Noname manuscript No.
(will be inserted by the editor)

Teleportation-Based Continuous Variable Quantum Cryptography

F. S. Luiz · Gustavo Rigolin

Received: date / Accepted: date

Abstract We present a continuous variable (CV) quantum key distribution (QKD) scheme based on the CV quantum teleportation of coherent states that yields a raw secret key made up of discrete variables for both Alice and Bob. This protocol preserves the efficient detection schemes of current CV technology (no single-photon detection techniques) and, at the same time, has efficient error correction and privacy amplification schemes due to the binary modulation of the key. We show that for a certain type of incoherent attack it is secure for almost any value of the transmittance of the optical line used by Alice to share entangled two-mode squeezed states with Bob (no 3 dB or 50% loss limitation characteristic of beam splitting attacks). The present CVQKD protocol works deterministically (no postselection needed) with efficient direct reconciliation techniques (no reverse reconciliation) in order to generate a secure key and beyond the 50% loss case at the incoherent attack level.

1 Introduction

Currently, the only absolutely secure way through which two parties (Alice and Bob) can, at least theoretically, secretly share a random sequence of bits (key) is given by quantum cryptography, whose security is guaranteed by the validity of the laws of quantum mechanics [1]. This secret key is the most important ingredient in the implementation of classical cryptography protocols, such as the one-time pad, which are provably secure if the key is only known by Alice and Bob.

F. S. Luiz
Departamento de Física, Universidade Federal de São Carlos, São Carlos, SP 13565-905, Brazil

Gustavo Rigolin
Departamento de Física, Universidade Federal de São Carlos, São Carlos, SP 13565-905, Brazil
E-mail: rigolin@ufscar.br

The original QKD protocols are based on single photons ("discrete" states), requiring photon-counting techniques to their implementation [1,2]. However, single photon detectors are not as efficient and fast (short response time) as standard telecommunication PIN photodiodes used to detect bright light (many photons) [2]. In quantum mechanics these bright quantum states are described by the quadratures of a mode of the quantized electromagnetic field and are also known as CV states due to the continuum spectrum of the quadratures. In order to explore the efficient and fast measurement schemes for such states (homodyne or heterodyne detection), QKD protocols based on several types of CV states and strategies were proposed [3,4,5,6,7,8,9,10,11,12,13, 14,15,16,17]. They are all called CVQKD protocols [18] and are considered theoretically secure [19].

The quantum resources of the first CVQKD protocols [3,4], whose security was equivalent to discrete QKD protocols, were either single-mode squeezed states, sent from Alice to Bob, or two-mode entangled squeezed states shared between them. In these early schemes the secret key was encoded either in binary alphabets composed of two different states (discrete modulation) [3] or in states with real and imaginary quadratures [4] chosen from Gaussian distributions (continuous modulation)[1]. An important development of CVQKD appeared in [5], where it was shown that coherent states are equally secure to generate a secret key between Alice and Bob if one uses a Gaussian continuous modulation and if the transmission loss from Alice to Bob does not exceed 50%. Subsequently, in [6] it was shown that if Bob accepts only certain measurement outcomes (postselection) to generate the key, or if Alice and Bob employ reverse reconciliation techniques [7], they can surpass the 50% loss threshold. Also, by employing at the same time reverse reconciliation and postselection one gets the greatest secure key rates [10].

A reconciliation technique is an error correction scheme implemented at the end of the protocol by Alice and Bob, in which they execute a set of tasks in order to agree on a common sequence of bits. This process is called direct if Alice, who sends the quantum states, communicates classically with Bob, who then processes his data using a predetermined algorithm to agree with Alice's random sequence of bits. Reverse reconciliation is the opposite scenario, where Bob communicates with Alice, who now manipulates her data in order to share a common key with Bob. So far, there is no CVQKD protocol that is secure for any value of loss that uses only direct reconciliation and no postselection.

In this article we show a different way to do CVQKD that is secure against individual attacks for losses close to 100% without resorting to either reverse reconciliation or postselection, the standard solutions to make a CVQKD pro-

[1] A discrete variable QKD scheme is based on the use of qubits or qudits (finite dimensional Hilbert spaces) while a CVQKD scheme employs physical systems described by infinite dimensional Hilbert spaces (such as coherent and squeezed states). Note, however, that in CVQKD protocols the key can be modulated using either discrete or continuous alphabets/variables [18]. In the present protocol we use a discrete alphabet of coherent states to modulate the key and a two-mode squeezed state to teleport the coherent state from Alice to Bob. This is why we call our protocol a teleportation-based CVQKD scheme.

tocol work securely for losses greater than 50%. Since this protocol works deterministically (no postselection) and uses a discrete modulation for the key, it achieves fairly high key rates over long distances, even assuming the usual conservative reconciliation efficiencies for CV protocols based on binary modulated keys [13]. Apart from its possible practical significance, this protocol also adds to our fundamental understanding of CVQKD since it is based on the active use of CV teleportation protocols [20], opening up alternative ways to understand the security of CVQKD as well as different routes for future unconditional security proofs.

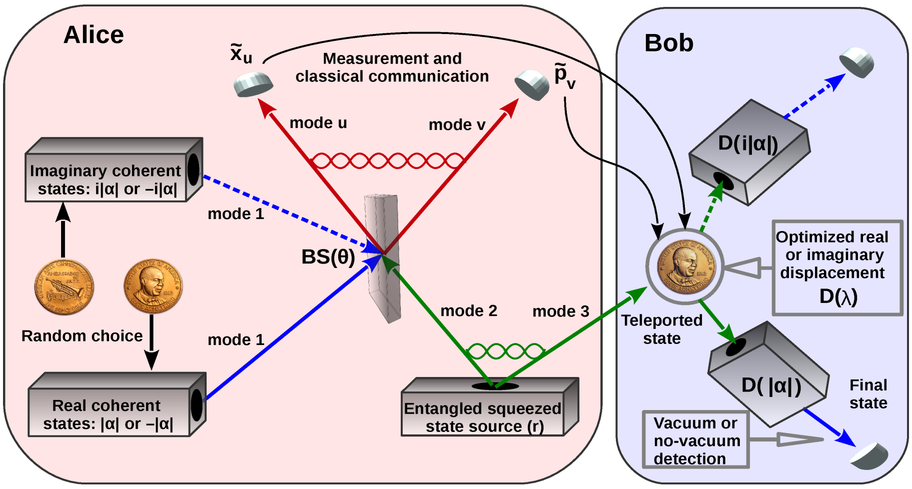
Alice
$\tilde{x}_u$
Measurement and classical communication
$\tilde{p}_v$
mode u
mode v
Imaginary coherent states: i|α| or −i|α|
mode 1
BS(θ)
Random choice
mode 1
Real coherent states: |α| or −|α|
mode 2
mode 3
Entangled squeezed state source (r)
Bob
D(i|α|)
Optimized real or imaginary displacement D(λ)
Teleported state
D(|α|)
Final state
Vacuum or no-vacuum detection

Fig. 1 Schematic representation of the teleportation-based CVQKD protocol. The encoding of the binary key on which Alice and Bob agree is $\{|-\alpha\rangle, |\alpha\rangle, |-i\alpha\rangle, |i\alpha\rangle\} = \{0, 1, 0, 1\}$, where α is a real number. See text and Appendix B for details.

Following [22,23], the main idea behind the present teleportation-based CVQKD scheme is the active use of the finite resources (finite squeezing) inherently associated to the CV teleportation protocol, combined with the knowledge of the pool of coherent states with Alice to be teleported to Bob [23]. It is by properly making use of these two pieces of information that we can build a protocol furnishing high key rates even in a scenario with high losses, turning the finiteness of squeezing into an advantage. Indeed, the CV teleportation protocol is not simply employed as an alternative to the direct sending of the states with Alice to Bob, as required by the aforementioned standard CVQKD protocols, where the greater the entanglement of the channel the more a flawless teleportation is achieved with subsequent higher key rates[2]. In the present protocol, however, less entanglement means more efficiency (see

[2] Note that the goals of the standard CV teleportation protocol [20] as well as the one of Ref. [23] are not a secure transmission of quantum states. The generalized CV teleportation protocol of Ref. [23] is used here as a tool to the development of the present CVQKD

Appendix D), since we show that for a lossy transmission the amount of entanglement (squeezing) maximizing the key rate is finite, dependent on the level of loss, and on the coherent states chosen for encoding the key. In other words, the maximally entangled (infinitely squeezed) channel connecting Alice and Bob is not the one yielding the greatest key rate.

2 The protocol

Let start describing the protocol (figure 1), whose main ingredient is the modified CV teleportation protocol presented in [23], where Bob can get an output state at the end of the teleportation nearly identical to the input state, even for low squeezing, if Alice and Bob know the set of input states to be teleported. (See Appendix A for a self-contained presentation of the modified CV teleportation protocol.) To achieve that Alice has to modify her beam splitter (BS) transmittance and Bob has to modify the displacement $\hat{D}_k(\lambda) = e^{\lambda \hat{a}_k^\dagger - \lambda^* \hat{a}_k}$ on his mode, from those given by the original CV teleportation protocol [20], according to the pool of input states. Here $\hat{a}_k$ ($\hat{a}_k^\dagger$) is the annihilation (creation) operator of mode k with quadratures $\hat{x}_k = (\hat{a}_k + \hat{a}_k^\dagger)/2$ and $\hat{p}_k = (\hat{a}_k - \hat{a}_k^\dagger)/2i$ and commutation relation $[\hat{x}_k, \hat{p}_k] = i/2$.

The present teleportation-based CVQKD protocol works as follows. Alice divides her pool of coherent states into two sets, $\{|\alpha\rangle, |-\alpha\rangle\}$ and $\{|i\alpha\rangle, |-i\alpha\rangle\}$, which we respectively call real and imaginary basis ($\alpha > 0$). Alice and Bob agree beforehand on the following binary encoding [8] in order to associate from each coherent state a bit value to the key: $\{|-\alpha\rangle, |-i\alpha\rangle\} \rightarrow 0$ and $\{|\alpha\rangle, |i\alpha\rangle\} \rightarrow 1$. At each run of the protocol, Alice randomly chooses between the real and imaginary basis and then randomly picks one of the two states belonging to the chosen basis. Let us generically call this state by $|\varphi\rangle$, which is teleported to Bob by means of a two-mode squeezed state $|\psi_r\rangle$, with squeezing parameter r [20, 21]. $|\psi_r\rangle$ is prepared by Alice, who keeps one of its mode and send the other to Bob. In order to finish her part in the teleportation, Alice combines her share of the entangled resource with $|\varphi\rangle$ in a BS with transmittance $\cos^2\theta$. After measuring the position and momentum quadratures of the modes outgoing the BS, Alice informs Bob of her measurement results ($\tilde{x}_u$ and $\tilde{p}_v$).

Bob, who now knows the values of $\tilde{x}_u$ and $\tilde{p}_v$, randomly chooses between two possible types of displacements $\hat{D}(\lambda)$ to implement on his mode ($\lambda = g_u\tilde{x}_u + ig_v\tilde{p}_v$), which we call real and imaginary displacements. These different types of displacements are given by different pairs of gains (g_u, g_v) and are optimized in the following sense. The real (imaginary) displacement is such that Bob's state, $\hat{\rho}_B$, has the greatest fidelity possible with Alice's input if she chose the real (imaginary) basis and the least fidelity if her choice was the imaginary (real) basis. Moreover, this is done such that the optimal (g_u, g_v) do not depend on the sign of the teleported coherent state but only on its being a

scheme. Without the present modifications, the protocols given in Refs. [20, 23] are not able to achieve a secure transmission of quantum states.

real or imaginary state (see figure 2 and the following paragraphs). Note that by fidelity we mean a quantity $F \in [0,1]$ that measures the similarity between two quantum states and in our case can be written as $F = \langle\varphi|\hat{\rho}_B|\varphi\rangle$, where $F = 0$ for orthogonal states and $F = 1$ for identical ones.

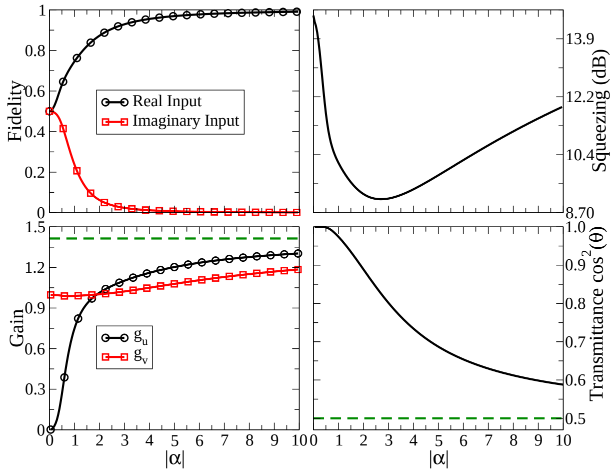

Fig. 2 Optimized parameters giving the greatest (least) fidelity for a teleported real (imaginary) coherent state. The optimal settings for the greatest (least) fidelity for an imaginary (real) input are obtained from the ones above by interchanging g_u with g_v and changing θ to $\pi/2 - \theta$. The squeezing remains unchanged. The dashed curves give the settings for the original CV teleportation protocol [20].

The next step of the protocol consists in Bob once again displacing his state. He applies $\hat{D}(\alpha)$ to his mode if he previously implemented the real displacement or $\hat{D}(i\alpha)$ otherwise. The goal of this last displacement is to transform either the states $|-\alpha\rangle$ or $|-i\alpha\rangle$ to vacuum states or to move farther from the vacuum the states $|\alpha\rangle$ or $|i\alpha\rangle$. One of these real (imaginary) states nearly describes $\hat{\rho}_B$ if Alice chose the real (imaginary) basis and Bob the real (imaginary) displacement in a given run of the protocol. After the last displacement Bob measures the intensity of his mode and associates the bit 0 if he sees no light (vacuum state) or the bit 1 if he sees any light (see figure 3). Note that the previous step can be modified to any strategy aimed to discriminate between two coherent states, such as the measurement of the quadratures of $\hat{\rho}_B$ using homodyne detection.

Alice and Bob repeat the previous steps until they have enough data to check for an eavesdropper and still get a secure key long enough for their purposes. After Alice finishing all teleportations and after Bob making all measurements, they use an authenticated classical channel to disclose the following information. Alice reveals to Bob the basis used at each run of the protocol but not the state. Bob reveals to Alice the instances where he used the optimal values of g_u and g_v matching the basis chosen by Alice. They

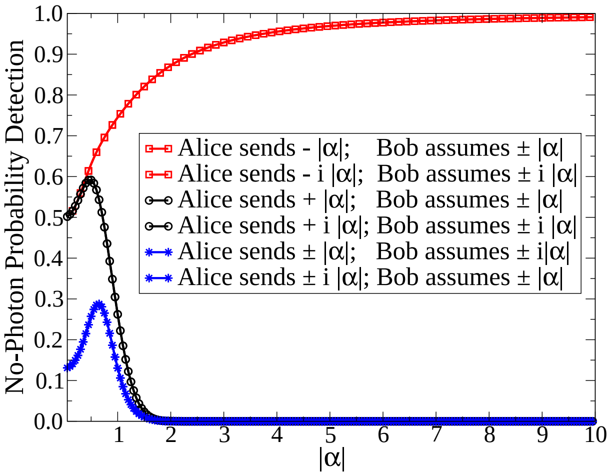

Fig. 3 Probabilities for Bob detecting the vacuum state at the end of a run of the protocol if Alice and Bob use the optimal settings given in figure 2. Whenever Bob (or Eve) assumes incorrectly the basis employed by Alice, he (she) cannot discern between the two possible inputs (star/blue curves). Note that this fact resembles the key generation scheme of the BB84 protocol [1] and is one of the reasons why this protocol is successful in establishing a secure key between Alice and Bob.

discard the data where no matches occurred and use a sample of the remaining data to check for the parameters of the quantum channel (loss and noise) they previously determined or assumed and to check for security. Then they implement error correction techniques on the non disclosed data (reconciliation stage) in order to agree on the random sequence of zeros and ones and, subsequently, generate the final secret key via standard privacy amplification techniques (classical algorithms devised to enhance the privacy of a shared random sequence of data).

As mentioned above, a key feature of the present protocol is the fact that the optimal (g_u, g_v) can be chosen such that they do not depend on the sign of the teleported coherent state, depending only on the state being real or imaginary. We can see that this can be done by looking at the functional form of F after a single run of the protocol. Assuming, for definiteness, we are dealing with real coherent states we have

$$F = h_1(r,\theta)\exp[f_1(\tilde{p}_v, \tilde{x}_u, g_v, g_u, r, \theta) + 2\alpha\tilde{x}_u f_2(g_u, r, \theta) + \alpha^2 f_3(r,\theta)], \qquad (1)$$

where the functions h_1 and $f_j, j = 1,2,3$, are given in Appendix B, along with all the mathematical details needed to understand the present protocol. Looking at (1) we see that F depends on α only linearly and quadratically. This means that we can cancel the dependence of F on the sign of α by eliminating the linear dependence on it. This is achieved by demanding that

$$f_2(g_u, r, \theta) = 0, \qquad (2)$$

which leads to

$$g_u(r,\theta) = \frac{\sinh(2r)\sin\theta}{\cosh^2 r - \cos(2\theta)\sinh^2 r}. \tag{3}$$

Furthermore, maximizing F with respect to g_v immediately gives

$$g_v(r,\theta) = \frac{2\coth r\cos\theta}{\coth^2 r + \cos(2\theta)}. \tag{4}$$

In figure 2 we show the optimal values for these quantities, where r and θ are chosen such that we get the greatest fidelity for a real teleported state and the least fidelity when teleporting an imaginary state. It is worth mentioning that this protocol is very robust to fluctuations about those optimal values as we show in detail in Appendix B. Also, the physical resources needed to implement the present protocol with reasonable key rates are already available, in particular the efficient production of two-mode squeezed states [21], the main ingredient of the present protocol.

Before we proceed with the security analysis of this protocol, let us review what we have so far. We showed, first, that it is possible to choose optimal parameters maximizing the fidelity *independently* of the sign of the teleported coherent state and, second, that this choice *depends* on the coherent state being real or imaginary. Third, we also showed that Bob can discern which state Alice teleported if, and only if, he chooses the right displacement to implement on his mode at the end of a single run of the protocol (see figure 3). Those three features reminds us of the working principles of the BB84 protocol [1], where Bob can only obtain the right bit in a given run of the protocol if he measures his qubit using the same basis employed by Alice to prepare it. In our case, the non-orthogonal basis of the BB84 protocol is related to the real and imaginary basis defined here; and the fact that the BB84 protocol only succeeds if Bob chooses the right measurement basis is connected here to the fact that Bob must choose the right displacements g_u and g_v to succeed.

3 Security analysis

Let us move to the security analysis, where we deal with individual (incoherent) attacks only. The intercept-resend attack, with an eavesdropper Eve blocking Bob's share of the entangled state (mode 3 in figure 1) and sending him a fake mode, is not as serious a threat as the BS attack we will be dealing with in what follows. This is true because Eve cannot know Alice's input with certainty *before* sending Bob the fake mode. Indeed, Eve can only hope to know Alice's input by knowing which basis she used and this only happens *after* Bob measures his mode.

The most serious incoherent attack to the present and all CVQKD schemes is the BS attack, in which Eve inserts a BS of transmittance η in the optical line connecting Alice and Bob and operates on the signal reaching her $(1-\eta)$ in the same way as Bob does with his share of the signal (η). Note that the BS attack is equivalent to a lossy transmission where $1-\eta$ of the signal is lost to the environment. For direct reconciliation [5,6], the secure key rate generated between Alice and Bob in the BS attack is

$$K = \max\{0, \beta I_{AB} - I_{AE}\} = \{0, \Delta I\}, \tag{5}$$

where I_{AB} and I_{AE} are the mutual information between Alice and Bob and Alice and Eve, respectively. β is the reconciliation efficiency and depends on the reconciliation software employed. For binary encodings that we use here it has a conservative value of $\beta \approx 80\%$ [13]. Since the present protocol and the BS attack are symmetric with respect the real and imaginary states, in the following security analysis we consider only the case where Alice used the real basis and Bob and Eve the real displacement, i.e., we assume Alice teleported either the coherent state $|\alpha\rangle$ or $|-\alpha\rangle$, with α real, and Bob and Eve correctly guessed that Alice chose a real coherent state.

A direct calculation of the mutual informations gives (see Appendix C),

$$\begin{aligned} I_{AY} = 1 + \sum_{j=0}^{1} [& q_j^Y \log_2 q_j^Y + (1-q_j^Y)\log_2(1-q_j^Y) \\ & -(1+q_j^Y - q_{\bar{j}}^Y)\log_2(1+q_j^Y - q_{\bar{j}}^Y)]/2, \end{aligned} \tag{6}$$

where $Y = B$ or E, $\bar{j} = 0(1)$ if $j = 1(0)$, and q_j^Y is the unconditional (no postselection) probability of Y to assign the bit j to the key if Alice teleported the corresponding state that encodes the bit j. In the present case q_0^Y means the probability of Y to detect the vacuum state at the end of a run of the protocol if Alice teleports $|-\alpha\rangle$ while q_1^Y is the probability of Y to detect any light if she teleports $|\alpha\rangle$. Note that q_j^Y depends on η and that $q_j^B(\eta) = q_j^E(1-\eta)$.

In figure 4 we plot ΔI for several values of loss employing the parameters shown in figure 2. The inset shows that it is possible to choose a value of α such that for $\beta = 0.8$ and 90% loss we get $K \approx 0.03$. This value should be contrasted with those without excess noise in [6], where by setting a perfect direct reconciliation ($\beta = 1$) and postselection one gets $K = 0.007$ at 75% loss, and with the ones in [10], where above 80% loss it is not possible to extract a secret key via direct reconciliation. In other words, we improve the key rate at about one order of magnitude even assuming more loss. To get such enormous gain in the key rate we need a squeezing of about 10 dB.

When the loss is exactly 100%, the protocol does not work since Bob's state is the vacuum state and Eve can also operate on a vacuum state instead of the intercepted signal. In this scenario Bob and Eve have the same mutual information with Alice. This suggests a possible attack on the present protocol, where for very high losses Eve chooses to operate on the vacuum state instead of her share of the intercepted signal. This seems reasonable since the vacuum state is closer to the state with Bob in a very lossy environment. If Eve chooses to work with both the intercepted signal and the vacuum state, the effective secure key rate that can be achieved between Alice and Bob is

$$K_e = \max\{0, \min\{\Delta I, \Delta I_0\}\}, \tag{7}$$

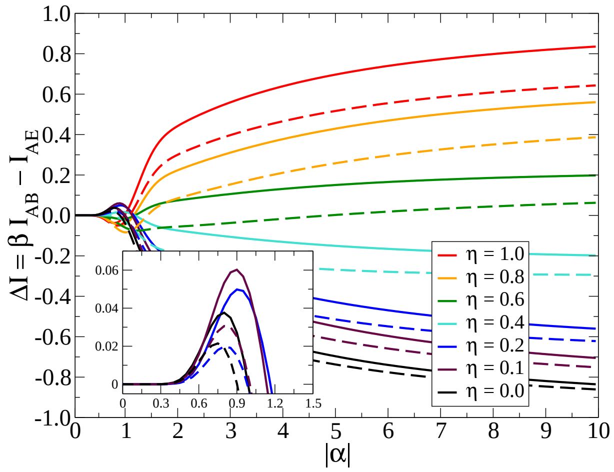

Fig. 4 All plots: Solid lines mean $\beta = 1.0$ and dashed lines $\beta = 0.8$. Main plot: For large values of $|\alpha|$ we have from top to bottom increasing (decreasing) loss (η). Inset: $\eta = 0.1$ (90% loss) for the greatest peaks of the solid and dashed curves while $\eta = 0.2$ (80% loss) for the corresponding lowest ones.

where $\Delta I_0 = \beta I_{AB} - I_{AE}^0$ and I_{AE}^0 is the mutual information between Alice and Eve assuming Eve's state is the vacuum.

Using for g_u and g_v their optimal previously obtained expressions when the matching condition occurs, Eqs. (3) and (4), K_e becomes a function of only r, θ, and η. Fixing η, we can optimize K_e as a function of r and θ once we choose a coherent state $|\alpha\rangle$ (see Appendix C). Working with $\beta = 0.8$, we obtained for 90% loss two regions of α in which a meaningful key can be obtained. For $\alpha \approx 0.5$ we have $K_e = 0.001$ with $r = 1.44$ (12.5 dB) and for $\alpha \approx 1.75$ we get $K_e \approx 0.009$ with $r \approx 0.93$ (8.1 dB). When the losses are 95% we get for $\alpha \approx 0.5$, $K_e \approx 0.0008$ with $r \approx 1.47$ (12.8 dB), and for $\alpha \approx 1.6$, $K_e \approx 0.001$ with $r \approx 0.85$ (7.4 dB). In Appendix D we give for every α between 0 and 10 the optimal values for the key rates and the corresponding optimal parameters leading to those key rates.

Table 1 Optimized key rates K_e for a fixed reconciliation efficiency β, loss $1 - \eta$, and squeezing r with the corresponding optimal parameters. We assume real states $|\alpha\rangle$.

β	loss	r(dB)	α	$\cos^2\theta$	g_u	g_v	K_e
0.8	95%	0.9(7.82)	1.65	0.058	0.957	0.632	2.9×10^{-3}
0.9	95%	0.7(6.08)	1.60	0.080	0.887	0.494	3.7×10^{-3}
1.0	99%	0.1(0.87)	1.50	0.114	0.186	0.068	3.0×10^{-6}
1.0	99%	0.2(1.74)	1.50	0.116	0.360	0.139	6.8×10^{-5}
1.0	99%	0.3(2.61)	1.50	0.108	0.516	0.206	4.2×10^{-4}
1.0	99%	0.4(3.47)	1.55	0.129	0.640	0.306	1.3×10^{-3}

Fortunately the present scheme can be secure for low squeezing r, in particular if Alice and Bob use state of the art reconciliation protocols in which $\beta \approx 1$. Working with fixed values of r and maximizing K_e as a function of θ we can show that for squeezing below 2 dB it is still possible to get a secure key. In table 1 we show the maximum K_e attainable for different values of squeezing and reconciliation efficiencies (β). Note that for $\beta = 0.8$ or 0.9 our numerical maximization indicated that one cannot get a secure key when losses are about or higher than 99% .

We can estimate how far Alice and Bob can be for the present protocol to work securely and with a reasonable bit generation rate as follows. Noting that state of the art generation rates of two-mode squeezed states [21] are of 10^6 events per second, and working with a key rate of at least $K_e = 10^{-3}$, the present protocol allows Alice and Bob to share at least 10^3 bits per second. With that in mind, looking at table 1 we see that for $\beta = 0.8$ we can get $K_e = 10^{-3}$ at 95% loss and for $\beta = 1.0$ we can go up to 99% loss. Now, assuming standard telecommunication fiber optics, we have an attenuation coefficient $\epsilon = 0.2\,\text{dB/km}$. Since the relation between distance L, loss $1 - \eta$ and ϵ is $\eta = 10^{-\epsilon L/10}$ [2], we get for 95% loss $L = 65$ km and for 99% loss $L = 100$ km.

We have also computed for several values of reconciliation efficiency β and squeezing r the optimal key rate as a function of the loss or, equivalently, the distance between Alice and Bob. The free parameters in the optimization procedure were the coherent state α and Alice's BS transmittance $\cos^2\theta$; g_u and g_v were set to the values given in Eqs. (3) and (4).

In Fig. 5 we show the optimal key rate K_e, Eq. (7), and in Figs. 6 and 7 the optimal parameters leading to the curves shown in Fig. 5.

Looking at Fig. 5 we note that there exist two distinct regimes for the behavior of the optimal key rate K_e. The first one, for losses below 50%, as we increase the loss we decrease K_e. The second regime occurs for losses greater than 50%. In this case K_e first increases with more loss, reaching its maximum value at about 80% loss, and then decreases with loss. It is worth mentioning that at losses about 50% no key can be established, at least to the precision of our numeric computations (6 significant figures). We can understand that fact remembering that at 50% loss the density matrices describing the states with Bob and Eve are equal and, therefore, the mutual information between Bob and Alice is exactly equal to the one between Eve and Alice; no secure key can be established in this case [3]. For a similar reason we cannot get a secure key for losses close to 100%, since in this situation Eve employs the vacuum state which is very close to the state with Bob, who receives almost no signal. Thus, it is expected that very close to the 50% loss or to the 100% loss no key can be generated. Moreover, as the loss approaches 50%, either from below or

[3] In other words, as we approach the value of 50% loss, either from above or below, the states reaching Bob and Eve become more and more equal and the key rate must necessary decrease, being exactly zero when we reach the 50% loss threshold since in this situation Bob and Eve have exactly the same state.

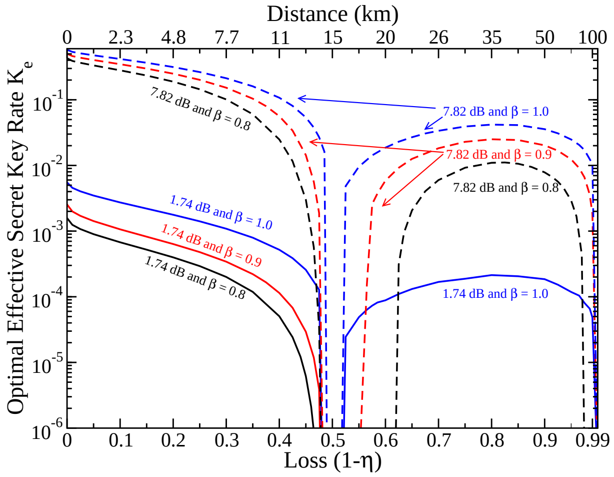

Fig. 5 Optimal key rate as a function of loss (lower horizontal axis) or, equivalently, as a function of the distance between Alice and Bob (upper horizontal axis), assuming standard fiber optics attenuation (0.2 dB/km). The squeezing r (in dB) of the quantum channel connecting Alice and Bob as well as the reconciliation efficiency β employed in the computation of the key are indicated in the curves.

above, and as the loss tends to 100%, the key rate decreases very fast, being exactly zero at those two values of loss for the reasons given above.

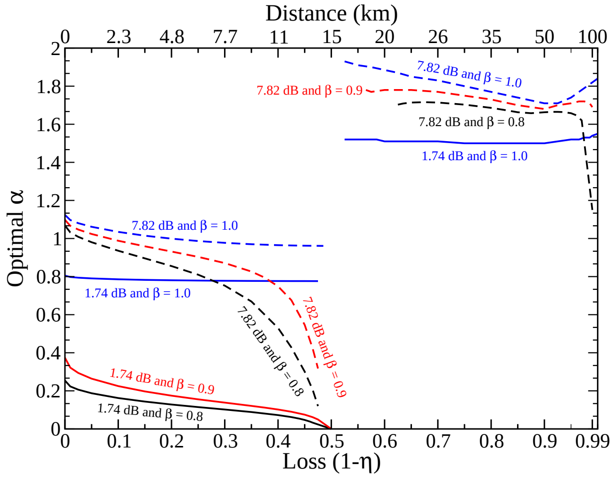

Fig. 6 Coherent state α leading to the optimal key rates shown in Fig. 5.

Looking at Fig. 7 we can see the main reason why this protocol works securely when Eve implements the BS attack and operates on her share of the

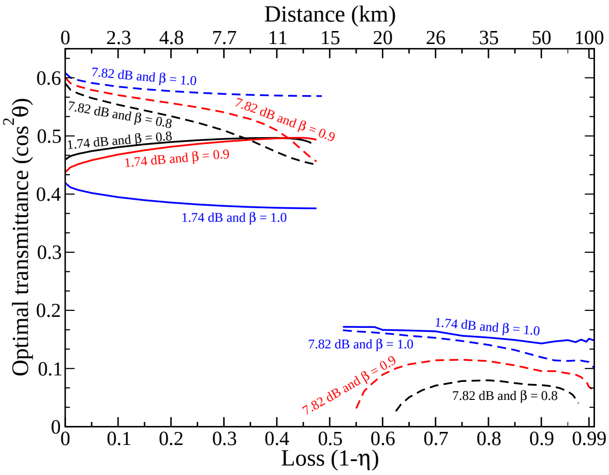

Fig. 7 Alice's BS transmittance $\cos^2\theta$ leading to the optimal key rates shown in Fig. 5. The optimal g_u and g_v can be obtained using Eqs. (3) and (4) and the data above to obtain θ by noting that $0 < \theta < \pi/2$.

signal in the *same* way as Bob, even when we cross the 50% loss threshold. It is due to the fact that the optimal transmittance ($\cos^2\theta$) for Alice's BS leading to the highest mutual information between Alice and Bob, and therefore to the optimum key rate K_e, depends on the loss of the quantum channel connecting them. (We should not forget that Alice's BS transmittance also depends on whether we have real or imaginary states. We are considering, as stated in the beginning of this section, the situation where Alice employed the real basis and both Bob and Eve correctly chose the real displacements.) Indeed, since Bob receives η of the signal in a lossy transmission, Alice sets the transmittance of her BS in order to maximize the mutual information between her and Bob in this scenario. However, Eve gets $1-\eta$ of the signal, which requires a completely different value of transmittance for Alice's BS in order to make Eve's state a good approximation to the teleported one. In other words, since Alice chooses the optimal setting for her BS according to the intensity of the signal reaching Bob (η), Eve's share of the teleported state is not as good a description of the original teleported state as Bob's share is. Because of this fact the mutual information between Alice and Eve (I_{AE}) is lower than the one between Alice and Bob (I_{AB}), which is the ingredient needed to establish a secure key between Alice and Bob.

A final remark is in order before we finish this section. The previous security analysis was carried out assuming an individual (incoherent) BS attack and Eve operating *exactly* as Bob in order to extract the secure key. Therefore, it is important to extend the security analysis here in at least two ways to check whether the interesting security properties of the present protocol still hold, in particular its secure operation above the 50% loss threshold. First, we need to check different scenarios at the incoherent attack level. For example, what would happen if Eve attenuates her share of the signal to the same intensity reaching Bob and only then operates on her share to extract the key? Second, it is crucial to study more powerful attacks, such as collective and coherent attacks. Moreover, it is also important to point out that it is not obvious that the techniques employed in the security analysis of collective and coherent attacks for Gaussian modulated CV protocols can be directly employed here (we employed binary discrete modulation/encoding). This is due to the fact that a non-Gaussian encoding of the key, even if employing Gaussian states, have non-Gaussian entanglement-based representations, and the latter fact means that the calculation of Eve's information cannot rely on the optimality proofs of continuous modulated protocols [18]. In other words, a whole new mathematical analysis must be done in order to compute in our case the optimal Holevo's bound (upper bound of Eve's information), the quantity needed to investigate collective and more general forms of security attacks. So far we could not solve that problem or find its solution in the literature. A possible starting point in this direction would be to generalize the analysis in Ref. [24] to the present protocol in order to estimate at least lower and upper bounds on the secure key rate when Eve implements collective attacks.

We also remark that our main goal in writing this article was to present a new way of doing CVQKD based on the CV teleportation protocol and to understand its *potential* as a viable secure alternative to realize CVQKD. We compared its efficiency and security to the ones of the standard CVQKD protocols when those protocols operate under the same assumptions as ours, i.e, a BS attack (loss in the channel) and no excess noise. The standard CVQKD protocols we used as a benchmark of comparison were those of Refs. [5,6]. And when it comes to efficiency in the security scenario described above, our protocol gives higher key rates than the ones of the aforementioned references. This is the main message we wanted to pass by writing this article and we hope to encourage those working with CVQKD to further assess the security of the present protocol under more severe attacks.

4 Conclusion

In summary, we proposed a new and efficient CVQKD scheme with a binary encoding for the key (discrete modulation) based on the CV teleportation of coherent states, where the CV teleportation protocol is not just a substitute to the direct sending of coherent states from Alice to Bob for the usual CVQKD protocols. Rather, the resources needed to implement the CV teleportation protocol play a direct role in the generation of the secret key since Alice's BS transmittance, the squeezing of the entangled channel, and Bob's displacement are all tuned in order to generate a secret key.

We showed that the present teleportation-based CVQKD protocol is secure against individual attacks and in particular that it works with direct reconciliation and no postselection even for very high loss in the optical channel connecting Alice and Bob. Moreover, we showed that it is possible to achieve fairly high key rates with mild squeezing (≈ 2 dB) near the 100% loss regime. This fact combined with the high repetition rates of CV technology may lead to efficient long distance QKD protocols. Indeed, once a mildly squeezed two-mode entangled state channel is established between Alice and Bob, directly or via entanglement swapping techniques, they can generate a secret key using the present CVQKD scheme.

Finally, the present CVQKD protocol naturally leads to many interesting open questions. First, since we have only dealt with the noiseless case, the next question is to understand how robust the present scheme is to the addition of noise at the transmission line. Second, can reverse reconciliation and/or postselection increase the key rates of this scheme and decrease even more the level of squeezing to generate a secure key? Third, will the present protocol still work in a very lossy environment if it suffers different types of security attacks, such as the collective and coherent attacks? Those are the problems we will be tackling in the near future and, so far, the main message one can extract from the present article is that for individual BS attacks we have a teleportation-based CVQKD protocol, built on a binary encoding for the key, with at least the same level of security of the standard CVQKD protocols and, at the same time, operating beyond the 50% loss threshold without resorting to postselection or reverse reconciliation.

Acknowledgments

FSL and GR thank CNPq (Brazilian National Council for Scientific and Technological Development) for funding and GR thanks CNPq/FAPESP (State of São Paulo Research Foundation) for financial support through the National Institute of Science and Technology for Quantum Information.

A The modified CV teleportation protocol

A key ingredient to the present scheme is the CV teleportation protocol [20] adapted to the case where Alice and Bob has a complete knowledge of the pool of possible states to be teleported [23]. With such a knowledge, Alice and Bob can greatly improve the fidelity between the teleported state with Bob and Alice's input by changing certain parameters of the original proposal. Our goal in this section is to review in a self contained way this modified CV teleportation protocol, following closely the presentation given in [23].

Let $\hat{x}_k = (\hat{a}_k + \hat{a}_k^\dagger)/2$ and $\hat{p}_k = (\hat{a}_k - \hat{a}_k^\dagger)/2i$ be the position and momentum quadratures of mode k, respectively, where $\hat{a}_k$ and $\hat{a}_k^\dagger$ are the annihilation and creation operators with commutation relation $[\hat{a}_k, \hat{a}_k^\dagger] = 1$.

Any input state with Alice can be expressed in the position basis as

$$|\varphi\rangle = \int dx_1 \varphi(x_1)|x_1\rangle, \tag{8}$$

where the integral covers the entire real line and $\varphi(x_1) = \langle x_1|\varphi\rangle$. The entangled two-mode squeezed state shared between Alice and Bob can also be expressed in the position basis,

$$|\psi_r\rangle = \int dx_2 dx_3 \psi_r(x_2, x_3)|x_2, x_3\rangle, \tag{9}$$

with $\psi_r(x_2,x_3) = \langle x_2, x_3|\psi_r\rangle$ and $|x_2,x_3\rangle = |x_2\rangle \otimes |x_3\rangle$. Here the first two modes/kets are with Alice and the third one with Bob. Using Eqs. (8) and (9) the initial state describing all modes before the teleportation is as follows,

$$|\Psi\rangle = |\varphi\rangle \otimes |\psi_r\rangle = \int dx_1 dx_2 dx_3 \varphi(x_1)\psi_r(x_2,x_3)|x_1,x_2,x_3\rangle. \qquad (10)$$

The teleportation begins sending mode 1 (input state) and mode 2 (Alice's share of the entangled state) into a BS with transmittance $\cos^2\theta$ (see figure 1). If $\hat{B}_{12}(\cos^2\theta)$ is the operator representing the action of the BS in the position basis we have [18]

$$\hat{B}_{12}(\cos^2\theta)|x_1,x_2\rangle = |x_1\sin\theta + x_2\cos\theta, x_1\cos\theta - x_2\sin\theta\rangle. \qquad (11)$$

Inserting equation (11) into (10) and changing variables such that $x_v = x_1\sin\theta + x_2\cos\theta$ and $x_u = x_1\cos\theta - x_2\sin\theta$ we get

$$|\Psi'\rangle = \int dx_v dx_u dx_3 \varphi(x_v\sin\theta + x_u\cos\theta) \times\psi_r(x_v\cos\theta - x_u\sin\theta, x_3)|x_v,x_u,x_3\rangle \qquad (12)$$

for the total state after modes 1 and 2 go through the BS.

In the next step Alice measures the momentum and position quadratures of modes v and u, respectively. Since Alice will project mode v onto the momentum basis, it is convenient to rewrite equation (12) using the Fourier transformation relating the position and momentum basis,

$$|x_v\rangle = \frac{1}{\sqrt{\pi}}\int dp_v e^{-2ix_vp_v}|p_v\rangle. \qquad (13)$$

This leads to

$$|\Psi'\rangle = \frac{1}{\sqrt{\pi}}\int dp_v dx_v dx_u dx_3 \varphi(x_v\sin\theta + x_u\cos\theta) \times\psi_r(x_v\cos\theta - x_u\sin\theta, x_3)e^{-2ix_vp_v}|p_v,x_u,x_3\rangle. \qquad (14)$$

Let us assume Alice obtains for the momentum of mode v and for the position of mode u the values $\tilde{p}_v$ and $\tilde{x}_u$. Thus, the state after the measurement is

$$|\Psi''\rangle = \hat{P}_{\tilde{p}_v,\tilde{x}_u}|\Psi'\rangle/\sqrt{\mathrm{p}(\tilde{p}_v,\tilde{x}_u)},$$

where $\hat{P}_{\tilde{p}_v,\tilde{x}_u} = |\tilde{p}_v,\tilde{x}_u\rangle\langle\tilde{p}_v,\tilde{x}_u| \otimes 1_3$ is the von Neumann projector describing the measurements. Here 1_3 is the identity operator acting on mode 3 and $\mathrm{p}(\tilde{p}_v,\tilde{x}_u) = \mathrm{tr}\,(|\Psi'\rangle\langle\Psi'|\hat{P}_{\tilde{p}_v,\tilde{x}_u})$ is the probability of measuring momentum $\tilde{p}_v$ and position $\tilde{x}_u$, with tr denoting the total trace. Specifying to the position basis and using that $\langle p_v|\tilde{p}_v\rangle = \delta(p_v - \tilde{p}_v)$ and $\langle x_u|\tilde{x}_u\rangle = \delta(x_u - \tilde{x}_u)$ we have

$$|\Psi''\rangle = |\tilde{p}_v,\tilde{x}_u\rangle \otimes |\chi'\rangle, \qquad (15)$$

where Bob's state is

$$|\chi'\rangle = \frac{1}{\sqrt{\pi\mathrm{p}(\tilde{p}_v,\tilde{x}_u)}}\int dx_v dx_3 e^{-2ix_v\tilde{p}_v}\varphi(x_v\sin\theta + \tilde{x}_u\cos\theta) \times\psi_r(x_v\cos\theta - \tilde{x}_u\sin\theta, x_3)|x_3\rangle. \qquad (16)$$

Here

$$\mathrm{p}(\tilde{p}_v,\tilde{x}_u) = \int dx_3|\Psi'(\tilde{p}_v,\tilde{x}_u,x_3)|^2 \qquad (17)$$

and $\Psi'(\tilde{p}_v, \tilde{x}_u, x_3) = \langle \tilde{p}_v, \tilde{x}_u, x_3 | \Psi' \rangle$ such that

$$\Psi'(\tilde{p}_v, \tilde{x}_u, x_3) = \frac{1}{\sqrt{\pi}} \int dx_v \varphi(x_v \sin\theta + \tilde{x}_u \cos\theta) \\ \times \psi_r(x_v \cos\theta - \tilde{x}_u \sin\theta, x_3) e^{-2ix_v\tilde{p}_v}, \tag{18}$$

where equation (18) was obtained using (14).

Via a classical channel Alice sends to Bob her measurement results, allowing Bob to displace his mode quadratures as follows, $x_3 \rightarrow x_3 + g_u\tilde{x}_u$ and $p_3 \rightarrow p_3 + g_v\tilde{p}_v$. Mathematically this corresponds to the application of the displacement operator $\hat{D}(\lambda) = e^{\lambda\hat{a}^\dagger - \lambda^*\hat{a}} = e^{-2iRe[\lambda]\hat{p} + 2iIm[\lambda]\hat{x}}$, with $\lambda = g_u\tilde{x}_u + ig_v\tilde{p}_v$ and * denoting the complex conjugation. Since $\hat{x}$ and $\hat{p}$ commute with their commutator Glauber's formula applies, giving $\hat{D}(\lambda) = e^{iRe[\lambda]Im[\lambda]}e^{-2iRe[\lambda]\hat{p}}e^{2iIm[\lambda]\hat{x}}$ and finally

$$\hat{D}(g_u\tilde{x}_u + ig_v\tilde{p}_v)|x_3\rangle = e^{ig_u g_v \tilde{x}_u \tilde{p}_v} e^{2ig_v\tilde{p}_v x_3} |x_3 + g_u\tilde{x}_u\rangle. \tag{19}$$

Bob's state after the displacement, $|\chi\rangle = \hat{D}(g_u\tilde{x}_u + ig_v\tilde{p}_v)|\chi'\rangle$, can be written as follows if we use equation (19) and change variable such that $x_3 \rightarrow x_3 - g_u\tilde{x}_u$,

$$|\chi\rangle = \int dx_3 \chi(x_3)|x_3\rangle, \tag{20}$$

with

$$\chi(x_3) = \frac{e^{-ig_u g_v \tilde{x}_u \tilde{p}_v}}{\sqrt{\pi \mathrm{p}(\tilde{p}_v, \tilde{x}_u)}} \int dx_v \varphi(x_v \sin\theta + \tilde{x}_u \cos\theta) \\ \times \psi_r(x_v \cos\theta - \tilde{x}_u \sin\theta, x_3 - g_u\tilde{x}_u) e^{-2i(x_v - g_v x_3)\tilde{p}_v}. \tag{21}$$

In order to estimate after a single run of the protocol the closeness of Bob's state, $\hat{\rho}_B = |\chi\rangle\langle\chi|$, with the original one at Alice's, $\rho_{input} = |\varphi\rangle\langle\varphi|$, we use the fidelity

$$F = \langle\varphi|\hat{\rho}_B|\varphi\rangle = \int dx_3' dx_3 \varphi^*(x_3')\chi(x_3')\chi^*(x_3)\varphi(x_3). \tag{22}$$

In general F depends on the input state $|\varphi\rangle$, the measurement outcomes of Alice ($\tilde{x}_u$ and $\tilde{p}_v$), the squeezing r of the entangled two-mode squeezed state, θ, g_u, and g_v. Also, F achieves its highest value ($F = 1$) if we have a flawless teleportation ($\hat{\rho}_B = \hat{\rho}_{input}$) and its minimal one ($F = 0$) if the output is orthogonal to the input.

We will be dealing with input states given by coherent states, $|\varphi\rangle = |\alpha e^{i\xi}\rangle$, with α and ξ reals, and with entangled two-mode squeezed states shared between Alice and Bob $|\psi_r\rangle = \sqrt{1 - \tanh^2 r}\sum_{n=0}^{\infty} \tanh^n r|n\rangle_A \otimes |n\rangle_B$, where $|n\rangle_{A(B)}$ are Fock number states with Alice (Bob) and r is the squeezing parameter. When $r = 0$ we have $|00\rangle$, the vacuum state, and for $r \rightarrow \infty$ the unphysical maximally entangled Einstein-Podolsky-Rosen (EPR) state.

In the position basis we have [18]

$$\varphi(x_1) = \langle x_1|\alpha e^{i\xi}\rangle = \left(\frac{2}{\pi}\right)^{1/4} e^{-x_1^2 + 2\alpha e^{i\xi}x_1 - \alpha^2/2 - \alpha^2 e^{i2\xi}/2} \tag{23}$$

and

$$\psi_r(x_2, x_3) = \langle x_2, x_3|\psi_r\rangle = \sqrt{\frac{2}{\pi}} \exp\left[-e^{-2r}(x_2 + x_3)^2/2 \ -e^{2r}(x_2 - x_3)^2/2\right]. \tag{24}$$

Note that for a two-mode squeezed state the variance $\Delta_r^2(x_2 - x_3) = \langle\psi_r|(x_2 - x_3)^2|\psi_r\rangle - \langle\psi_r|(x_2 - x_3)|\psi_r\rangle^2 = e^{-2r}/2$, which is employed to measure the squeezing of this state in decibel:

$$I_{\mathrm{dB}} = -10\log_{10}\left[\frac{\Delta_r^2(x_2 - x_3)}{\Delta_0^2(x_2 - x_3)}\right] = 20r\log_{10}(e). \tag{25}$$

B The teleportation-based CVQKD protocol

The present CVQKD protocol is based on a binary encoding for the key such that $\{|-\alpha\rangle, |\alpha\rangle, |-i\alpha\rangle, |i\alpha\rangle\} = \{0, 1, 0, 1\}$, with α a real number. These states are to be teleported from Alice to Bob randomly. A step by step description of a successful run of the protocol, generating a common random bit between Alice and Bob, is as follows. (1) Alice randomly chooses between the real or imaginary coherent state "basis" and then randomly prepares $|\pm\alpha\rangle$ or $|\pm i\alpha\rangle$, respectively, to teleport to Bob. In Fig. 1 we describe the case where Alice chooses $|\alpha\rangle$ (mode 1 given by the solid/blue line). (2) Alice generates a two-mode squeezed entangled state (modes 2 and 3), whose squeezing parameter r is chosen according to the value of α, and sends mode 3 to Bob. (3) Alice adjusts the beam splitter (BS) transmittance according to her choosing the real or imaginary basis and then sends mode 1 to interact with her share of the two-mode squeezed state (mode 2). (4) She measures the position and momentum quadratures of the modes u and v, respectively, that emerge after the BS and classically informs Bob of those results ($\tilde{x}_u$ and $\tilde{p}_v$). (5) Bob randomly chooses (g_u, g_v) from two possible pairs of values and implements a displacement operation on his mode given by $\hat{D}(\lambda)$, where $\lambda = g_u\tilde{x}_u + ig_v\tilde{p}_v$. g_u and g_v are such that the fidelity of Bob's output state with Alice's input is greatest if she chooses a real (imaginary) state and he assumes a real (imaginary) state and, at the same time, least if she chooses an imaginary (real) state and he assumes a real (imaginary) state. The optimal pair $(g_u,\, g_v)$ depends on the input being a real or imaginary coherent state but not on its sign. (6) Bob implements another displacement on his mode, $\hat{D}(\alpha)$ or $\hat{D}(i\alpha)$, depending on the choice he made for the pair (g_u, g_v). Fig. 1 shows the case in which Bob assumes Alice chooses the real basis (solid lines). Had he assumed the wrong basis, which Alice and Bob will discover classically communicating after finishing the whole protocol, they would discard this run of the protocol. (7) Bob measures the intensity of his mode and assigns the bit value 0 if he sees no light (vacuum mode) and the bit 1 otherwise.

B.1 Fidelity analysis

We will explicitly analyze the case where Alice chooses the real basis, namely, she teleports either $|-\alpha\rangle$ or $|\alpha\rangle$ to Bob. The calculations for the imaginary basis are similar and only the final results for this case will be given. Therefore, assuming that we have a real coherent state, Eqs. (20), (23), and (24) when inserted into Eq. (22) give

$$F = h_1(r,\theta)\exp[f_1(\tilde{p}_v, \tilde{x}_u, g_v, g_u, r, \theta) + 2\alpha\tilde{x}_u f_2(g_u, r, \theta) + \alpha^2 f_3(r,\theta)], \tag{26}$$

where

$$\begin{aligned}
h_1(r,\theta) &= \sqrt{1-\cos^2(2\theta)\tanh^4 r}, \\
f_1(\tilde{p}_v, \tilde{x}_u, g_v, g_u, r, \theta) &= \Big\{ \left[g_u^2\tilde{x}_u^2 - g_v^2\tilde{p}_v^2\right]\cos(2\theta)\tanh r + 4g_u\tilde{x}_u^2\sin\theta \\
&\quad +4g_v\tilde{p}_v^2\cos\theta\Big\}\tanh r \\
&\quad +\tilde{x}_u^2\left[-g_u^2 + \frac{2}{\cosh^2 r - \cos(2\theta)\sinh^2 r} - 2\right] \\
&\quad +\tilde{p}_v^2\left[-g_v^2 + \frac{2}{\cosh^2 r + \cos(2\theta)\sinh^2 r} - 2\right], \\
f_2(g_u, r, \theta) &= g_u - \{g_u\cos(2\theta)\tanh r + 2[1 + g_u\cos\theta]\sin\theta\}\tanh r \\
&\quad +2\left(\frac{1}{\cos(2\theta)\sinh^2 r - \cosh^2 r} + 1\right)\cos\theta, \\
f_3(r,\theta) &= -\frac{\{\cosh r - [\tanh r\cos(2\theta) + \sin(2\theta)]\sinh r\}^2}{\cosh^2 r - \cos(2\theta)\sinh^2 r}.
\end{aligned}$$

Since we want the optimal F in a way that the optimal settings do not depend on the sign of α we set $f_2(g_u, r, \theta) = 0$. This gives the following value for g_u,

$$g_u(r,\theta) = \frac{\sinh(2r)\sin\theta}{\cosh^2 r - \cos(2\theta)\sinh^2 r}. \tag{27}$$

Moreover, since g_v only appears in the exponent and we want the maximum of F, we maximize the exponent as a function of g_v. Differentiating the exponent with respect to g_v and equating to zero we get

$$g_v(r,\theta) = \frac{2\coth r\cos\theta}{\coth^2 r + \cos(2\theta)}. \tag{28}$$

Inserting g_u and g_v back into F we finally obtain

$$\begin{aligned} F^{\mathrm{re}}(r,\theta) =& \sqrt{1-\cos^2(2\theta)\tanh^4 r} \\ & \times \exp\left\{\frac{-\alpha^2\{\cosh r - \sinh r[\cos(2\theta)\tanh r + \sin(2\theta)]\}^2}{\cosh^2 r - \cos(2\theta)\sinh^2 r}\right\}, \end{aligned} \tag{29}$$

where we use the superscript "re" to remind us that this is the optimal F for real inputs. Also, it is important to note that the optimal expression for F, as well as for g_u and g_v, do not depend on the measurement outcomes $\tilde{x}_u$ and $\tilde{p}_v$ obtained by Alice. This is one of the reasons making the present CVQKD scheme yield high key rates without postselecting a subset of all possible measurement outcomes of Alice.

For an imaginary input, namely, either $|i\alpha\rangle$ or $|-i\alpha\rangle$, the roles of g_u and g_v are reversed. In order to have a solution for F independent of the sign of the imaginary coherent state we fix g_v. Then, we maximize the exponent of F as a function of g_u. The final result is that we obtain the same expressions for g_u and g_v as given before for the real case and the following expression for the fidelity:

$$\begin{aligned} F^{\mathrm{im}}(r,\theta) =& \sqrt{1-\cos^2(2\theta)\tanh^4 r} \\ & \times \exp\left\{\frac{-\alpha^2\{\cosh r + \sinh r[\cos(2\theta)\tanh r - \sin(2\theta)]\}^2}{\cosh^2 r + \cos(2\theta)\sinh^2 r}\right\}. \end{aligned} \tag{30}$$

Comparing both expressions for the fidelity we see that

$$F^{\mathrm{re}}(r,\theta) = F^{\mathrm{im}}(r,\pi/2-\theta). \tag{31}$$

The final calculations needed to determine the optimal r and θ are as follows. We want r and θ such that if Alice chooses the real basis and Bob assumes Alice chose the real basis, F^{re} is maximal and F^{im} is minimal. This is achieved maximizing the following function:

$$\Pi^{\mathrm{re}}(r,\theta) = F^{\mathrm{re}}(r,\theta)[1-F^{\mathrm{im}}(r,\theta)]. \tag{32}$$

It is not possible, however, to analytically solve the optimization problem associated to Eq. (32) and get simple closed expressions for the optimal r and θ. Thus, the maximization of Eq. (32) is carried out numerically once the value of α is specified. This is what was done to get the optimal data shown in figure 2 of the main text.

The optimal parameters if Alice chooses the imaginary basis and Bob assumes Alice chose the imaginary basis is obtained imposing that F^{re} be minimal and F^{im} be maximal. This is obtained maximizing the following function:

$$\Pi^{\mathrm{im}}(r,\theta) = F^{\mathrm{im}}(r,\theta)[1-F^{\mathrm{re}}(r,\theta)] = \Pi^{\mathrm{re}}(r,\pi/2-\theta). \tag{33}$$

It is clear by the last equality that the optimal θ for the imaginary input is obtained from the optimal one for the real input by subtracting it from $\pi/2$. The relations between the optimal settings for the real and imaginary inputs are as follows:

$$\theta^{\mathrm{re}} = \pi/2 - \theta^{\mathrm{im}}, \tag{34}$$

$$g_v^{\mathrm{re}} = g_u^{\mathrm{im}}, \tag{35}$$

$$g_u^{\mathrm{re}} = g_v^{\mathrm{im}}, \tag{36}$$

$$r^{\mathrm{re}} = r^{\mathrm{im}}. \tag{37}$$

B.2 Key generation analysis

The state with Bob after finishing the teleportation protocol is given by equation (20), where he has already implemented either the real or imaginary displacement on his mode. By real and imaginary displacements we mean that Bob applied the displacement $\hat{D}(\lambda)$, with $\lambda = g_u\tilde{x}_u + ig_v\tilde{p}_v$, using either the real (g_u^{re} and g_v^{re}) or imaginary (g_u^{im} and g_v^{im}) optimal parameters.

In the next step of the teleportation-based CVQKD protocol, he implements another displacement, which depends on whether he chose the real or imaginary displacement. For a previously real displaced mode he now applies the displacement $\hat{D}(\alpha)$ and for a previously imaginary displaced mode he applies $\hat{D}(i\alpha)$. The goal of these last displacements is to transform states nearly described by $|-\alpha\rangle$ or $|-i\alpha\rangle$ to vacuum states and to push further away from the vacuum the states $|\alpha\rangle$ or $|i\alpha\rangle$. Note that Bob's state will be very close to one of those four states only if the "matching condition" occurred, i.e., if Alice teleported a real (imaginary) state and Bob used the optimal settings presuming a real (imaginary) input by Alice.

Mathematically, the state after the last displacement is

$$|\tilde{\chi}\rangle = \hat{D}(\gamma)|\chi\rangle, \tag{38}$$

where $\gamma = \alpha$ or $\gamma = i\alpha$. The probability to detect the vacuum state is

$$Q_0^B = |\langle 0|\tilde{\chi}\rangle|^2 = |\langle -\gamma|\chi\rangle|^2 = \left| \int dx_3 \varphi_{-\gamma}^*(x_3)\chi(x_3) \right|^2, \tag{39}$$

where we used that $\hat{D}(\gamma) = \hat{D}^\dagger(-\gamma)$ and $\langle 0|\hat{D}(\gamma) = \langle -\gamma|$. In equation (39) $\varphi_{-\gamma}^*(x_3)$ is the complex conjugate of (23), with the subscript $-\gamma$ as a reminder to which coherent state the kernel $\varphi(x_3)$ refers to, and $\chi(x_3)$ is given by equation (20).

Figure 3 in the main text is a plot of Q_0^B for all possible combinations of input state by Alice and displacement by Bob when a matching condition occurs (the first four curves from top to bottom). The fifth and sixth curves are Q_0^B averaged over all possible measurement outcomes $\tilde{x}_u$ and $\tilde{p}_v$ for Alice, weighted by Alice's probability to get $\tilde{x}_u$ and $\tilde{p}_v$ (cf. equation (17)),

$$q_0^B = \int d\tilde{p}_v d\tilde{x}_u \mathrm{p}(\tilde{p}_v, \tilde{x}_u) Q_0^B(\tilde{p}_v, \tilde{x}_u). \tag{40}$$

This averaging is needed whenever the matching condition does not occur since Q_0^B depends on $\tilde{x}_u$ and $\tilde{p}_v$ in this case. See figure 8 for a reproduction of figure 3 of the main text but this time with a different caption, where we employ the notation just developed to describe each one of the plotted curves.

We have also tested the robustness of the optimal settings by randomly and independently changing the optimal parameters about their correct values. As can be seen in figure 9, the optimal settings are very robust, supporting fluctuations of ±2% about the optimal values for small and large α. For small α fluctuations of ±10% is still tolerable.

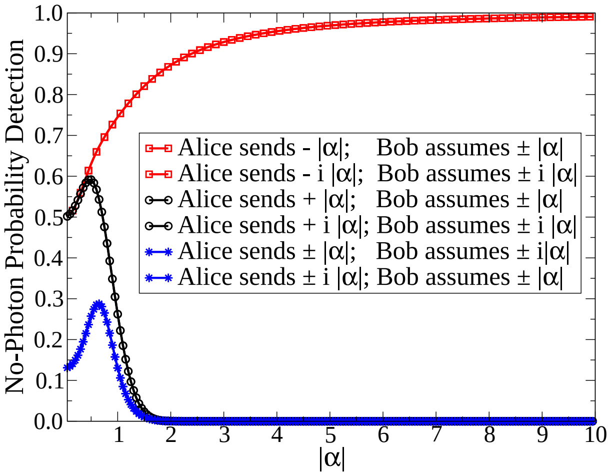

Fig. 8 The first curve is Q_0^B computed with the following parameters, Alice's input $= |-\alpha\rangle, r^{\text{re}}, \theta^{\text{re}}, \lambda = g_u^{\text{re}}\tilde{x}_u + ig_v^{\text{re}}\tilde{p}_v, \gamma = \alpha$. The second curve is Q_0^B for Alice's input $= |-i\alpha\rangle, r^{\text{im}}, \theta^{\text{im}}, \lambda = g_u^{\text{im}}\tilde{x}_u + ig_v^{\text{im}}\tilde{p}_v, \gamma = i\alpha$. The third curve is Q_0^B for Alice's input $= |\alpha\rangle, r^{\text{re}}, \theta^{\text{re}}, \lambda = g_u^{\text{re}}\tilde{x}_u + ig_v^{\text{re}}\tilde{p}_v, \gamma = \alpha$. The fourth curve is Q_0^B for Alice's input $= |i\alpha\rangle, r^{\text{im}}, \theta^{\text{im}}, \lambda = g_u^{\text{im}}\tilde{x}_u + ig_v^{\text{im}}\tilde{p}_v, \gamma = i\alpha$. The fifth curve is the averaged Q_0^B for Alice's input $= |\pm\alpha\rangle, r^{\text{re}}, \theta^{\text{re}}, \lambda = g_u^{\text{im}}\tilde{x}_u + ig_v^{\text{im}}\tilde{p}_v, \gamma = i\alpha$. The sixth curve is the averaged Q_0^B for Alice's input $= |\pm i\alpha\rangle, r^{\text{im}}, \theta^{\text{im}}, \lambda = g_u^{\text{re}}\tilde{x}_u + ig_v^{\text{re}}\tilde{p}_v, \gamma = \alpha$.

C Security analysis

We want to study how the teleportation-based CVQKD protocol responds to a lossy channel, or equivalently, to the BS attack. This will allow us to determine the level of loss in which a secure key can be extracted via direct reconciliation and no postselection.

C.1 Lossy channel or the presence of Eve

We want to investigate the security of the present scheme to the BS attack. In the BS attack an eavesdropper (Eve) inserts a BS of transmittance η, $0 \leq \eta \leq 1$, during the transmission to Bob of his share of the entangled two-mode squeezed state (mode 3 in figure 1). In this case Bob will receive a signal with intensity η and Eve the rest. With her share of the signal, $1-\eta$, Eve proceeds as Bob in order to extract information of the key.

The BS is inserted before Bob receives his mode and therefore before he applies the displacements $\hat{D}(\lambda)$ and $\hat{D}(\gamma)$, with $\gamma = \alpha$ or $i\alpha$. Bob's state before the insertion of the BS is $|\chi'\rangle$ as given in equation (16). Hence, the joint state of Bob and Eve before the BS is

$$|\Omega\rangle = |\chi'\rangle|0\rangle = \int dx_3dx_4\langle x_3|\chi'\rangle\langle x_4|0\rangle|x_3\rangle|x_4\rangle = \int dx_3dx_4\chi'(x_3)\varphi_0(x_4)|x_3,x_4\rangle, \quad (41)$$

with $\varphi_0(x_4)$ given by Eq. (23) with $\alpha = 0$. But since

$$\hat{B}_{34}(\eta)|x_3,x_4\rangle = \left|\sqrt{\eta}x_3 - \sqrt{1-\eta}x_4, \sqrt{1-\eta}x_3 + \sqrt{\eta}x_4\right\rangle \quad (42)$$

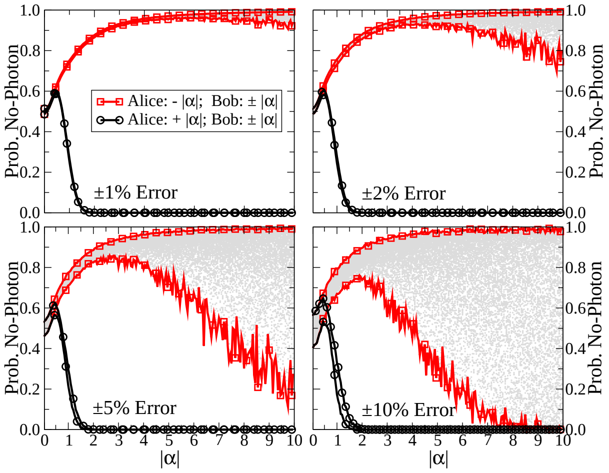

Fig. 9 For each value of α we have implemented 100 realizations of random fluctuations about the input state, about the optimal values r, θ, g_v, g_u, and about γ. We worked with Alice's sending a real state and Bob assuming a real state. Similar results are obtained for the imaginary matching condition. The red/square curves connects the maximal and minimal values for q_0^B due to the random fluctuations assuming Alice sent a negative real state. The gray dots between the red/square curves represent the value of q_0^B at each realization. The black/circle curves has the same meaning of the red/square curves but assuming Alice sent a positive real state.

we have after the BS,

$$\begin{aligned}|\Omega\rangle &= \hat{B}_{34}(\eta)|\chi'\rangle_3|0\rangle_4\\ &= \int dx_3 dx_4 \chi'(x_3)\varphi_0(x_4)\left|\sqrt{\eta}x_3 - \sqrt{1-\eta}x_4, \sqrt{1-\eta}x_3 + \sqrt{\eta}x_4\right\rangle,\\ &= \int dx_3 dx_4 \chi'(\sqrt{\eta}x_3 + \sqrt{1-\eta}x_4)\varphi_0(\sqrt{\eta}x_4 - \sqrt{1-\eta}x_3)|x_3, x_4\rangle.\end{aligned} \tag{43}$$

The last equality was obtained making the following change of variables, $x_3 \to \sqrt{\eta}x_3 + \sqrt{1-\eta}x_4$ and $x_4 \to \sqrt{\eta}x_4 - \sqrt{1-\eta}x_3$. Bob's state after the BS is given by the partial trace of the state $\rho_{BE} = |\Omega\rangle\langle\Omega|$ with respect to Eve's mode, $\rho'_B = \mathrm{tr}_E(\rho_{BE})$. In the position basis we have

$$\rho'_B = \int dx_4 \langle x_4|\rho_{BE}|x_4\rangle = \int dx_3 dx'_3 \rho'_B(x_3, x'_3)|x_3\rangle\langle x'_3| \tag{44}$$

where

$$\begin{aligned}\rho'_B(x_3, x'_3) = &\int dx_4 \chi'(\sqrt{\eta}x_3 + \sqrt{1-\eta}x_4)\chi'^*(\sqrt{\eta}x'_3 + \sqrt{1-\eta}x_4)\\ &\times\varphi_0(\sqrt{\eta}x_4 - \sqrt{1-\eta}x_3)\varphi_0^*(\sqrt{\eta}x_4 - \sqrt{1-\eta}x'_3).\end{aligned} \tag{45}$$

Note that Eve's state is $\rho'_E = \mathrm{tr}_B(\rho_{BE})$, which is simply obtained from equation (45) by changing $\eta \to 1 - \eta$.

Using the state ρ'_B (ρ'_E) Bob (Eve) proceeds as explained before to finish all the steps of a single run of the teleportation-based CVQKD protocol. Bob displaces his mode by λ, which depends on whether he assumed Alice teleported a real or imaginary state, finishing the teleportation stage of the protocol. His state at this stage is $\rho_B = \hat{D}(\lambda)\rho'_B\hat{D}^\dagger(\lambda)$. Then he implements the last displacement $\hat{D}(\gamma)$, which depends on his first displacement as explained before, and measures the intensity of his mode. Hence, Bob's probability to detect the vacuum state (no-light) is

$$Q_0^B(\tilde{p}_v, \tilde{x}_u) = \text{tr}\,[|0\rangle\langle 0|\,\hat{D}(\gamma)\rho_B\hat{D}^\dagger(\gamma)] = \langle -\lambda-\gamma|\rho'_B|-\lambda-\gamma\rangle, \tag{46}$$

where we have made explicit that Q_0^B depends on the measurement outcomes of Alice when $\eta \neq 1$, i.e., when we have a lossy channel. In the position representation we have

$$Q_0^B(\tilde{p}_v, \tilde{x}_u) = \int dx_3 dx'_3 \varphi^*_{-\lambda-\gamma}(x_3)\rho'_B(x_3, x'_3)\varphi_{\,-\lambda-\gamma}(x'_3). \tag{47}$$

As before, we define the unconditional (no postselection) probability as

$$q_0^B = \int d\tilde{p}_v d\tilde{x}_u \mathrm{p}(\tilde{p}_v, \tilde{x}_u) Q_0^B(\tilde{p}_v, \tilde{x}_u) \tag{48}$$

and in figure 10 we show its value for several values of loss.

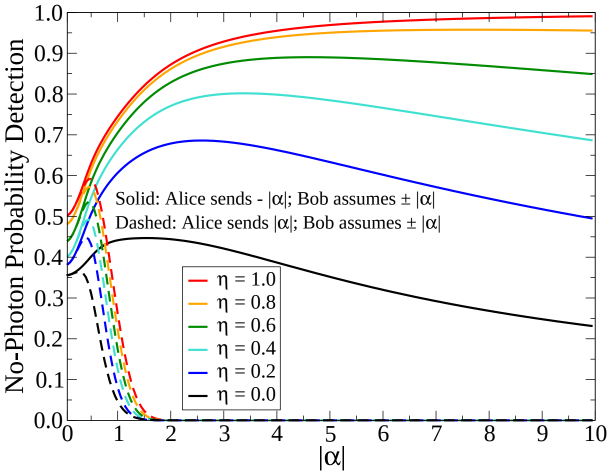

Fig. 10 Probability q_0^B to detect the vacuum state for several values of loss $(1-\eta)$, which increases (η decreases) from top to bottom. The other parameters used to compute q_0^B, namely, r, θ, g_v, g_u, and γ, were the optimal ones when the matching condition occurs. The remaining parameter, Alice's input, was set to $-\alpha$ (solid lines) and α (dashed lines).

C.2 Secure key rates

For direct reconciliation the secure key rate between Alice and Bob is

$$K = \max\{0, \beta I_{AB} - I_{AE}\} = \{0, \Delta I\}, \tag{49}$$

where β is the reconciliation efficiency, I_{AB} the mutual information between Alice and Bob, and I_{AE} the mutual information between Alice and Eve. In what follows we will prepare the ground for defining and computing those mutual informations for our problem. Also, since the present teleportation-based CVQKD protocol is symmetric to both matching conditions, we will work with the one where Alice teleported a real state and Bob implemented the real displacement.

Let X and Y be two binary discrete variables, whose possible values for X are $x = 0, 1$ and for Y are $y = 0, 1$. If we associate variable X to Alice and adopt the convention $\{-|\alpha\rangle, |\alpha\rangle\} = \{0, 1\}$ we have

$$P_X(0) = P_X(1) = 1/2, \tag{50}$$

where $P_X(x)$ is the probability distribution associated to X. This means that Alice randomly chooses between the negative or positive coherent states at each run of the protocol.

If we associate variable Y to Bob we can define the conditional probability of Bob assigning the value y to his variable if Alice assigned the value x as $P_{Y|X}(y|x)$. For the present protocol, and according to the encoding that Alice and Bob mutually agreed on for the key, the four conditional probabilities are

$$P_{Y|X}(0|0) = q_0^B(-\alpha), \tag{51}$$

$$P_{Y|X}(1|0) = 1 - q_0^B(-\alpha), \tag{52}$$

$$P_{Y|X}(0|1) = q_0^B(\alpha), \tag{53}$$

$$P_{Y|X}(1|1) = 1 - q_0^B(\alpha), \tag{54}$$

where q_0^B, the probability to detect the vacuum state, is given by equation (48). If we define

$$q_1^B(\alpha) = 1 - q_0^B(\alpha), \tag{55}$$

where q_1^B is the probability to detect light, we have

$$P_{Y|X}(0|0) = q_0^B(-\alpha), \tag{56}$$

$$P_{Y|X}(1|0) = 1 - q_0^B(-\alpha), \tag{57}$$

$$P_{Y|X}(0|1) = 1 - q_1^B(\alpha), \tag{58}$$

$$P_{Y|X}(1|1) = q_1^B(\alpha). \tag{59}$$

Note that we have explicitly written the dependence of q_j^B, $j = 0, 1$, on Alice's teleported state to remind us that we should compute it using the appropriate sign for α.

We can understand the previous conditional probabilities as follows. If Alice teleports the state $|-\alpha\rangle$ (bit 0) and Bob displaces his mode by α, for a faithful teleportation he will likely detect the vacuum state after that final displacement and assign correctly the bit 0. The chance for that happening is quantified by $P_{Y|X}(0|0) = q_0^B(-\alpha)$. He will obviously make a mistake, assigning erroneously the bit 1, if he does not detect the vacuum state. For that reason we have $P_{Y|X}(1|0) = 1 - q_0^B(-\alpha)$. In the same fashion, if Alice teleports the state $|\alpha\rangle$ (bit 1) and Bob displaces his mode by α, for a faithful teleportation he will very likely not detect the vacuum state and will correctly assign the bit 1. This event occurs with probability $1 - q_0^B(\alpha)$, which implies $P_{Y|X}(1|1) = 1 - q_0^B(\alpha)$. He makes a mistake if he gets the vacuum state and therefore $P_{Y|X}(0|1) = q_0^B(\alpha)$.

Since the conditional probability is related to the joint probability distribution $P_{XY}(x, y)$ by the rule $P_{XY}(x, y) = P_X(x)P_{Y|X}(y|x)$ we have

$$P_{XY}(0, 0) = q_0^B(-\alpha)/2, \tag{60}$$

$$P_{XY}(0, 1) = [1 - q_0^B(-\alpha)]/2, \tag{61}$$

$$P_{XY}(1, 0) = [1 - q_1^B(\alpha)]/2, \tag{62}$$

$$P_{XY}(1, 1) = q_1^B(\alpha)/2. \tag{63}$$

If we now use that $P_Y(y) = \sum_x P_{XY}(x,y)$ we have

$$P_Y(0) = [1 + q_0^B(-\alpha) - q_1^B(\alpha)]/2, \tag{64}$$

$$P_Y(1) = [1 + q_1^B(\alpha) - q_0^B(-\alpha)]/2. \tag{65}$$

The mutual information between Alice and Bob is defined as

$$I_{AB} = \sum_{x=0}^{1}\sum_{y=0}^{1} P_{XY}(x,y)\log_2\left[\frac{P_{XY}(x,y)}{P_X(x)P_Y(y)}\right] \tag{66}$$

and a direct computation using Eqs. (50) and (60)-(65) gives

$$\begin{aligned} I_{AB} &= 1 + [q_0^B \log_2 q_0^B + (1-q_0^B)\log_2(1-q_0^B) + q_1^B\log_2 q_1^B \\ &+(1-q_1^B)\log_2(1-q_1^B)]/2 - [(1+q_0^B-q_1^B)\log_2(1+q_0^B-q_1^B) \\ &+(1+q_1^B-q_0^B)\log_2(1+q_1^B-q_0^B)]/2. \end{aligned} \tag{67}$$

Here we have dropped the $\pm\alpha$ dependence since q_0^B is always computed with $-\alpha$ and q_1^B with α. Note that I_{AB} also depends on r, θ, g_v, g_u, and η. In order to obtain I_{AE} we simply replace η for $1-\eta$ in the expression for I_{AB} since $q_j^B \to q_j^E$ if $\eta \to 1-\eta$.

Using equation (67) and the equivalent one for I_{AE} we can compute the secret key rate K (equation (49)). Figure 4 in the main text was obtained this way, where we employed for each curve a different value for η and for all of them the optimal values of r, θ, g_v, and g_u assuming the real matching condition as given in figure 2 of the main text.

Note that when the loss is precisely 50% no key can be extracted since Bob's and Eve's state are exactly the same, leading to $I_{AB} = I_{AE}$ and $K = 0$. When the loss is exactly 100%, the protocol does not work either. In this case Bob's state is the vacuum state $|0\rangle$, i.e., he receives no signal, and Eve can also operate on a vacuum state instead of the intercepted signal. It is clear, thus, that Bob and Eve will have the same mutual information with Alice and obviously $K = 0$.

This suggests a possible attack on the present protocol whenever we have high losses. Indeed, Eve can work with a vacuum state instead of her share of the intercepted signal since the former is closer to the state with Bob, whose state in a very lossy environment is nearly the vacuum state. Therefore, we have to improve the security analysis when we have great losses in order to handle the fact that Eve can work with both the intercepted signal and the vacuum state. In this situation, the effective secure key rate that can be achieved between Alice and Bob is

$$K_e = \max\{0, \min\{\Delta I, \Delta I_0\}\}, \tag{68}$$

where $\Delta I_0 = \beta I_{AB} - I_{AE}^0$ and I_{AE}^0 is the mutual information between Alice and Eve assuming Eve's state is the vacuum. I_{AE}^0 is easily obtained from the general expression for I_{AE} by setting $\eta = 1.0$, the case where Bob receives the whole signal and Eve gets nothing, i.e., she has the vacuum state.

Table I of the main text was obtained maximizing K_e for several values of fixed r, η, and β. Equations (27) and (28) was used for g_u and g_v and θ was determined in such a way that K_e be maximal. As always, we assumed the real matching condition to fix the remaining parameters needed to evaluate K_e, namely, Alice's input was either $|-\alpha\rangle$ or $|\alpha\rangle$ and Bob's final displacement was $\hat{D}(\alpha)$.

D Further examples

Assuming squeezing is a cheap resource, we can let r, together with θ, be a free parameter in the maximization of the key rate. In this scenario, we get the results in Figs. 11 and 13 for the effective optimal key rates for several values of loss. The optimal parameters leading to such key rates are given in Figs. 12 and 14.

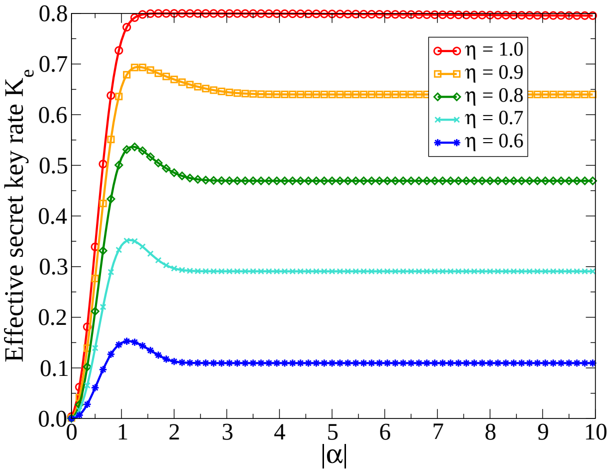

Fig. 11 Here both r and θ are adjusted to get the optimal key rates with $\beta = 0.8$. We assume the real matching condition.

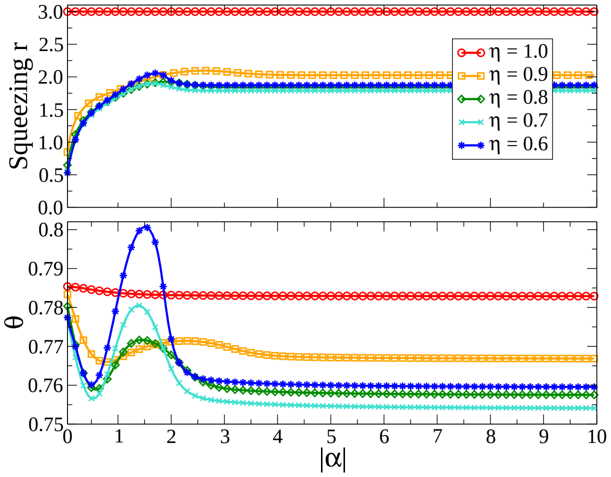

Fig. 12 Optimal parameters leading to the key rates in figure 11. In the maximization process we have restricted r from 0 to 3 while θ could assume any value. The optimal g_u and g_v are obtained using these values of θ and r to evaluate Eqs. (27) and (28).

It is interesting to note that whenever we have loss ($\eta \neq 1.0$) the optimal squeezing is not the greatest value possible. For losses lower than 50% (η from 1.0 to 0.6) the greater the loss the lower the key rate. Interestingly, the behavior for losses greater than 50% is different. Once you cross the border of 50% loss, more loss means a better key rate. But this trend stops at about 70% loss ($\eta = 0.3$), from which the key rate starts to decrease again with loss. When the exact values of 50% or 100% loss is used, no effective key rate can be achieved since Bob and Eve share the same level of information with Alice. We also remark that in most of the cases the optimal squeezing is not greater than $r = 2.0(17.4\text{dB})$.

Finally, it is important to note that for losses lower than 50%, i.e., when more than half of the signal sent from Alice reaches Bob, the effective key rate K_e is simply K as given by

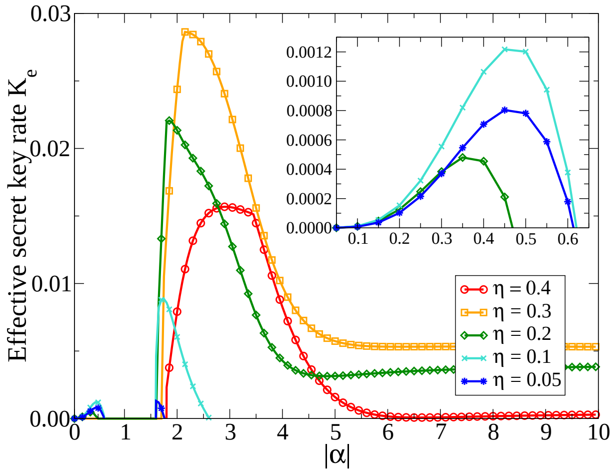

Fig. 13 Here both r and θ are adjusted to get the optimal key rates with $\beta = 0.8$. We assume the real matching condition.

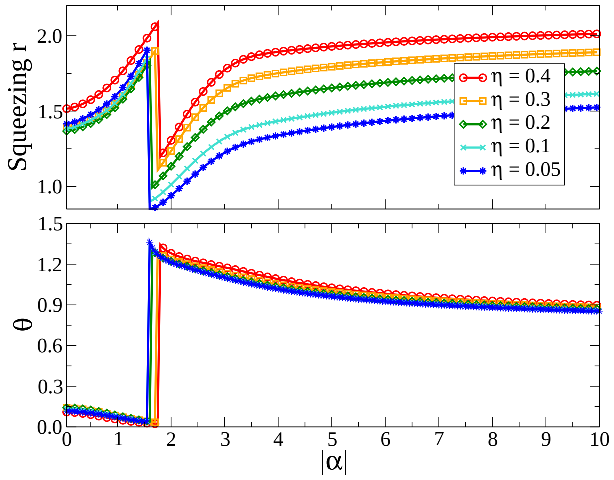

Fig. 14 Optimal parameters leading to the key rates in figure 13. In the maximization process we have restricted r from 0 to 3 while θ could assume any value. The optimal g_u and g_v are obtained using these values of θ and r to evaluate Eqs. (27) and (28).

equation (49). However, when we go beyond the level of 50% loss, equation (68) starts to be relevant. Depending on the value of $|\alpha|$, either $\varDelta I$ or $\varDelta I_0$ is the lowest term that defines the key. That is why in the cases with more than 50% loss the curves for K_e have an abrupt behavior. And for very high loss, $\varDelta I_0$ is always the lowest term.

References

1. Bennett, C. H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing, pp. 175 (1984)
   Ekert, A. K.: Quantum cryptography based on Bells theorem. Phys. Rev. Lett. **67**, 661 (1991); Bennett, C. H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121 (1992); Bennett, C. H., Brassard, G., Mermin, N. D.: Quantum cryptography without Bells theorem. Phys. Rev. Lett. **68**, 557 (1992)
2. Extensive reviews of the discrete variable protocols in [1] and their descendants can be found in: Gisin, N., Ribordy, G., Tittle, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. **74**, 145 (2002); Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301 (2009)
3. Ralph, T. C.: Continuous variable quantum cryptography. Phys. Rev. A **61**, 010303(R) (1999); Hillery, M.: Quantum cryptography with squeezed states. Phys. Rev. A **61**, 022309 (2000); Reid, M. D.: Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations. Phys. Rev. A **62**, 062308 (2000)
4. Cerf, N. J., Lévy, M., Van Assche, G.: Quantum distribution of Gaussian keys using squeezed states. Phys. Rev. A **63**, 052311 (2001)
5. Grosshans, F., Grangier, Ph.: Continuous Variable Quantum Cryptography Using Coherent States. Phys. Rev. Lett. **88**, 057902 (2002)
6. Silberhorn, Ch., Ralph, T. C., Lütkenhaus, N., Leuchs, G.: Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit. Phys. Rev. Lett. **89**, 167901 (2002); Lorenz, S., Korolkova, N., Leuchs, G.: Continuous-variable quantum key distribution using polarization encoding and post selection. Appl. Phys. B **79**, 273 (2004)
7. Grosshans, F., Van Assche, G., Wenger, J., Brouri, R., Cerf, N. J., Grangier, Ph.: Quantum key distribution using gaussian-modulated coherent states. Nature (London) **421**, 238 (2003); Legré, M., Zbinden, H., Gisin, N.: Implementation of continuous variable quantum cryptography in optical fibres using a go-&-return configuration. Quantum Inf. Comput. **6**, 326 (2006); Lodewyck, J., Debuisschert, T., Tualle-Brouri, R., Grangier, Ph.: Controlling excess noise in fiber-optics continuous-variable quantum key distribution. Phys. Rev. A **72**, 050303(R) (2005); Lodewyck, J., Bloch, M., García-Patrón, R., Fossier, S., Karpov, E., Diamanti, E., Debuisschert, T., Cerf, N. J., Tualle-Brouri, R., McLaughlin, S. W., Grangier, Ph.: Quantum key distribution over 25km with an all-fiber continuous-variable system. Phys. Rev. A **76**, 042305 (2007); Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, Ph., Diamanti, E.: Experimental demonstration of long-distance continuous-variable quantum key distribution. Nature Photonics **7**, 378 (2013)
8. Hirano. T., Yamanaka, H., Ashikaga, M., Konishi, T., Namiki, R.: Quantum cryptography using pulsed homodyne detection. Phys. Rev. A **68**, 042331 (2003); Namiki, R., Hirano, T.: Security of quantum cryptography using balanced homodyne detection. Phys. Rev. A **67**, 022308 (2003); Namiki, R., Hirano, T.: Practical Limitation for Continuous-Variable Quantum Cryptography using Coherent States. Phys. Rev. Lett. **92**, 117901 (2004); Namiki, R., Hirano, T.: Efficient-phase-encoding protocols for continuous-variable quantum key distribution using coherent states and postselection. Phys. Rev. A **74**, 032302 (2006)
9. Weedbrook, Ch., Lance,A. M., Bowen, W. P., Symul, Th., Ralph, T. C., Lam, P. K.: Quantum Cryptography Without Switching. Phys. Rev. Lett. **93**, 170504 (2004); Lance, A. M., Symul, Th., Sharma, V., Weedbrook, Ch., Ralph, T. C., Lam, P. K.: No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light. Phys. Rev. Lett. **95**, 180503 (2005)
10. Heid, M., Lütkenhaus, N.: Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. Phs. Rev. A **73** 052316 (2006); Heid, M., Lütkenhaus, N.: Security of coherent-state quantum cryptography in the presence of Gaussian noise. Phs. Rev. A **76** 022313 (2007)

11. Pirandola, S., Mancini, S., Lloyd, S., Braunstein, S. L.: Continuous-variable quantum cryptography using two-way quantum communication. Nature Phys. **4**, 726 (2008)
12. García-Patrón, R., Cerf, N. J.: Continuous-Variable Quantum Key Distribution Protocols Over Noisy Channels. Phys. Rev. Lett. **102**, 130501 (2009)
13. Leverrier, A., Grangier, Ph.: Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation. Phys. Rev. Lett. **102**, 180504 (2009); Leverrier, A., Grangier, Ph.: Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation. Phys. Rev. A **83**, 042312 (2011)
14. Sych, D., Leuchs, G.: Coherent state quantum key distribution with multi letter phase-shift keying. New J. Phys. **12**, 053019 (2010)
15. Madsen, L. S., Usenko, V. C., Lassen, M., Filip, R., Andersen, U. L.: Continuous variable quantum key distribution with modulated entangled states. Nat. Commun. 3:1083 doi: 10.1038/ncomms2097 (2012)
16. Pirandola, S., Ottaviani, C., Spedalieri, G., Weedbrook, Ch., Braunstein, S. L., Lloyd, S., Gehring, T., Jacobsen, Ch. S., Andersen, U. L.: High-rate measurement-device-independent quantum cryptography. Nature Photonics **9**, 397 (2015); Li, Z., Zhang, Y.-C., Xu, F., Peng, X., Guo,H.: Continuous-variable measurement-device-independent quantum key distribution. Phys. Rew. A **89**, 052301 (2014)
17. Borelli, L. F. M., Aguiar, L. S., Roversi, J. A., Vidiella-Barranco, A.: Quantum key distribution using continuous-variable non-Gaussian states. Quantum Inf. Process. **15**, 893 (2016)
18. See [2] and in particular the following references for reviews on CVQKD protocols: Braunstein, S. L., van Loock, P.: Quantum information with continuous variables. Rev. Mod. Phys. **77**, 513 (2005); Weedbrook, Ch., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H., Lloyd, S.: Gaussian quantum information. Rev. Mod. Phys. **84**, 621 (2012)
19. Gottesman, D., Preskill, J.: Secure quantum key distribution using squeezed states. Phys. Rev. A **63**, 022309 (2001); Grosshans, F., Cerf, N. J.: Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks. Phys. Rev. Lett. **92**, 047905 (2004); Iblisdir, S., Van Assche, G., Cerf, N. J.: Security of Quantum Key Distribution with Coherent States and Homodyne Detection. Phys. Rev. Lett. **93**, 170502 (2004); Grosshans, F.: CollectiveAttacks and Unconditional Security in Continuous Variable Quantum KeyDistribution. Phys. Rev. Lett. **94**, 020504 (2005); Navascués, M., Acín, A.: SecurityBounds for Continuous Variables Quantum Key Distribution. Phys. Rev. Lett. **94**, 020505 (2005); Navascués, M., Grosshans, F., Acín, A.: Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. Phys. Rev. Lett. **97**, 190502 (2006); García-Patrón, R., Cerf, N. J.: Unconditional Optimality of Gaussian Attacks against Continuous-Variable Quantum Key Distribution. Phys. Rev. Lett. **97**, 190503 (2006); Renner, R., Cirac, J. I.: de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. Phys. Rev. Lett. **102**, 110504 (2009); Zhao, Y.-B., Heid, M., Rigas, J., Lütkenhaus, N.: Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks. Phys. Rev. A **79**, 012307 (2009); Weedbrook, Ch., Pirandola, S., Lloyd, S., Ralph, T. C.: Quantum Cryptography Approaching the Classical Limit. Phys. Rev. Lett. **105**, 110501 (2010); Leverrier, A., García-Patrón, R., Renner, R., Cerf, N. J.: Security of Continuous-Variable Quantum Key Distribution Against General Attacks. Phys. Rev. Lett. **110**, 030502 (2013); Jouguet, P., Kunz-Jacques, S., Diamanti, E.: Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. Phys. Rev. A **87**, 062313 (2013); Huang, J.-Z., Kunz-Jacques, S., Jouguet, P., Weedbrook, Ch., Yin, Z.-Q., Wang, Sh., Chen, W., Guo, G.-C., Han, Z.-F.: Quantum hacking on quantum key distribution using homodyne detection. Phys. Rev. A **89**, 032304 (2014)
20. Vaidman, L.: Teleportation of quantum states. Phys. Rev. A **49**, 1473 (1994); Braunstein, S. L., Kimble, H. J.: Teleportation of Continuous Quantum Variables. Phys. Rev. Lett. **80**, 869 (1998); Furusawa, A., Sørensen, J. L., Braunstein, S. L., Fuchs, C. A., Kimble, H. J., Polzik, E. S.: Unconditional Quantum Teleportation. Science **282**, 706 (1998)

21. Yoshino, K.-i., Aoki, T., Furusawa, A.: Generation of continuous-wave broadband entangled beams using periodically poled lithium niobate waveguides. Appl. Phys. Lett. **90**, 041111 (2007); Lee, N., Benichi, H., Takeno, Y., Takeda, Sh., Webb, J., Huntington, E., Furusawa, A.: Teleportation of Nonclassical Wave Packets of Light. Science **332**, 330 (2011)
22. Gordon, G., Rigolin, G.: Quantum cryptography using partially entangled states. Opt. Commun. **283**, 184 (2010)
23. Luiz, F. S., Rigolin, G.: Optimal continuous variable quantum teleportation protocol for realistic settings. Annals of Physics **354**, 409 (2015)
24. Becir, A., Wahiddin, M. R. B.: Tight bounds for the eavesdropping collective attacks on general CV-QKD protocols that involve non-maximally entanglement. Quantum Inf. Process. **12**, 1155 (2013)