar{n'}\mathbf{1} & \sqrt{\bar{n'}-1}\mathbb{Z} \\ \sqrt{\bar{n'}-1}\mathbb{Z} & \bar{n'}\mathbf{1} \end{pmatrix} \oplus a \begin{pmatrix} \mathbf{0} & \\ & \mathbf{1} \end{pmatrix}, \tag{40}$$

where $\bar{n}$ is the initial photon number of the TMSV state (prior to the side-channel), $\bar{n'}$ is some positive, real number less than $\bar{n}$ and $a = (\bar{n} - \bar{n'})$. If the Trojan horse mode is modulated by $m\alpha$, we can say that the first quadrature of this mode after the attenuator is $m'\alpha$, where m' is some positive, real number less than m. Then, the key rate is lower-bounded by the key rate calculated before, but with $\bar{n}$ and m replaced by $\bar{n'}$ and m' respectively. More specifically, the expression for k in Eq. (38) becomes

$$k(\bar{n'}, m') = \sqrt{m'^2(2\bar{n'}+1)+1} \tag{41}$$

$$= \sqrt{Tm^2(2T^2\bar{n'}+1)+1}, \tag{42}$$

where T is the transmission of the attenuator. This expression rapidly approaches unity as T decreases. Here we have assumed that the Trojan horse state passes through the attenuator twice: once prior to modulation and once after modulation. Hence, we have set $m' = \sqrt{T}m$ and $\bar{n'} = T^2\bar{n}$.

The expression for the maximum secret key rate in this case is an upper bound: whilst the addition of Gaussian noise to Eve's idler mode cannot increase the Holevo bound of her mutual information with Bob's values, it is not immediately obvious whether it in fact decreases it. It is therefore not obvious whether this upper bound is tight, or whether the power of the side-channel would be even further reduced by the attenuation; this is a question that is open to further study.

Without upper-bounding the incoming photon number, the addition of an attenuator does not provide provable security by itself, since we do not know the initial values of m and $\bar{n}$, hence quantum metrological tools are still required. It may be possible to find an upper-bound on the incoming photon number for a given device, using physical considerations, such as the point at which damage to the modulator from the incoming photons would become obvious to Alice.

In order to limit the effects of a Trojan horse mode introduced via the main channel, the passive architecture to limit Trojan horse attacks in the DV case, introduced in [30], could be implemented in the CV case. The incoming photon number is bounded using the LIDT of the optical fibre constituting the main quantum channel; the photon number threshold is dependent on the frequency of the incoming photons, since lower frequency photons are less energetic, however the frequency is bounded from below by an optical fibre loop and a filtering block, which select for frequencies. There is then an attenuator, which greatly reduces the photon number of any incoming state. In this case, the attenuation will not decrease the magnitude of modulation of the Trojan horse state compared to the signal state, as it does in the case in which the Trojan horse photons do not enter via the main channel. This is because the signal state will be attenuated in the same way as the Trojan horse state. The incoming photons sent by Eve would still be attenuated, leading to damping of the off-diagonal elements of $V_{E1,E2}|\alpha$. By suitably choosing the attenuation, bearing in mind the maximum photon number of Eve's Trojan horse state, Alice could decrease the correlations between Eve's Trojan horse mode and her idler mode to an arbitrary degree, and hence could effectively reduce Eve's side-channel to a leakage mode ($\bar{n} = 0$).

Bounding the incoming photon number using the LIDT raises another issue, since we have assumed that modulation of the signal mode is unbounded, and hence can be taken to infinity. Since the photon number of the signal state will also be limited by the LIDT, this is not entirely true. However, if the LIDT is sufficiently high, this should not greatly affect the secret key rate. Increasing the LIDT does not increase the photon number of Eve's outgoing side-channel mode as long as the attenuation is raised accordingly.

One further possible problem could occur if the attenuator itself is not properly characterised. If it re-radiates absorbed photons, or scatters light in such a way that it is accessible to Eve, the attenuator itself may provide a leakage side-channel. Alternatively, it may have a much higher transmission at certain frequencies, allowing Eve to send Trojan horse photons through without much attenuation.

Acknowledgments

This work was made possible via the EPSRC Quantum Communications Hub (Grant No. EP/M013472/1). The authors would like to thank Pieter Kok, Scott E. Vinay, Panagiotis Papanastasiou, Romain Alléaume, Marco Lucamarini, Rupesh Kumar, and Vladyslav Usenko, for comments and feedback.

[1] J. Watrous, *The theory of quantum information* (Cambridge University Press, Cambridge, 2018).
[2] M. Hayashi, *Quantum Information Theory: Mathematical Foundation* (Springer-Verlag Berlin Heidelberg, 2017).
[3] A. Holevo, *Quantum Systems, Channels, Information: A Mathematical Introduction* (De Gruyter, Berlin-Boston, 2012).
[4] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[5] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145-196 (2002).
[6] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, M. Peev, Rev. Mod. Phys. **81**, 1301 (2008).
[7] E. Diamanti and A. Leverrier, Entropy **17**, 6072-6092 (2015).
[8] S. Pironio, A. Acin, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).
[9] C. H. Bennett, and G. Brassard, Proc. IEEE International Conf. on Computers, Systems, and Signal Processing, Bangalore, pp. 175–179 (1984).
[10] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901(2003).
[11] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).
[12] V. Scarani and C. Kurtsiefer, Theor. Comput. Sci. **560**, 27 (2014).
[13] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photon. **4**, 686 (2010).
[14] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A **78**, 042333 (2008).
[15] N. Jain, E. Anisimova, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, New J. Phys. **16**, 123030 (2014).
[16] H. Häseler, T. Moroder, and N. Lütkenhaus, Phys. Rev. A **77**, 032303 (2008).
[17] J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **87**, 062329 (2013).
[18] X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, Phys. Rev. A **87**, 052309 (2013).
[19] P. Jouguet, S. Kunz-Jacques, and E. Diamanti, Phys. Rev. A **87**, 062313 (2013).
[20] J.-Z. Huang, S. Kunz-Jacques, P. Jouguet, C. Weedbrook, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, and Z.-F. Han, Phys. Rev. A **89**, 032304 (2014).
[21] H. Qin, R. Kumar, and R. Alléaume, Phys. Rev. A **94**, 012325 (2016).
[22] H. Qin, R. Kumar, V. Makarov, and R. Alléaume, Phys. Rev. A **98**, 012312 (2018).
[23] A. K. Ekert, Phys. Rev. Lett. **67**, 661–663 (1991).
[24] S. L. Braunstein, and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
[25] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
[26] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nat. Photon. **9**, 397 (2015).
[27] A. Vakhitov, V. Makarov, and D. R. Hjelme, J. Mod. Opt. **48**, 2023 (2001).
[28] S. E. Vinay and P. Kok, Phys. Rev. A **97**, 042335 (2018).
[29] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Phys. Rev. A **73**, 022320 (2006).
[30] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Phys. Rev. X **5**, 031030 (2015).
[31] K. Tamaki, M. Curty, and M. Lucamarini, New J. Phys. **18**, 065008 (2016).
[32] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[33] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquadt, and G. Leuchs, IEEE J Sel Top Quantum Electron. **21**, 168 (2014).
[34] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[35] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and Ph Grangier, Quantum Info. Comput. **3**, 535 (2003).
[36] V. C. Usenko and R. Filip, Entropy **18**, 20 (2016).
[37] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A **96**, 062309 (2017).
[38] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A **93**, 032309 (2016).
[39] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).
[40] F. Grosshans, Phys. Rev. Lett. **94**, 020504 (2005).
[41] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017). See also arXiv:1510.08863.
[42] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi, Quantum Sci. Technol. **3**, 035009 (2018).
[43] T. M. Cover, and J. A. Thomas, *Elements of Information Theory* (2nd edition, Wiley, 2006).
[44] Note that if $m = 1$, this reduces to the previous case. Note also that if $m = 0$, we do not have a side-channel and so $k = 1$, hence the "effective loss" is equal to the observed loss, as we would expect.
[45] S. L. Braunstein and C. M. Caves, Phys. Rev. Lett. **72**, 3439 (1994).

[46] S. L. Braunstein, C. M. Caves, and G. J. Milburn, Ann. Phys. **247**, 135-173 (1996).
[47] M. G. A. Paris, Int. J. Quant. Inf. **7**, 125-137 (2009).
[48] V. Giovannetti, S. Lloyd, and L. Maccone, Nature Photon. **5**, 222 (2011).
[49] D. Braun, G. Adesso, F. Benatti, R. Floreanini, U. Marzolino, M. W. Mitchell, and S. Pirandola, Rev. Mod. Phys. **90**, 035006 (2018).
[50] S. Pirandola, and C. Lupo, Phys. Rev. Lett. **118**, 100502 (2017); *ibidem* **119**, 129901 (2017).
[51] R. Laurenza, C. Lupo, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Quantum Meas. Quantum Metrol. **5**, 1–12 (2018).

APPENDIX A: CALCULATION OF THE K-VALUE FOR ANY M-VALUE

The steps to study the setup in Fig. 9 are very similar to those for the $m = 1$ case. By using a beamsplitter on modes 1 and 2 followed by two-mode squeezers on modes 2 and 3 and then on modes 1 and 3, we can show that the setup is equivalent to one in which the signal state is modulated by $k_1\alpha$ and a single pure side-channel mode is modulated by $k_2\mathbb{Z}\alpha$ (as in Fig. 2, but with different values for k_1 and k_2). We then again use the fact that this gives the same key rate as a setup in which the side-channel mode is modulated by $k_2\alpha$ instead of by $k_2\mathbb{Z}\alpha$, and hence that it gives the same key rate as one in which the signal state is modulated by $k = \sqrt{k_1^2 + k_2^2}$, with a beamsplitter in the main channel.

We label the initial covariance matrix of the total state as $V_0^{m\neq1}$, the initial covariance matrix for fixed α as $V_0^{m\neq1}|\alpha$ and the initial quadratures for fixed α as $X_0^{m\neq1}|\alpha$, and then use the subscripts 1, 2 and 3 to denote these objects after the beamsplitter, the first two-mode squeezer and the second two-mode squeezer respectively. The optical circuit is the same as in Fig. 3; only the parameters of the optical components are changed for the $m \neq 1$ case.

The first and second moments of the initial state are

$$X_0^{m\neq1}|\alpha = \begin{pmatrix} \alpha \\ m\alpha \\ 0 \end{pmatrix}, \tag{A1}$$

$$V_0^{m\neq1}|\alpha = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \cosh 2r\mathbf{1} & \sinh 2r\mathbb{Z} \\ \mathbf{0} & \sinh 2r\mathbb{Z} & \cosh 2r\mathbf{1} \end{pmatrix}, \tag{A2}$$

$$V_0^{m\neq1} = \begin{pmatrix} (\mu+1)\mathbf{1} & m\mu\mathbf{1} & \mathbf{0} \\ m\mu\mathbf{1} & (m^2\mu + \cosh 2r)\mathbf{1} & \sinh 2r\mathbb{Z} \\ \mathbf{0} & \sinh 2r\mathbb{Z} & \cosh 2r\mathbf{1} \end{pmatrix}. \tag{A3}$$

The first optical component is a beamsplitter that sets the quadratures of modes 2 and 3 to 0 (moves the entire displacement onto mode 1). This beamsplitter has angle

$$\theta_1^{m\neq1} = \arccos \frac{1}{\sqrt{m^2+1}}, \tag{A4}$$

and changes the first and second moments of the state to

$$X_1^{m\neq1}|\alpha = \begin{pmatrix} \sqrt{m^2+1}\alpha \\ 0 \\ 0 \end{pmatrix}, \tag{A5}$$

$$V_1^{m\neq1}|\alpha = \begin{pmatrix} \frac{m^2\cosh 2r+1}{m^2+1}\mathbf{1} & \frac{2m\sinh^2 r}{m^2+1}\mathbf{1} & my^{(1)}\mathbb{Z} \\ \frac{2m\sinh^2 r}{m^2+1}\mathbf{1} & \frac{m^2+\cosh 2r}{m^2+1}\mathbf{1} & y^{(1)}\mathbb{Z} \\ my^{(1)}\mathbb{Z} & y^{(1)}\mathbb{Z} & \cosh 2r\mathbf{1} \end{pmatrix}, \tag{A6}$$

$$V_1^{m\neq1} = V_1^{m\neq1}|\alpha \oplus (m^2+1)\mu \begin{pmatrix} \mathbf{1} & & \\ & \mathbf{0} & \\ & & \mathbf{0} \end{pmatrix}, \tag{A7}$$

where $y^{(1)} = (\sinh 2r)/\sqrt{m^2+1}$.

The next component purifies the second mode, reducing the state to a bipartite state. It acts on the second and third modes and has squeezing parameter $r_2^{m\neq1} = -\operatorname{arcsinh}\frac{\sqrt{2}\sinh r}{\sqrt{m^2\cosh 2r+m^2+2}}$. The first and second moments become

$$X_2^{m\neq1}|\alpha = \begin{pmatrix} \sqrt{m^2+1}\alpha \\ 0 \\ 0 \end{pmatrix}, \tag{A8}$$

$$V_2^{m\neq1}|\alpha = \begin{pmatrix} \frac{m^2\cosh 2r+1}{m^2+1}\mathbf{1} & \mathbf{0} & y^{(2)}\mathbb{Z} \\ \mathbf{0} & \mathbf{1} & \mathbf{0} \\ y^{(2)}\mathbb{Z} & \mathbf{0} & \frac{m^2\cosh 2r+1}{m^2+1}\mathbf{1} \end{pmatrix}, \tag{A9}$$

$$V_2^{m\neq1} = V_2^{m\neq1}|\alpha \oplus (m^2+1)\mu \begin{pmatrix} \mathbf{1} & & \\ & \mathbf{0} & \\ & & \mathbf{0} \end{pmatrix}, \tag{A10}$$

where

$$y^{(2)} = \frac{\sqrt{2}m\sinh r\sqrt{m^2\cosh 2r+m^2+2}}{m^2+1}. \tag{A11}$$

The final component unsqueezes the remaining two modes, such that the state for fixed α is a vacuum state. The squeezing parameter is $r_3^{m\neq1} = -\operatorname{arcsinh}\frac{m\sinh r}{\sqrt{m^2+1}}$. The first and second moments become

$$X_3^{m\neq1}|\alpha = \begin{pmatrix} \frac{\sqrt{m^2\cosh 2r+m^2+2}}{\sqrt{2}}\alpha \\ -m\sinh r\mathbb{Z}\alpha \\ 0 \end{pmatrix} = \begin{pmatrix} k_1^{m\neq1}\alpha \\ k_2^{m\neq1}\mathbb{Z}\alpha \\ 0 \end{pmatrix}, \tag{A12}$$

$$V_3^{m\neq1}|\alpha = \begin{pmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \mathbf{1} \end{pmatrix}, \quad V_3^{m\neq1} = \begin{pmatrix} x_+\mathbf{1} & y^{(3)}\mathbb{Z} \\ y^{(3)}\mathbb{Z} & x_-\mathbf{1} \end{pmatrix}, \tag{A13}$$

where

$$x_\pm = \frac{1}{2}(m^2\mu\cosh 2r \pm m^2\mu + 2), \tag{A14}$$

$$y^{(3)} = -\frac{m\mu\sinh r\sqrt{m^2\cosh 2r+m^2+2}}{\sqrt{2}}. \tag{A15}$$

Since we have shown that there is an optical circuit that reversibly converts the initial state of the setup in

Fig. 9 to the initial state of the setup in Fig. 2, the two setups must have the same secret key rate for the same thermal noise. As shown in the main text, this also means that the setup in Fig. 9 has the same secret key rate as the side-channel-free setup with an "effective modulation" of $\mu^{eff} = k^2\mu$, an "effective channel loss" of $\eta^{eff} = \frac{\eta}{k^2}$ and an "effective excess noise" of $\epsilon^{eff} = k^2\epsilon$, where

$$k = \sqrt{k_1^2 + k_2^2} \tag{A16}$$

$$= \sqrt{\frac{1}{2}(m^2 \cosh 2r + m^2 + 2) + m^2 \sinh^2 r} \tag{A17}$$

$$= \sqrt{m^2(2\bar{n} + 1) + 1}. \tag{A18}$$

This is the result given in the main text.