Composable security of two-way continuous-variable quantum key distribution

Shouvik Ghorai, Eleni Diamanti, and Anthony Leverrier

1LIP6, CNRS, Sorbonne Université, Paris, France
2Inria Paris, France

(Dated: July 2, 2018)

We present a general framework encompassing a number of continuous-variable quantum key distribution protocols, including standard one-way protocols, measurement-device-independent protocols as well as some two-way protocols, or any other continuous-variable protocol involving only a Gaussian modulation of coherent states and heterodyne detection. The main interest of this framework is that the corresponding protocols are all covariant with respect to the action of the unitary group $U(n)$, implying that their security can be established thanks to a Gaussian de Finetti reduction. In particular, we give a composable security proof of two-way continuous-variable quantum key distribution against general attacks. We also prove that no active symmetrization procedure is required for these protocols, which would otherwise make them prohibitively costly to implement.

Quantum key distribution (QKD) allows two distant parties, Alice and Bob with access to an untrusted quantum channel and an authenticated classical channel, to share a secret key which can later be used to encrypt classical messages. The remarkable property of QKD is that its security can be established in the information-theoretic setting, without appealing to any computational assumptions. While the first protocols relied on a discrete encoding of information and required single-photon detectors [1, 2], a new generation of protocols called “continuous-variable” (CV) encode the information on the quadratures of the quantized electromagnetic field, allowing coherent detection to advantageously replace single-photon detection [3]. There is, however, a price to pay for this simplified experimental setup and this is increased difficulty of establishing security proofs due to the fact that the finite-dimensional Hilbert space of discrete-variable QKD has to be replaced by an infinite-dimensional Fock space. Notably, the theoretical tools developed for analyzing discrete-variable protocols – de Finetti theorems [4–6], entropic uncertainty relations [7], entropy accumulation [8] – need not directly work in the CV setting.

Fortunately, some of these proof techniques have been successfully adapted to continuous variables and two one-way CV QKD protocols are now established to be secure against general attacks. These are the no-switching protocol [9] where Alice sends coherent states with a Gaussian modulation and Bob performs heterodyne (or dual-homodyne) detection, and the BB84-inspired protocol of Ref. [10] where Alice sends squeezed states along one of the two quadratures and Bob performs homodyne detection. The security of the latter follows from a continuous-variable version of the entropic uncertainty principle [11] while that of the former protocol is established thanks to a recently developed Gaussian de Finetti theorem [12, 13, 38].

Establishing the security of two-way CV QKD, where Alice and Bob send quantum information back and forth through the channel, has been an outstanding goal in the field and partial progress was obtained in Refs [14–19]. However, to the best of our knowledge, none of these works has proven its security against general attacks in the composable setting. A notable recent result shows that for all two-way CV QKD protocols, it is sufficient to consider collective attacks [19]. Unfortunately, we don’t know how to analyze this restricted class of attacks in the composable setting, the main issue being the difficulty of estimating the covariance matrix of the state shared by Alice and Bob without assuming that this state is Gaussian or admits bounded higher moments for instance.

In the present paper, we explore the possibility of applying the Gaussian de Finetti reduction to CV QKD beyond one-way schemes, for instance to the measurement-device-independent (MDI) CV QKD protocol of Ref. [20], the two-way protocol with Gaussian displacements of Ref. [14] as well as a variant of floodlight (FL) QKD [21, 22]. What makes these protocols particularly noteworthy is that they display a symmetry with respect to the unitary group $U(n)$, where $n$ is the number of rounds of the protocols. This is a significant strengthening of the usual invariance under Alice and Bob randomly permuting their $n$ subsystems in a coordinated fashion. Recall that the standard argument for establishing the security of a protocol is to first remark that it is sufficient to consider attacks displaying the same symmetry as the protocol, and then that the usual de Finetti theorem precisely asserts that permutation-invariant states are close to independent and identically distributed (i.i.d.) states, which correspond to collective attacks [23]. For CV QKD, however, collective attacks remain nontrivial to analyze due to the infinite dimensionality of the Hilbert space. In that case, the stronger $U(n)$-symmetry allows us to exploit the Gaussian de Finetti theorem stating that it is in fact sufficient to consider a class of Gaussian collective attacks, which turn out to be fairly simple to handle.

A potential issue raised by exploiting the invariance under $U(n)$ is whether an active symmetrization must be enforced by Alice and Bob, which would in particular require picking a Haar random matrix in $U(n)$ and make the whole protocol impractical. Here, following the idea of Portmann [24] of dividing the QKD protocol into two parts (first identifying a min-entropy resource, and then
extracting the key), we are able to show that no active symmetrization is needed for our security proof to go through, a result similar to what was known for discrete-variable protocols [5].

In the following, we first describe our general framework and show how it encompasses one-way as well as two-way protocols. Then we explain in which sense they are covariant with respect to the action of the unitary group $U(n)$, and how to exploit the Gaussian de Finetti reduction to show that it is sufficient to analyze Gaussian collective attacks. Finally, we discuss in more detail the case of Gaussian two-way protocols.

A general framework for Gaussian protocols with heterodyne detection. — One-way CV QKD already gives rise to a zoo of different protocols depending on the states sent by Alice (coherent, squeezed or thermal), their modulation (Gaussian, discrete, along one or two quadratures) and Bob’s detection (homodyne or heterodyne): see Ref. [3] for a recent overview of CV protocols. Two-way QKD offers even more possibilities! As a first simplification, let us restrict our attention to the so-called “entanglement-based” (EB) protocols where the honest parties prepare bipartite pure states such as two-mode squeezed vacuum states (TMSS) and exchange optical modes through an untrusted quantum channel. This is without loss of generality since any Prepare-and-Measure (PM) protocol admits an EB version with the same security [25], and it is therefore sufficient to analyze the latter version even if one implements the PM scheme.

Gaussian protocols stand out among all CV protocols because as the ones where Alice and Bob start out by preparing two-mode squeezed vacuum states (TMSS) and only perform Gaussian operations and measurements (homodyne or heterodyne): indeed Gaussian attacks are then asymptotically optimal provided that the covariance matrix of the state shared by the honest parties is known, meaning that the security proof is not composable [26–28]. In this paper, we consider all protocols where Alice and Bob prepare TMSS, possibly perform two-mode squeezing or beamsplitter transformations (as described later) and finally measure their respective modes with heterodyne detection.

The main feature of these protocols is that they are covariant with respect to the action of the unitary group $U(n)$. Let us explain what this means. Given an $n$-mode Fock space with annihilation operators $a=(a_1, \ldots, a_n)$, the unitary group acts on this space by mapping $a$ to $Ua$, and similarly $a^\dagger$ to $Ua^\dagger$, where $a_i^\dagger$ is the creation operator of mode $i$, and $U$ is the complex conjugate of $U$. A beamsplitter of transmittance $t \in [0,1]$ and a two-mode squeezing operator with gain $g \geq 1$ act on a 2-mode Hilbert space with annihilation operators $a$ and $b$ via the respective transformations $[a, a^\dagger, b, b^\dagger]^T \rightarrow B(t)[a, a^\dagger, b, b^\dagger]^T$ and $[a, a^\dagger, b, b^\dagger]^T \rightarrow S(g)[a, a^\dagger, b, b^\dagger]^T$ with [29]:

$$B(t) = \begin{bmatrix} \sqrt{t}a_1 & \sqrt{1-t}a_2 \\ \sqrt{t}b_1 & \sqrt{1-t}b_2 \end{bmatrix}, \quad S(g) = \begin{bmatrix} \sqrt{\frac{g}{1-g}}a_1 & -\sqrt{\frac{g}{1-g}}a_2 \\ \sqrt{\frac{g}{1-g}}b_1 & \sqrt{\frac{g}{1-g}}b_2 \end{bmatrix},$$

and $\sigma_x = [\frac{1}{2} \frac{1}{2} \frac{1}{2} -\frac{1}{2} 0]$. Finally, heterodyne detection is nothing else than a generalized measurement where the POVM elements are given by coherent states, as follows from the resolution of the identity of an $n$-mode Fock space: $1_{\mathcal{M}} = \frac{1}{\pi} \int |\alpha\rangle\langle\alpha|d\alpha$, with $d\alpha$ the uniform measure on $\mathbb{C}^n$. This can be formalized as a quantum-classical map $\mathcal{M}$ defined by $\mathcal{M}(\rho) = \frac{1}{\pi} \int |\alpha\rangle\langle\alpha|\rho|\alpha\rangle\langle\alpha|d\alpha$ where the superscript ‘cl’ means that this is a classical state encoding the value of $\alpha$ and not a coherent state. An important property of beamsplitters, two-mode squeezing and heterodyne detection is that they all commute with the action of the unitary group in the following sense:

$$[S^{\otimes n}, U \otimes \overline{U}] = [B^{\otimes n}, U \otimes \overline{U}] = [\mathcal{M}, \mathcal{U}] = 0, \quad (1)$$

where $S,B$ and $U$ refer to the action of the symplectic operations $S,B$ and $U$ on their corresponding Fock space [30]. For this reason, protocols that start with vacuum states and where the honest parties apply two-mode squeezing (to prepare TMSS or to amplify a signal as in FL QKD), beamsplitters and perform heterodyne measurements will be covariant with respect to $U(n)$ acting as a product of the form $U^{\otimes p} \otimes \overline{U}^{\otimes q}$, where $p+q$ is the total number of modes held by Alice and Bob, for each round of the protocol.

Examples of such CV protocols include the one-way no-switching protocol of Ref. [9] and the two-way protocol with Gaussian displacements of Ref. [14], whose optical schemes are respectively covariant with respect to $U_A \otimes U_B$, and $U_{A_0} \otimes U_{A_2} \otimes U_{B_1} \otimes U_{B_2}$. The second case is displayed on Fig. 1. Our framework also allows for signal amplification thanks to two-mode squeezing similarly to what is done in FL QKD (see Fig. 2).

Security proof with the Gaussian de Finetti reduction. — A QKD protocol typically consists of three different stages: (i) state distribution, (ii) measurement and parameter estimation, (iii) error reconciliation and privacy amplification. State distribution can be modeled in two distinct ways: either by describing how Alice and Bob prepare the state and distribute it using some untrusted quantum channel (or possibly several channels), or by assuming that the state is given to them by the adversary. The goal of the second stage of the protocol is to obtain a min-entropy resource, in the language of Ref. [24]: the modes are measured with heterodyne detection, yielding classical strings, $X$ for Alice and $Y$ for Bob, one of which is then processed to give the raw key $Z = f(X)$, or $Z = f(Y)$, via some key map $f$ [23, 30]. The size of the strings $X,Y$ depends on the number of modes held by the honest parties: $X,Y \in \mathbb{C}^n$ for one-way CV QKD, while $X = (X_1, X_2), Y = (Y_1, Y_2) \in \mathbb{C}^n \times \mathbb{C}^n$ for two-way CV QKD, and $X,Y$ are even triplets of $n$-dimensional vectors in the case of FL protocols (see Fig. 2). Parameter estimation then consists in a test that checks whether the correlations between $X$ and $Y$ are sufficient to imply a lower bound on the smooth min-entropy $H_{\min}^\varepsilon(Z|E)_{RE}$, where $\varepsilon$ is the smoothing parameter and $E$ is the quantum register held by the adversary [23]. If the test passes, the protocol continues, otherwise...
it aborts. As usual, one can consider without loss of generality that the whole state $\rho_{ABE}$ before measurement is pure. The final stage of the protocol transforms this min-entropy resource, $Z$, into a secret key using the standard techniques of QKD: error reconciliation and privacy amplification.

Assuming as usual that error reconciliation and privacy amplification are correctly implemented, it is sufficient to establish the existence of a (smooth) min-entropy resource to prove the security of the protocol [24]. In other words, we simply need to make sure that the probability that the test passes and that the string $X$ has low min-entropy with respect to Eve’s register $E$ should be upper bounded by some small $\varepsilon$.

There are many subtleties involved with CV QKD, one being how to perform the parameter estimation (i.e., the test $T$) in a composable fashion. A possibility introduced in [31] is to postpone the parameter estimation until after error reconciliation, so that one of the parties obtains both $X$ and $Y$ and be able to compute the Gram matrix and perform the test $T$. This is fine since parameter estimation and error reconciliation are classical maps that commute.

What is crucial here is that both $M$ and $T$ commute with the action $U$ of the unitary group. For $T$, this follows from Eq. (1); for $M$, it results from the choice of the region $\Gamma$ of valid Gram matrices, which itself is a consequence of the invariance of the optical setup of the protocol (see Figs 1 and 2). This implies as proven in [6] and [12] that the security of the map $T \circ M$ (and therefore of the overall QKD protocol) can be analyzed by considering only de Finetti states, which in our case are $SU(m,m)$ coherent states if Alice and Bob hold in total $m = d_A + d_B$ modes per round of the protocol. As introduced in Ref. [13], $SU(m,m)$ generalized coherent states are i.i.d. Gaussian states of the form $|\Lambda\rangle^{\otimes n}$ where $|\Lambda\rangle$ is a $2m$-mode Gaussian state parametrized by an $m \times m$ matrix complex $\Lambda = [\Lambda_{i,j}]$ with spectral norm $\|\Lambda\| < 1$ and defined as

$$|\Lambda\rangle = \det(1 - \Lambda \Lambda^\dagger)^{1/2} \exp \left( \sum_{i,j=1}^{m} \Lambda_{ij} a_i^\dagger b_j^\dagger \right) \text{vacuum}$$

where the creation operators of Alice and Bob’s modes are denoted $a_1^\dagger, \ldots, a_m^\dagger, b_1^\dagger, \ldots, b_m^\dagger$. For instance, $SU(1,1)$ coherent states are simply two-mode squeezed vacuum states. In particular, the methods developed in [12] show that $\varepsilon$-security against Gaussian collective attacks then implies $\varepsilon'$-security against general attacks, with $\varepsilon' / \varepsilon = O(n^{m^2})$. In other words, it is sufficient to show that the protocol is secure when the overall pure state $\rho_{ABE}$ at the start of the protocol is a mixture of such $SU(m,m)$ coherent states. For the protocols considered here, $m$ is in general a small constant ($2$ for the no-switching protocol, $4$ for the two-way protocol and $6$ for FL QKD), meaning that the loss in the security parameter can easily be compensated by reducing the final key length by a negligible amount. As an indication that this proof technique is rather tight, recall that the de Finetti reduction of [6] applied to the BB84 protocol yields a ratio $\varepsilon' / \varepsilon = O(n^{15})$ between security against general and collective attacks.

The novelty here compared to [12, 31] is that we restrict our analysis to $T \circ M$ instead of the whole QKD protocol. While the latter doesn’t commute with the unitary group (because of error reconciliation for instance) and one had to symmetrize the state in order to enforce the correct invariance, the min-entropy resource part of the protocol commutes with the action of $U(n)$ and the work of Portman allows us to infer the security of the QKD protocol [24]. For this reason, the proof holds without any need for actively symmetrizing the state, even at the classical level. This settles an open question from Refs [12, 31].

**About MDI CV QKD.** — At first sight, MDI CV QKD doesn’t quite fit our framework since it involves a third node, controlled by Charlie, performing a Bell measurement consisting of homodyning two modes. More precisely, the idea is that both Alice and Bob prepare a two-mode squeezed vacuum state, keep one mode each and send their other mode to Charlie who performs entanglement swapping, publicly announcing the results of his Bell measurement, and allowing Alice and Bob to conditionally displace their remaining mode in order to create some correlations [20]. In this scenario, one could a priori consider that there are four optical modes: one for Alice, one for Bob and two measured by Charlie, hinting that one should appeal to a proof technique similar to that of two-way CV QKD. This is for instance an approach followed in [32] where it was realized that this
scheme has the advantage of not requiring much public communication for parameter estimation. However, this description doesn’t seem compatible with the Gaussian de Finetti reduction since the homodyne detection performed by Charlie breaks the invariance of the protocol under the group $U(n)$. An alternative approach is to view this scheme as a special case of one-way CV QKD by treating Charlie’s communication as part of the state distribution: once Alice and Bob’s displacements have been performed, the two honest parties are left with a bipartite two-mode quantum state, i.e., with one mode each. This is the same situation as after state distribution in the EB version of the no-switching protocol [9]. In this sense, while MDI CV QKD is implemented similarly as a two-way CV QKD protocol, its security can be analyzed as a one-way CV QKD, with a Gaussian de Finetti reduction involving $SU(2,2)$ coherent states. In particular, the reduction from Ref. [12] together with the security proof of Ref. [31] establish the security of MDI CV QKD against general attacks (see also [33]).

**An example: two-way Gaussian CV QKD with heterodyne detection.**—The PM version of the protocol is as follows: Alice sends coherent states with a Gaussian modulation to Bob, who performs a random Gaussian displacement to the mode he receives and sends it back through the quantum channel. Alice measures the output mode with heterodyne detection, and computes a weighted sum of this result and the value of her initial coherent state. This serves as the raw key. The weights in the sum as well as the variances of the Gaussian distribution should be optimized to yield the maximum key rate. Note that this protocol differs a little bit from the one of Ref. [14] in that here Bob always performs a displacement (no Off-configuration), that the weights of the sum are optimized and that Bob also exploits the second output of his beamsplitter to guess the raw key. The setup of the corresponding EB version is depicted on Fig. 1.

If the quantum channels are covariant with respect to the action of the unitary group, as expected for instance in the case of a passive adversary and a bosonic phase-insensitive channel, then the covariance matrix of the state $\rho_{A_1,A_2,B_1,B_2}$ is invariant under $U_{A_1} \otimes U_{A_2} \otimes U_{B_1} \otimes U_{B_2}$, as detailed in Appendix A 1. For this protocol, the set $\Gamma$ of acceptable covariance matrices will therefore satisfy the same symmetry. This implies that the Gaussian de Finetti reduction can be applied to provide a composable security proof against general attacks. In particular, this means that Gaussian attacks, described by $SU(4,4)$ generalized coherent states, are asymptotically optimal and that the asymptotic key rate can be computed with standard techniques [29]: see Appendix B for details.

**About Floodlight (FL) QKD.**—FL QKD offers the perspective of much higher key rates than traditional QKD at metropolitan range by exploiting multimode encoding and employing signal amplification techniques to compensate for the extra losses present in two-way QKD compared to one-way QKD. However, establishing the security of this scheme has proven challenging. Here, we note that variants of FL QKD fit our framework, provided that the encoding is done through a random Gaussian displacement by Bob, instead of applying a random phase to the signal. Indeed, such a (binary) phase-shift breaks the $U(n)$-symmetry of the protocol. A description of such a Gaussian protocol appears on Fig. 2. There are two additional elements compared to two-way CV QKD: Alice attenuates her signal before sending it through the quantum channel with a beamsplitter, and Bob is allowed to amplify his signal with a two-mode squeezers before sending it back to Alice. In total, both Alice and Bob hold three optical modes for each of the $n$ instances, and the protocol is invariant under the action of the unitary group $U(n)$ acting as $U_{A_1} \otimes U_{A_2} \otimes U_{B_1} \otimes U_{B_2} \otimes U_{B_3}$. In particular, this implies that one can use the Gaussian de Finetti reduction to reduce the security proof to considering Gaussian attacks, parametrized by $SU(6,6)$ generalized coherent states.

**Conclusion.**—In this work, we considered a large class of CV QKD protocols which are invariant with respect to the unitary group $U(n)$ and showed that it is sufficient to establish their security against Gaussian collective attacks. This extends the results of Ref. [12] to two-way protocols which are known to display improved
tolerance to noise compared to the no-switching protocol, and provides the first composable security proof for two-way CV QKD protocols against general attacks. Moreover, by exploiting the modularity of the QKD protocols as introduced by Portmann, we proved that active symmetrization of the data is not needed to apply the de Finetti reduction and to obtain security.

Acknowledgments

We acknowledge funding from European Union’s Horizon 2020 research and innovation programme under the Marie Skodowska-Curie grant agreement No 675662 and French National Research Agency (ANR) projects QRYPTOS, quBIC.

[1] C. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems and Signal Processing (1984), vol. 175.
[2] A. Ekert, Phys. Rev. Lett. 67, 661 (1991).
[3] E. Diamanti and A. Leverrier, Entropy 17, 6072 (2015).
[4] M. Christandl, R. König, G. Mitchison, and R. Renner, Comm. Math. Phys. 273, 473 (2007).
[5] R. Renner, Nat. Phys. 3, 645 (2007).
[6] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. 102, 020504 (2009).
[7] M. Tomamichel and R. Renner, Phys. Rev. Lett. 106, 110506 (2011).
[8] F. Dupuis, O. Fawzi, and R. Renner, arXiv preprint 1607.01796 (2016).
[9] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. 93, 170504 (2004).
[10] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A 63, 052311 (2001).
[11] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. 109, 100502 (2012).
[12] A. Leverrier, Phys. Rev. Lett. 118, 200501 (2017).
[13] A. Leverrier, Journal of Mathematical Physics 59, 042202 (2018).
[14] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nat. Phys. 4, 726 (2008).
[15] M. Sun, X. Peng, Y. Shen, and H. Guo, International Journal of Quantum Information 10, 1250059 (2012).
[16] Y.-C. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, M. Sun, X. Peng, and H. Guo, J. Phys. B 47, 035501 (2014).
[17] C. Ottaviani, S. Mancini, and S. Pirandola, Phys. Rev. A 92, 062323 (2015).
[18] C. Ottaviani and S. Pirandola, Scientific Reports 6, 22225 (2016).
[19] Q. Zhuang, Z. Zhang, N. Lütkenhaus, and J. H. Shapiro, arXiv preprint arXiv:1805.10314 (2018).
[20] 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).
[21] Q. Zhuang, Z. Zhang, J. Dove, F. N. Wong, and J. H. Shapiro, Phys. Rev. A 94, 012322 (2016).
[22] Z. Zhang, Q. Zhuang, F. N. Wong, and J. H. Shapiro, Phys. Rev. A 95, 012332 (2017).
[23] R. Renner, International Journal of Quantum Information 6, 1 (2008).
[24] C. Portmann, arXiv preprint arXiv:1705.10595 (2017).
[25] F. Grosshans, N. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Information and Computation 3, 535 (2003).
[26] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. 96, 080502 (2006).
[27] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. 97, 190503 (2006).
[28] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. 97, 190502 (2006).
[29] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. 84, 621 (2012).
[30] P. J. Coles, E. M. Metodiev, and N. Lütkenhaus, Nat. Comm. 7, 11712 (2016).
[31] A. Leverrier, Phys. Rev. Lett. 114, 070501 (2015).
[32] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. Lett. 120, 220505 (2018).
[33] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. A 97, 052327 (2018).
[34] R. Renner and J. I. Cirac, Phys. Rev. Lett. 102, 110504 (2009).
[35] C. Weedbrook, C. Ottaviani, and S. Pirandola, Phys. Rev. A 89, 012309 (2014).
[36] J. Eisert, S. Scheel, and M. B. Plenio, Phys. Rev. Lett. 89, 137903 (2002).
[37] I. Devetak and A. Winter, in Proc. R. Soc. A (2005), vol. 461, pp. 207–235.
[38] Alternatively, one can obtain a security proof for this specific protocol with a worse key rate in the finite-size regime by first reducing the problem to that of collective attacks using an exponential version of de Finetti theorem [34] and then establishing the security of the protocol against collective attacks in a composable setting [31].
[39] We abuse notation slightly in Eq. (1) by considering that 𝔅 applies to |αcl⟩ is the obvious way, that is, by mapping |αcl⟩ to |Uαcl⟩.
Appendix

In this appendix, we first study in detail in Section A why the two-way and the FloodLight CV QKD protocols respect the symmetry of the unitary group $U(n)$. Then for completeness, we provide in Section B the explicit calculations of the asymptotic secret key rate of our version of the two-way protocol;

Appendix A: Symmetry of the two-way and floodlight protocols with respect to $U(n)$.

1. Two-way protocol

To show that the protocol is covariant with respect to the action of $U(n)$, when the quantum channel is assumed to display this symmetry, one can use the commutation relations

$$[S^\otimes n, U \otimes U] = [B^\otimes n, U \otimes U] = [M, U] = 0.$$ 

But it is easier to see it graphically: first Alice and Bob can each apply $U \otimes U$ to their initial vacuum states (before their respective two-mode squeezed state) without changing the protocol. Then one can follow how these maps propagate through the circuit, as depicted on Fig. 3.

![Graphical depiction of the two-way protocol](image)

FIG. 3: Propagation of the unitaries through the circuit of the two-way protocol.

2. Floodlight protocol

The analysis is similar to the case of two-way CV QKD: one simply follows the propagation of unitaries through the quantum circuit, as depicted on Fig. 4.
(a) Unitaries applied to vacuum

(b) Commutation with initial squeezers

(c) Commutation with Alice’s beamsplitter

(d) Covariance of the forward channel

(e) Commutation with Bob’s beamsplitter

(f) Commutation with Bob’s second squeezer

(g) Covariance of the backward channel

FIG. 4: Propagation of the unitaries through the circuit of the FL protocol.
Appendix B: Secret key rate of the two-way protocol

We have seen in the main text how to analyze the security of some Gaussian CV QKD protocols. Such an analysis doesn’t require any assumption about the untrusted quantum channels controlled by the adversary. In order to assess the performance of QKD protocols, however, it is necessary to provide a (realistic) model of the expected quantum channels. In the context of continuous-variable communication, a standard approach is to model the quantum channels via thermal bosonic channels. Such channels are parametrized by two quantities corresponding to loss and noise: \( \tau \in [0, 1] \) is the transmittance of the channel and \( \xi \geq 0 \) is the so-called excess noise. With these notations, preparing an initial TMSS with covariance matrix
\[
\begin{bmatrix}
V_{12} & \sqrt{V_{12} - 1} \sigma_z \\
\sqrt{V_{12} - 1} \sigma_z & V_{12}
\end{bmatrix}
\]
and sending the second mode through the channel of parameters \((\tau, \xi)\) yields a Gaussian state with covariance matrix
\[
\begin{bmatrix}
V_{12} & \sqrt{\tau V_{12} - 1} \sigma_z \\
\sqrt{\tau V_{12} - 1} \sigma_z & \tau V_{12} (\tau V_{12} - 1 + \xi) + 1
\end{bmatrix}
\]
where \( \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \).

In this section, we review how to estimate the (asymptotic) secret key rate of this protocol. Similar analyses can be found in Refs [14, 17, 18, 35] for instance.

We use the notations depicted on Fig. 5. Alice and Bob each start with a two-mode squeezed vacuum state, of respective variances \( V_A \) and \( V_B \). Alice sends one mode \((A_1')\) through the quantum channel and Bob mixes one of his modes \((B_1')\) together with the output of the quantum channel \((C_1)\) on a beamsplitter of transmittance \( T \). Bob then sends back one of the output modes back through the quantum channel. Alice finally performs a two-mode squeezing operation with squeezing \( g \) on her two modes. All the mode are measured with heterodyne detection, and we choose the outcome corresponding to mode \( A_2 \) to be the raw key. The values of the three squeezing operations and of the beamsplitter are optimized so as to maximize the secret key rate.

\[
\begin{align*}
V_A &= v + 1, \\
V_B &= v' + 1
\end{align*}
\]

\[
\begin{align*}
z &= \sqrt{v^2 + 2v}, \\
z' &= \sqrt{v'^2 + 2v'}
\end{align*}
\]

For the purpose of assessing the performance of the protocol, it is useful to compute the key rate in realistic conditions. Here, we choose to model the quantum channels by thermal channels with transmittance \( \tau \) and excess noise \( \xi \).

Let us follow the notations of Fig. 5 and compute the various covariance matrices, the one of interest being \( \Gamma_{A_1 A_2 B_1 B_2} \). We also use the following conventions:

\[
\begin{align*}
\Gamma_{A_1 A_2 B_1 B_2} &= 1_4 + \begin{bmatrix}
v & z \\
z & v
\end{bmatrix}
\begin{bmatrix}
v' & z' \\
z' & v'
\end{bmatrix}
\end{align*}
\]

where we omit the zeroes in the matrices.

**FIG. 5:** Description of the two-way protocol.
Mode $A'_1$ goes through the quantum channel $(\tau, \xi)$, yielding:

$$\Gamma_{A'_1C_1B_1B'_1} = I_4 + \begin{bmatrix} v & \sqrt{T}z \\ \sqrt{T}z & \tau(v + \xi) \\ v' & z' \\ z' & v' \end{bmatrix}.$$

The beamsplitter interaction gives

$$\Gamma_{A'_1C_2B_2B_1} = \left( I_2 \oplus \left[ \begin{array}{cc} \sqrt{T}I_2 & \sqrt{1-T}I_2 \\ -\sqrt{1-T}I_2 & \sqrt{T}I_2 \end{array} \right] \oplus I_2 \right) \Gamma_{A_1C_1B_1B_1} \left( I_2 \oplus \left[ \begin{array}{cc} \sqrt{T}I_2 & -\sqrt{1-T}I_2 \\ \sqrt{1-T}I_2 & \sqrt{T}I_2 \end{array} \right] \oplus I_2 \right)$$

$$= I_4 + \begin{bmatrix} v & \sqrt{T}z \\ \sqrt{T}z & -\sqrt{(1-T)T}z \\ T\tau(v + \xi) + (1-T)v' & -\sqrt{T(1-T)}(\tau(v + \xi) - v') \\ (1-T)\tau(v + \xi) + Tv' & \sqrt{(1-T)z'} \end{bmatrix}.$$

Since the matrices are symmetric, we simply write $*$ in the bottom left matrix to improve the readability.

Now mode $C_2$ goes back through the quantum channel $(\tau, \xi)$. One obtains:

$$\Gamma_{A'_1C'_2B_2B_1} = I_4 + \begin{bmatrix} v & \sqrt{T}z \\ \sqrt{T}z & -\sqrt{(1-T)T}z \\ T\tau^2(v + \xi) + (1-T)\tau v' + \tau \xi & -\sqrt{T(1-T)}\tau(v + \xi) - v' \\ (1-T)\tau(v + \xi) + Tv' & \sqrt{(1-T)z'} \end{bmatrix}$$

$$= I_4 + \begin{bmatrix} v & z_1 & z_2 \\ * & v_1 & z_1' \\ * & v_2 & z_2' \\ * & * & v' \end{bmatrix} = \begin{bmatrix} V & z_1 & z_2 \\ * & V_1 & z_1' \\ * & V_2 & z_2' \\ * & * & V' \end{bmatrix}$$

with

- $v_1 := T\tau^2(v + \xi) + (1-T)\tau v' + \tau \xi$
- $v_2 := (1-T)\tau(v + \xi) + Tv'$
- $z_1 := \sqrt{T}z$
- $z_2 := -\sqrt{(1-T)T}z$
- $z_{12} := -\sqrt{T(1-T)}\tau(v + \xi) - v'$
- $z'_1 := \sqrt{(1-T)z'}$
- $z'_2 := \sqrt{Tz'}$
- $V_1 := 1 + v_i$

Finally, Alice applies two-mode squeezing to her two modes, in order to form the raw key. This can be interpreted as performing a weighted combination of her two modes. The value of the squeezing is optimized so as to maximize the expected secret key.

$$\Gamma_{A_1A_2B_2B_1} = \left( \begin{bmatrix} \sqrt{g} & -\sqrt{g-1} \\ -\sqrt{g-1} & \sqrt{g} \end{bmatrix} \oplus I_4 \right) \Gamma_{A'_1C'_2B'_2B_1} \left( \begin{bmatrix} \sqrt{g} & -\sqrt{g-1} \\ -\sqrt{g-1} & \sqrt{g} \end{bmatrix} \oplus I_4 \right)$$

with $g \geq 1$.

This gives:

$$\Gamma_{A_1A_2B_2B_1} = \begin{bmatrix} gV + (g-1)V_1 + 2\sqrt{g(g-1)}z_1 & \sqrt{g(g-1)}(V + V_1) + (2g-1)z_1 \\ (g-1)V + gV_1 - 2\sqrt{g(g-1)}z_1 & \sqrt{g}z_2 - \sqrt{g-1}z_{12} - \sqrt{g-1}z'_1 \end{bmatrix}$$

$$= \begin{bmatrix} * & * \\ (g-1)V + gV_1 - 2\sqrt{g(g-1)}z_1 & \sqrt{g}z_2 - \sqrt{g-1}z_{12} - \sqrt{g-1}z'_1 \end{bmatrix}.$$
The raw key is defined to be \( X_2 \), the measurement outcome obtained when performing heterodyne detection on mode \( A_2 \).

In order to compute the secret key rate, it will also be useful to compute the covariance matrix \( \Gamma_{A_1 \cdots A_2 B_1 | X_2} \) of the state \( A_1 B_2 B_1 \) conditioned on the measurement result \( X_2 \). Given a general covariance matrix of the form \( \Gamma = \begin{bmatrix} A & C \\ C^T & B \end{bmatrix} \), the covariance matrix of the state conditioned on the measurement result of heterodyning the modes corresponding to block \( A \) is [36]

\[
\Gamma_{A_1 \cdots A_2 B_1 | X_2} = B - C^T (A + \mathbb{I}_2)^{-1} C,
\]

with the following submatrices in our case where Alice measures the second mode with heterodyne detection:

\[
A := \begin{pmatrix} (g - 1) V + g V_1 & -2 \sqrt{g (g - 1)} z_1 \end{pmatrix} \mathbb{I}_2,
\]

\[
B := \begin{bmatrix} g V + (g - 1) V_1 + 2 \sqrt{g (g - 1)} z_1 & \sqrt{g} z_2 - \sqrt{g - 1} z_2' \\ 0 & \sqrt{g} z_2 - \sqrt{g - 1} z_2' \end{bmatrix},
\]

\[
C := \begin{pmatrix} - \sqrt{g (g - 1)} (V + V_1) + (2 g - 1) z_1 & - \sqrt{g - 1} z_2 + \sqrt{g} z_2' \\ 0 & - \sqrt{g - 1} z_2 + \sqrt{g} z_2' \end{pmatrix}.
\]

**Secret key rate**

With the above covariance matrices at hand, we are now ready to compute the asymptotic key rate of the two-way protocol for a typical thermal bosonic channel of transmittance \( \tau \) and excess noise \( \xi \).

Exploiting the Gaussian de Finetti reduction as explained in the main text, the asymptotic key rate is given by the Devetak-Winter formula [37]: It reads:

\[
K = \frac{1}{2} (\beta I(X_2; (Y_1, Y_2)) - \chi(X_2; E)),
\]

where we choose \( X_2 \), the measurement outcome of heterodyning mode \( A_2 \), to be the raw key. Here, \( \beta \leq 1 \) is the so-called “reconciliation efficiency”. The factor \( 1/2 \) reflects the fact that we compute a key rate per channel use, and that two channels are used in two-way CV QKD.

Let \( \Gamma_{X_1 X_2 Y_1 Y_2} \) denote the covariance matrix of the measurement outcomes. It if given by:

\[
\Gamma_{X_1 X_2 Y_1 Y_2} = \frac{1}{2} (\Gamma_{A_1 A_2 B_1 B_2} + \mathbb{I}_8).
\]

A subtlety of the EB protocol is that the parties might need to rescale their classical data in order to perform error reconciliation. This is for instance the case of the variable \( Y_2 \): it is better for Bob to exploit the value of the second mode, \( B_1' \), of his two-mode squeezer, which can be obtained by rescaling \( Y_2 \) by \( \sqrt{2(V_B - 1)/(V_B + 1)} \). The new covariance matrix is given by:

\[
\Gamma_{X_1 X_2 Y_1 Y_2} = \text{diag} \left( 1, 1, \sqrt{2(V_B - 1)/V_B + 1}, 1 \right) \Gamma_{X_1 X_2 Y_1 Y_2} \text{diag} \left( 1, 1, \sqrt{2(V_B - 1)/V_B + 1}, 1 \right),
\]

where \( \text{diag}(a, \ldots, z) \) is the diagonal matrix with diagonal coefficients \( a, \ldots, z \).

The mutual information \( I(X_2; (Y_1, Y_2')) \) is given by

\[
I(X_2; (Y_1, Y_2')) = \log_2 \left[ \frac{\det \Gamma_{X_2 | X_2} \det \Gamma_{Y'_2 | Y_2}}{\det \Gamma_{X_2 | Y_2'}} \right].
\]

The Holevo information \( \chi(X_2; E) \) can be computed as follows:

\[
\chi(X_2; E) = S(E) - S(E|X_2) = S(A_1 A_2 B_1 B_2) - S(A_1 B_1 B_2 | X_2),
\]

where we used the fact that Eve’s register \( E \) can be assumed without loss of generality to purify the systems \( A_1 A_2 B_1 B_2 \). Moreover, because we assume that Alice performs a heterodyne detection, which projects the state onto a pure coherent state, we also have \( S(A_1 B_1 B_2 | X_2) = S(E | X_2) \).
Let us denote by $\nu_1, \nu_2, \nu_3, \nu_4$ the symplectic eigenvalues of $\Gamma_{A_1 A_2 B_1 B_2}$ and by $\tilde{\nu}_1, \tilde{\nu}_2, \tilde{\nu}_3$ the symplectic eigenvalues of $\Gamma_{A_1 B_1 B_2 | X_2}$, which is the covariance matrix of the postmeasurement state after Alice has obtained outcome $X_2$. Then, the Holevo information is given by

$$\chi(X_2; E) = \sum_{i=1}^{4} g(\nu_i) - \sum_{i=1}^{3} g(\tilde{\nu}_i),$$

with the function $g$ defined by

$$g(x) := \frac{x+1}{2} \log_2 \left( \frac{x+1}{2} \right) - \frac{x-1}{2} \log_2 \left( \frac{x-1}{2} \right).$$

Recall that the symplectic eigenvalues of the matrix $\Gamma$ correspond to the standard eigenvalues of $|i\Omega\Gamma|$, or equivalently, to the modulus of the eigenvalues of $i\Omega\Gamma$, where the symplectic form $\Omega$ is given by $\Omega = \bigoplus_{i=1}^{d} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, and $d$ is the number of modes.

Finally, the key rate is obtained by optimizing over the choices of the variances $V_A, V_B$, transmittance $T$ and squeezing gain $g$.

We plot on Fig. 6 the asymptotic key rate of the two-way protocol and of the (one-way) no-switching protocol, in the case of a noiseless channel ($\xi = 0$), assuming perfect reconciliation efficiency. The key rate of the one-way protocol can be obtained similarly by imposing $V_A = 1$, i.e., Alice sends the vacuum to Bob, fixing $T = 0$ so that mode $B_2$ contains the vacuum, and getting rid of the final squeezer in Alice’s lab (by choosing $g = 1$).

![FIG. 6: Secret key rate of the two-way CV QKD protocol (full line) and of the one-way no-switching protocol (dashed line), assuming a pure-loss channel ($\xi = 0$) and perfect reconciliation efficiency ($\beta = 1$).](image)

We plot on Fig. 7 the key rate of the two protocols with a noisy channel ($\xi = 0.1$), and realistic reconciliation efficiency, $\beta = 0.95$. The advantage of the two-way protocol is clear in this case.
FIG. 7: Secret key rate of the two-way CV QKD protocol (full line) and of the one-way no-switching protocol (dashed line), assuming a noisy channel ($\xi = 0.1$) and imperfect reconciliation efficiency ($\beta = 0.95$).

We plot on Fig. 8 the tolerable excess noise of the two-way and one-way no-switching protocol against the channel transmittance $\tau$, that is the value of $\xi$ for which the key rate becomes 0. The main advantage of the two-way protocol is its much larger tolerance to noise.

FIG. 8: Maximum tolerable excess noise $\xi$ for the two-way CV QKD protocol (full line) and the one-way no-switching protocol (dashed line), assuming perfect reconciliation efficiency ($\beta = 1$).