High-rate measurement-device-independent quantum cryptography

Pirandola, Stefano; Ottaviani, Carlo; Spedalieri, Gaetana; Weedbrook, Christian; Braunstein, Samuel L.; Lloyd, Seth; Gehring, Tobias; Jacobsen, Christian Scheffmann; Andersen, Ulrik Lund

Published in:
Nature Photonics

Link to article, DOI:
10.1038/nphoton.2015.83

Publication date:
2015

Document Version
Peer reviewed version

High-rate quantum cryptography in untrusted networks

Stefano Pirandola,[1] Carlo Ottaviani,[1] Gaetana Spedalieri,[1] Christian Weedbrook,[2] Samuel L. Braunstein,[1] Seth Lloyd,[3] Tobias Gehring,[4] Christian S. Jacobsen,[4] and Ulrik L. Andersen[4]

[1]*Department of Computer Science, University of York, York YO10 5GH, United Kingdom*
[2]*Department of Physics, University of Toronto, Toronto M5S 3G4, Canada and QKD Corp., 112 College St., Toronto M5G 1L6, Canada*
[3]*MIT – Department of Mechanical Engineering and Research Laboratory of Electronics, Cambridge MA 02139, USA*
[4]*Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kongens Lyngby, Denmark*

We extend the field of continuous-variable quantum cryptography to a network formulation where two honest parties connect to an untrusted relay by insecure quantum links. To generate secret correlations, they transmit coherent states to the relay where a continuous-variable Bell detection is performed and the outcome broadcast. Even though the detection could be fully corrupted and the links subject to optimal coherent attacks, the honest parties can still extract a secret key, achieving high rates when the relay is proximal to one party, as typical in public networks with access points or proxy servers. Our theory is confirmed by an experiment generating key-rates which are orders of magnitude higher than those achievable with discrete-variable protocols. Thus, using the cheapest possible quantum resources, we experimentally show the possibility of high-rate quantum key distribution in network topologies where direct links are missing between end-users and intermediate relays cannot be trusted.

Quantum key distribution (QKD) [1, 2] is one of the most active areas in quantum information [3, 4], with a number of in-field implementations, including the development of metropolitan networks based on point-to-point QKD protocols [5–8]. A typical QKD protocol involves two parties, conventionally called Alice and Bob, who aim to generate a secret key by exchanging quantum systems over an insecure communication channel. Security is assessed against the most powerful attack on the channel, where an eavesdropper, conventionally called Eve, perturbs the quantum systems using the most general strategies allowed by quantum mechanics.

While this theoretical analysis is fundamental for testing the basic security of a protocol, it may be insufficient to guarantee its viability in realistic implementations, where flaws in the devices may provide alternative 'side-channels' to be attacked [9, 10]. These weaknesses naturally arise in realistic models of networks (e.g., the Internet) where two end-users are not connected by direct lines but must exploit one or more intermediate nodes, whose operation may be tampered with by Eve.

In this scenario, Ref. [11] has recently introduced a general method to guarantee security. Considering arbitrary quantum systems as information carriers, Ref. [11] designed a swapping-like protocol where secret correlations are established by the measurement of a third untrusted party. This idea of 'measurement-device independence' has been independently introduced in Ref. [12] in the specific context of qubits (weak pulses and decoy states), with a series of further investigations [14–22].

In this paper we develop the notion of measurement-device independence for bosonic systems. In this way we extend the field of continuous-variable quantum cryptography [4, 23–27] to a more robust network formulation. In fact, we consider the basic network topology where Alice and Bob communicate by connecting to an untrusted relay via insecure links. To create secret correlations, they transmit random coherent states to the relay where a continuous-variable Bell detection is performed and the outcome broadcast. Despite the possibility that the relay could be fully tampered with, and the links subject to optimal coherent attacks, Alice and Bob are still able to extract a secret key.

Our analysis shows that the optimal configuration of the protocol corresponds to the relay being close to one party, e.g., Alice, in which case remarkable rates can be achieved, orders of magnitude higher than those achievable with discrete-variable protocols over comparable distances [12, 20–22]. Our theoretical prediction is fully confirmed by a proof-of-principle experiment, where 10^{-2} secret bits per relay use are distributed at 10dB loss in Bob's link, equivalent to 50km in standard optical fibre (at the loss rate of 0.2dB/km). Such rate corresponds to hundreds of kbits/s using state-of-the-art clock rates at 75MHz [22]. Furthermore, assuming ideal reconciliation, our experiment shows a potential rate of about 10^{-4} secret bits per relay use over a very lossy link, with 34dB loss corresponding to 170km in fibre.

Note that this asymmetric configuration resembles the typical topology of a public network where a user connects its device to a proxy server to communicate with remote users. This setup is here studied in the full optical regime but may also occur in a mixed technology environment where a wireless device (e.g., the infrared port of a laptop or phone) connects to a nearby access point, which is the hub of a star network of remote users connected by long optical fibres.

We remark that our formulation provides conceptual and practical advantages with respect to traditional quantum cryptography. First we move from a point-to-point to a robust end-to-end formulation, which removes both trust and complexity from the middle nodes. In particular, the fact that the relay is just performing a simple detection on the incoming systems removes ex-

pensive quantum sources from the network. This feature makes the key rate orders of magnitude higher than that of protocols based on a central distribution of entanglement [28, 29]. Second we fully exploit the advantages provided by continuous variables using the cheapest possible quantum sources (coherent states) and the most efficient quantum measurements (homodyne detectors). This other feature makes our protocol easy to implement on realistic networks with key rates out of the reach of any protocol based on discrete-variable systems.

Thus, our work exploits the cheapest quantum resources to prove high-rate QKD in untrusted networks where direct links are missing between two end-users. This represents the first step towards the realization of scalable models of secure quantum networks, based on the end-to-end principle [30] and the modern notion of 'reliability from unreliable parts' [31].

I. RESULTS

For simplicity, we start by describing the protocol in noiseless links, explaining the basic mechanism of the relay. Then we consider the most general eavesdropping strategy against the relay and the links, showing how this strategy can be reduced to a coherent Gaussian attack of the links only. Finally we derive the secret-key rate of the protocol and we compare theoretical and experimental performances in the optimal configuration.

Basic idea.– Consider two distant parties, Alice and Bob, aiming to share a secret key. At one side, Alice prepares a mode A in a coherent state $|\alpha\rangle$ whose amplitude α is modulated by a Gaussian distribution with zero mean and large variance, equal to $\varphi \gg 1$ in each quadrature. At the other side, Bob prepares his mode B in another coherent state $|\beta\rangle$ whose amplitude β is modulated by the same Gaussian distribution as Alice. Modes A and B are then sent to an intermediate station, which is the continuous-variable Bell relay shown in Fig. 1(i).

The relay performs a continuous-variable Bell detection on the incoming modes, by mixing them in a balanced beam splitter whose output ports are conjugately homodyned [32]. This detection corresponds to measuring the quadrature operators $\hat{q}_- = (\hat{q}_A - \hat{q}_B)/\sqrt{2}$ and $\hat{p}_+ = (\hat{p}_A + \hat{p}_B)/\sqrt{2}$, whose classical outcomes are combined in a complex variable $\gamma := (q_- + ip_+)/\sqrt{2}$ with probability $p(\gamma)$. The outcome γ is then communicated to Alice and Bob via a classical public channel.

In this process the relay acts as a correlator [11]. One can check that the outcome γ creates *a-posteriori* correlations between the parties, being equal to $\gamma = \alpha - \beta^* + \hat{\delta}$ with $\hat{\delta}$ detection noise. As a result, the knowledge of γ enables each party to infer the variable of the other party by simple postprocessing. For instance, Bob may compute $\beta^* + \gamma = \alpha + \hat{\delta}$ decoding Alice's variable [33]. Thus, conditioned on γ, Alice and Bob's mutual information increases from $I(\alpha : \beta) = 0$ to $I(\alpha : \beta|\gamma) > 0$.

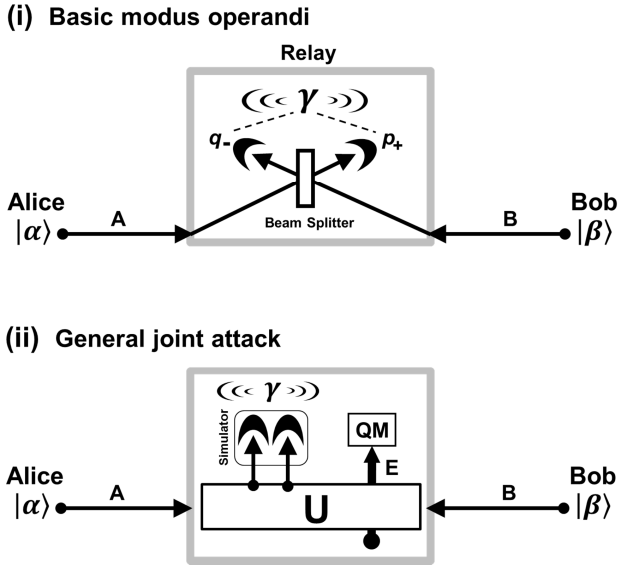

FIG. 1: (i) Modus operandi of the continuous-variable Bell relay (see text for explanation). (ii) Joint attack of the protocol. In each use of the relay, modes A and B unitarily interact with ancillary vacuum modes. Two outputs simulate the relay, while the remaining outputs E are stored in a quantum memory (QM) measured by Eve at the end of the protocol.

Averaging over all possible outputs γ, the honest parties will share $I_{AB} = \int d^2\gamma p(\gamma) I(\alpha : \beta|\gamma)$ mean bits per use of the relay, which is logarithmically increasing in the modulation φ. Despite Eve also having access to the classical communication and operating the relay, she cannot steal any information, since she only knows γ and $I(\alpha : \gamma) = I(\beta : \gamma) = 0$. As a result, Eve is forced to attack the links and/or corrupt the relay.

Protocol under general eavesdropping.– The most general eavesdropping strategy of our protocol is a joint attack involving both the relay and the two links as depicted in Fig. 1(ii). In each use of the relay, Eve may intercept the two modes, A and B, and make them interact with an ensemble of ancillary vacuum modes via a general unitary U. Among the output modes, two are sent to a simulator of the relay, where they are homodyned and the result γ broadcast. The remaining modes E are stored in a quantum memory which is measured at the end of the protocol.

Note that a more general attack may involve a unitary applied to all modes which are transmitted over many uses of the relay. However, this can always be reduced to the previous attack, coherent within the single use, by assuming that Alice and Bob perform random permutations on their data [34, 35]. Also note that, in Eve's simulator, any other higher-rank measurement of the quadratures can always be purified into a rank-one measurement by enlarging the set of the ancillas E. If other observables are measured or no detection occurs, the communication of a fake variable γ can be easily detected from the analysis of the empirical data [11].

In order to deal with the joint attack of Fig. 1(ii), Alice and Bob must retrieve the joint statistics of the variables α, β, and γ. Since the protocol is performed many times, Alice and Bob can compare a small part of their data via the public channel and reconstruct the probability distribution $p(\alpha,\beta,\gamma)$. As we show in the Supplementary Information, for any observed distribution $p(\alpha,\beta,\gamma)$, the security of the protocol does not change if we modify Eve's unitary U in such a way that her simulator works exactly as the original relay (so that the modes are mixed in a balanced beam splitter and conjugately homodyned). Thus, we can assume that the relay is properly operated (even if by Eve) with the unitary U restricted to be a coherent attack against the two links.

The description of this attack can further be simplified. Since the protocol is based on the Gaussian modulation and detection of Gaussian states, its optimal eavesdropping is based on a Gaussian unitary U [36]. Thus, from the first- and second-order statistical moments of the observed distribution $p(\alpha,\beta,\gamma)$, Alice and Bob construct a Gaussian distribution $p_G(\alpha,\beta,\gamma)$ and design a corresponding optimal Gaussian attack against the links.

From an operational point of view, the first-order moments are used to construct the optimal estimators of each other variable, while the second-order moments are used to derive the secret key rate of the protocol. In particular, Alice and Bob are able to compute their mutual information I_{AB} and upperbound Eve's stolen information I_E via the Holevo bound. As long as the condition $R := I_{AB} - I_E > 0$ is satisfied, they can postprocess their data via standard procedures of error correction and privacy amplification, and distill an average of R secret bits per use of the relay.

Coherent Gaussian attack of the links.– Following the previous reasoning, the cryptoanalysis of the protocol can be reduced to studying a coherent Gaussian attack against the two links, assuming a properly-working relay. Attacks of this kind can be constructed by correlating two canonical forms [37, 38]. The most realistic scenario is the Gaussian attack depicted in Fig. 2.

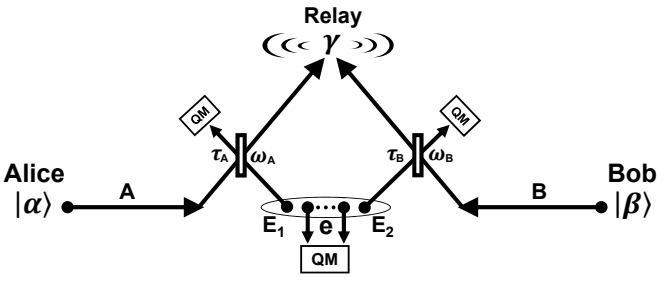

FIG. 2: Protocol in the presence of a coherent Gaussian attack. The two travelling modes, A and B, are mixed with two ancillary modes, E_1 and E_2, via two beam splitters, with transmissivities τ_A and τ_B, which introduce thermal noise with variances, ω_A and ω_B, respectively. The ancillary modes belong to a reservoir of ancillas (E_1, $\mathbf{e}$, E_2) which is globally in a pure Gaussian state. All Eve's output is stored in a quantum memory (QM) measured at the end of the protocol.

In this attack, the two travelling modes, A and B, are mixed with two ancillary modes, E_1 and E_2, by two beam splitters with transmissivities τ_A and τ_B, respectively. These ancillary modes belong to a reservoir of ancillas (E_1, E_2 plus an extra set $\mathbf{e}$) which is globally described by a pure Gaussian state. The reduced state $\sigma_{E_1E_2}$ of the injected ancillas is a correlated thermal state with zero mean and covariance matrix in the normal form

$$\mathbf{V}_{E_1E_2} = \begin{pmatrix} \omega_A\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B\mathbf{I} \end{pmatrix}, \ \mathbf{G} := \begin{pmatrix} g & 0 \\ 0 & g' \end{pmatrix}, \qquad (1)$$

where $\omega_A, \omega_B \geq 1$ are the variances of the thermal noise affecting each link, while g and g' are correlation parameters which must satisfy physical constraints [39, 40] (see Supplementary Information). After interaction, all Eve's ancillas are stored in a quantum memory, which is coherently measured at the end of the protocol.

Note that our description of the attack is very general since any two-mode Gaussian state can be transformed into the previous normal form by local Gaussian unitaries [4]. In general, the injected state $\sigma_{E_1E_2}$ can be separable or entangled. The simplest case is when there are no correlations ($g = g' = 0$), so that $\sigma_{E_1E_2}$ is a tensor product and the attack collapses into a collective attack with two independent entangling cloners [24].

Secret-key rate of the protocol.– In the attack of Fig. 2, the relay provides $\gamma = \sqrt{\tau_A}\alpha - \sqrt{\tau_B}\beta^* + \hat{\delta}_{\text{noise}}$, where the empirical values of τ_A and τ_B are accessible to the parties from the first-order moments of the statistics $p(\alpha,\beta,\gamma)$. We assume that Alice is the encoder and Bob is the decoder, which means that α is inferred by processing β into an optimal estimator. For large modulation $\varphi \gg 1$, Alice and Bob's mutual information is given by $I_{AB} = \log_2(\varphi/\chi)$, where the equivalent noise $\chi = \chi(\tau_A, \tau_B, \omega_A, \omega_B, g, g')$ can be computed from the second-order moments of $p(\alpha,\beta,\gamma)$ (see Supplementary Information for more details).

From the analysis of the second-order statistical moments, Alice and Bob can derive the secret-key rate of the protocol, which becomes a simple function of τ_A, τ_B and χ in the limit of large modulation

$$R(\tau_A,\tau_B,\chi) = h\left(\tfrac{\tau_A\chi}{\tau_A+\tau_B} - 1\right) - h\left[\tfrac{\tau_A\tau_B\chi - (\tau_A+\tau_B)^2}{|\tau_A-\tau_B|(\tau_A+\tau_B)}\right] + \log_2\left[\tfrac{2(\tau_A+\tau_B)}{e|\tau_A-\tau_B|\chi}\right], \qquad (2)$$

where $h(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}$. The asymptotic rate is continuous in $\tau_A = \tau_B$, where it becomes

$$R(\chi) = h\left(\tfrac{\chi}{2} - 1\right) + \log_2\left[\tfrac{16}{e^2\chi(\chi-4)}\right]. \qquad (3)$$

As typical in QKD, the equivalent noise can be decomposed as $\chi = \chi_{\text{loss}} + \varepsilon$, where $\chi_{\text{loss}} = 2(\tau_A+\tau_B)/\tau_A\tau_B$ is the noise due to loss, while ε is the 'excess noise'. Thus, the key rate can be also expressed as $R = R(\tau_A, \tau_B, \varepsilon)$.

To study the maximum theoretical performance of the protocol we set $\varepsilon = 0$, therefore restricting Eve to a

pure-loss attack of the links with rate $R_{\rm loss}(\tau_A,\tau_B) := R(\tau_A,\tau_B,0)$. In the symmetric configuration $\tau_A=\tau_B:=\tau$, we find $R_{\rm loss}(\tau,\tau)\simeq 0$ at $\tau\simeq 0.84$, so that Alice's and Bob's distances from a perfectly-in-the-middle relay are limited to ≃3.8km in standard telecom fibres (0.2dB/km). For this reason, we consider asymmetric configurations where one of the links has small loss.

First suppose that Bob's link has small loss ($\tau_B\simeq 1$). We find $R_{\rm loss}\simeq \log_2[\tau_A/(1-\tau_A)e]$ which is zero at $\tau_A\simeq 0.73$. In telecom fibres this is still restrictive, since Alice's distance from the relay cannot exceed 6.8km. By contrast, suppose that Alice's link has small loss ($\tau_A\simeq 1$). Now we have $R_{\rm loss}\simeq h[(2-\tau_B)/\tau_B]+\log_2[\tau_B/(1-\tau_B)e]$, which goes to zero only for $\tau_B\to 0$, corresponding to Bob arbitrarily far from the relay. Thus, we find that extremely long distances can be achieved if the relay is sufficiently close to Alice [41]. These distances are fully quantified in the next section.

Long distance distribution via proximal relays.– Consider the asymmetric scenario in Fig. 3, where Alice and Bob exploit an untrusted relay at some short radial distance r from Alice and distance d from Bob. For pure-loss links ($\varepsilon=0$) and standard fibres (0.2dB/km), we can express the rate as $R_{\rm loss}=R_{\rm loss}(r,d)$. Solving $R_{\rm loss}=0$ we derive the security threshold in terms of Bob's maximum distance d for a given value of r.

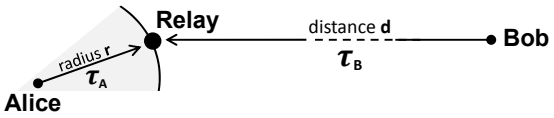

FIG. 3: Key-distribution via a proximal untrusted relay, at short radial distance r from Alice, and distant d from Bob.

As we see from Fig. 4, for a relay sufficiently close to Alice, Bob can be very far with key distribution being possible at distances well beyond 100km. This performance is very robust to the presence of excess noise $\varepsilon\neq 0$, coming from a coherent Gaussian attack of the links. In this general case, we can write the rate as $R=R(r,d,\varepsilon)$. Then, solving $R=0$ for high excess noise $\varepsilon=0.1$ [42] we derive the threshold in the inset of Fig. 4. As a result, key distribution is possible at very long distances even in the presence of very strong eavesdropping.

Experimental proof-of-principle.– Our theory has been experimentally confirmed. We have reproduced the asymmetric configuration of Fig. 3, with $\tau_A\simeq 1$ and variable τ_B, down to 4×10^{-4} corresponding to about 170km in standard optical fibre. A schematic of our experimental setup is depicted in Fig. 5 .

For every experimental point, we have evaluated the second-order moments of $p(\alpha,\beta,\gamma)$ and computed the experimental key rate $R=\xi I_{AB}-I_E$, with $\xi\leq 1$ being the reconciliation efficiency (current achievable value $\xi\simeq 0.97$ [43]). Experimental results are plotted in Fig. 6 and compared with the theoretical predictions, with excellent agreement. Assuming ideal reconciliation, the experimental rate approaches the theoretical limit of the pure-loss attack. Due to imperfections, we have extra noise in our data which affects the rate approximately in the same way as a coherent Gaussian attack with excess noise $\varepsilon\lesssim 0.02$. Note that we can potentially reach $R\simeq 10^{-4}$ secret bits per relay use over a link with 34dB loss, equivalent to 170km in standard optical fibre.

Such long distance results are only potential since the current reconciliation procedures for continuous-variable protocols do not have unit efficiency (indeed this is the

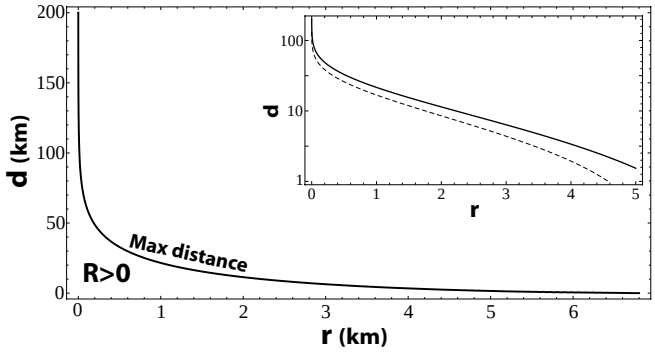

FIG. 4: Given a relay at distance r from Alice, the solid line represents the maximum distance d of Bob from this relay, within which key distribution is possible ($R>0$). The inset shows Bob's maximum distance (in logarithmic scale) when Eve performs a coherent Gaussian attack with excess noise $\varepsilon=0.1$ (dashed line). The corresponding security threshold is compared with that of the pure-loss attack (solid line).

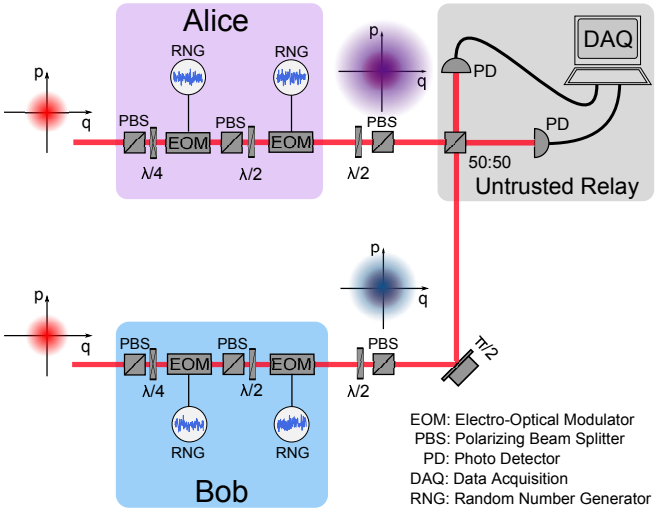

FIG. 5: Experimental setup. Alice and Bob apply amplitude and phase modulators to a pair of identical classical phase-locked bright coherent beams (providing a common local oscillator). At the output, the two modes emerge randomly-displaced in the phase space according to a Gaussian distribution. In particular, Bob's modulation is suitably attenuated to simulate loss in his link. At the relay, modes are mixed in a balanced beam splitter and the output ports photo-detected. Photocurrents are then processed to realize a continuous-variable Bell measurement (see Supplementary Information for more details).

main factor limiting the distance of continuous variable QKD). By taking this realistic limitation into account ($\xi \simeq 0.97$), we can still reach remarkably high rates over distances well beyond the typical connection lengths of a network. As we can see from Fig. 6, we can achieve $R \simeq 10^{-2}$ secret bits per relay use over a link with 10dB loss, equivalent to 50km in fibre.

This result is at least three orders of magnitude higher than that achievable with discrete-variables over comparable distances [12, 20–22]. Implementing our protocol with a 75MHz clock rate [22] would provide a secret-key rate in the range $75 \div 750$kbit/s at $50 \div 60$km, which is remarkably higher than the value $\lesssim 100$bit/s reported in [22] over similar distances. At the same time, we achieve the best performances of continuous variable protocols despite the fact we are removing their point-to-point quantum communication channel. For instance, working with a 1MHz clock rate at $50 \div 60$km, we can reach a rate of about $1 \div 10$kbit/s as in Ref. [27].

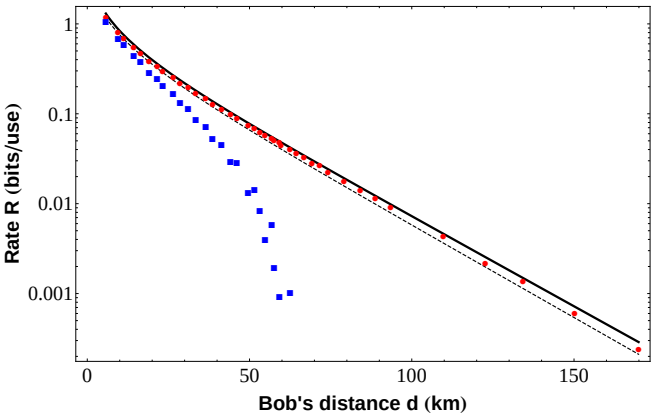

FIG. 6: Secret-key rate R versus Bob's distance d from the relay. Experimental points refer to ideal reconciliation ($\xi = 1$, red circles) and realistic reconciliation ($\xi \simeq 0.97$, blue squares). For comparison, we also plot the theoretical rates for a pure-loss attack (solid line) and a coherent Gaussian attack with excess noise $\varepsilon = 0.02$ (dashed line).

II. DISCUSSION

In this work, we have extended the field of continuous-variable quantum cryptography to a network formulation where two end-users do not access a direct quantum communication channel but are forced to connect to an untrusted relay via insecure quantum links. Despite the possibility that the relay could be fully corrupted and its links subject to coherent attacks, the end-users can still extract a secret key. This surprising result comes from a demanding cryptoanalysis of our model which represents the first continuous-variable protocol whose rate has been explicitly computed against a two-mode coherent attack.

An important feature is the simplicity of the relay, which does not possess any quantum source but just performs a standard optical measurement, with all the heavy procedures of data post-processing left to the end-users, fulfilling the idea behind the end-to-end principle. In particular, the relay implements a continuous-variable Bell detection which involves highly efficient photodetectors plus linear optics, whereas the discrete-variable version of this measurement needs nonlinear elements to operate deterministically. This feature combined with the use of coherent states makes the scheme very attractive, guaranteeing both cheap implementation and high rates.

We have found that the optimal network configuration is asymmetric with the untrusted relay acting as a proxy server near to one of the parties. In this case we have experimentally proven that remarkable rates can be reached, several orders of magnitude higher than those achievable with qubit-based protocols over comparable distances. Further improvements in the classical reconciliation techniques would make the performance of our protocol even better. From this point of view, our protocol can already be used for setting up very efficient star networks based on public access points. Further investigations could involve the analysis of mixed technology environments where some of the connections are established at low frequencies (infrared or microwave) with thermal effects becoming important [44–46].

By introducing the mediation of an untrusted and cheap relay, our work paves the way for extending quantum cryptography to more advanced models of networks where information is routed end-to-end through untrusted nodes, whereas current models are strongly based on computationally demanding point-to-point sessions of key distribution involving chains of trusted nodes [5–8]. Indeed our protocol can already be used to remove trust and reliability from half of the nodes of a large network, since any chain of nodes between two end-users can be decomposed into $n+1$ trusted nodes and n untrusted relays (so that only n temporary keys must be distributed along the chain, instead of $2n$ point-to-point keys). It is clear that further work is needed to extend the model and realize a fully untrusted network where only the end-users are trusted.

III. METHODS

Theoretical methods, experimental details and data analysis can be found in the Supplementary Information.

Acknowledgments

This work has been supported by EPSRC (grant numbers EP/J00796X/1 and EP/L011298/1), NSERC and the Leverhulme Trust.

[1] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145 (2002).

[2] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dusek, M., Lutkenhaus, N. & Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).

[3] Wilde, M. M. *Quantum Information Theory* (Cambridge University Press, Cambridge, 2013).

[4] Weedbrook, C., Pirandola, S., Garcia-Patron, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H. & Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).

[5] SECOQC, 2007, http://www.secoqc.net.

[6] Peev, M. *et al.* The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **11**, 075001 (2009).

[7] Tokyo QKD network 2010, www.uqcc.org/QKDnetwork.

[8] Sasaki, M. *et al.* Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **19**, pp. 10387-10409 (2011).

[9] Lydersen, L., Wiechers, C., Wittman, C., Elser, D., Skaar, D. & Makarov V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics* **4**, 686 (2010).

[10] Gerhardt, I., Liu, Q., Lamas-Linares A., Skaar J., Kurtsiefer C. & Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature Comm.* **2**, 349 (2011).

[11] Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).

[12] Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).

[13] Ma, X., Fred Fung, C.-H. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 052305 (2012).

[14] Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **86**, 062319 (2012).

[15] Wang, X.B. Three-intensity decoy state method for device independent quantum key distribution with basis dependent errors. *Phys. Rev. A* **87**, 012320 (2013).

[16] Branciard, C., Rosset, D., Liang, Y.-C. & Gisin, N. Measurement-device-independent entanglement witnesses for all entangled quantum states. *Phys. Rev. Lett.* **110**, 060405 (2013).

[17] Tomamichel, M., Fehr, S., Kaniewski, J. & Wehner, S. A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New J. Phys.* **15**, 103002 (2013).

[18] Ci Wen Lim, C., Portmann, C., Tomamichel, M., Renner, R. & Gisin, N. Device-independent quantum key distribution with local Bell test. *Phys. Rev. X* **3**, 031006 (2013).

[19] Abruzzo, S., Kampermann, H., & Bruß D. Measurement-device-independent quantum key distribution with quantum memories. *Phys. Rev. A* **89**, 012301 (2014).

[20] Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-World two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Phys. Rev. Lett.* **111**, 130501 (2013).

[21] Ferreira da Silva, T., Vitoreti, D., Xavier, G. B., do Amaral, G. C., Temporão, G. P. & von der Weid, J. P. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. *Phys. Rev. A* **88**, 052303 (2013).

[22] Tang, Y.-L. *et al.* Measurement-device-independent quantum key distribution over 200 km. Preprint arXiv:1407.8012.

[23] Cerf, N. J., Levy, M. & van Assche, G. Quantum distribution of Gaussian keys with squeezed states. *Phys. Rev.* **A** 63, 052311 (2001).

[24] Grosshans, F., van Assche, G., Wenger, J., Tualle-Brouri, R., Cerf, N. J. & Grangier, P. High-rate quantum cryptography using Gaussian-modulated coherent states. *Nature* (London) **421**, 238 (2003).

[25] Weedbrook, C., Lance, A. M., Bowen, W. P., Symul, T., Ralph, T. C. & Lam, P. K. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).

[26] Pirandola, S., Mancini, S., Lloyd, S. & Braunstein, S. L. Continuous-variable quantum cryptography with two-way quantum communication. *Nature Phys.* **4**, 726 (2008).

[27] Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics* **7**, 378–381 (2013).

[28] Ekert, A., K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).

[29] Weedbrook, C. Continuous-variable quantum key distribution with entanglement in the middle. *Phys. Rev. A* **87**, 022308 (2013).

[30] Saltzer, J. H., Reed, D. P. & Clark, D. D. End-to-end arguments in system design. *Proceedings of the Second International Conference on Distributed Computing Systems* (Paris, France, April 8-10, 1981).

[31] Baran, P. On distributed communications networks. *IEEE Trans. Commun.* **12**, pp. 1–9 (1964).

[32] Spedalieri, G., Ottaviani, C. & Pirandola, S. Covariance matrices under Bell-like detections. *Open Syst. Inf. Dyn.* **20**, 1350011 (2013).

[33] This kind of decoding based on the subtraction of a reference variable can also be found in two-way quantum cryptography [26].

[34] Renner, R. Symmetry of large physical systems implies independence of subsystems. *Nature Phys.* **3**, 645 (2007).

[35] 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).

[36] García-Patrón, R. & Cerf, N. J. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).

[37] Pirandola, S., Braunstein, S. L. & Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **101**, 200504 (2008).

[38] Pirandola, S., García-Patrón, R. Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **102**, 050503 (2009).

[39] Pirandola, S., Serafini, A. & Lloyd, S. Correlation matrices of two-mode bosonic systems. *Phys. Rev. A* ***79***,

052327 (2009).
[40] Pirandola, S. Entanglement reactivation in separable environments. *New J. Phys.* **15**, 113046 (2013).
[41] It is clear that the behaviour of the rate would be perfectly inverted if Bob were the encoder of the secret information and Alice the decoder.
[42] Note that these values are much higher than those typically appearing in experiments of continuous-variable QKD. For instance, $\varepsilon \lesssim 0.008$ in Ref. [27].
[43] Jouguet, P., Kunz-Jacques, S., & Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **84**, 062317 (2011).
[44] Weedbrook, C., Pirandola, S., Lloyd, S. & Ralph, T. C. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **105**, 110501 (2010).
[45] Weedbrook, C., Pirandola, S. & Ralph, T. C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **86**, 022318 (2012).
[46] Weedbrook, C., Ottaviani, C., & Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **89**, 012309 (2014).

Supplementary Information

Contents of the document. In Sec. I we give full details of our theoretical methods and derivations. We follow the notation of Ref. [S1], where $[\hat{q},\hat{p}] = 2i$ (i.e., $\hbar = 2$) so that the vacuum noise is set to 1 and $\hat{a} = (\hat{q}+i\hat{p})/2$. In Sec. II we thoroughly discuss the experimental setup and the post-processing of the data, including an analysis of the various finite-size effects.

I. THEORETICAL METHODS

In this section we describe the main theoretical methods used in our study. Adopting an entanglement-based representation of the protocol (Sec. I A), we first show how a joint attack of the relay and the links can be reduced to a Gaussian attack of the links with a properly-working relay (Sec. I B). Here the key-step is proving the measurement-device independence for our continuous-variable protocol, followed by the application of the known result on the extremality of Gaussian states. In Sec. I C, we then describe how to derive the secret-key rate of the protocol in the presence of an arbitrary Gaussian attack of the links. In Sec. I D we make our derivation more specific considering a realistic form of a coherent Gaussian attack, deriving an explicit analytical formula for the secret-key rate in Sec. I E. This rate is minimized and simplified in Sec. I F, and studied for specific configurations in Sec. I G. Finally, Sec. I H contains the technical derivation of the post-relay quantum covariance matrix (CM) which is central for the computation of the rate.

A. Cryptoanalysis of the protocol in the entanglement-based representation

To study the security of the protocol, we adopt an entanglement-based representation where each source of coherent states is realized by an Einstein-Podolsky-Rosen (EPR) state subject to heterodyne detection. As in the top panel of Fig. 7, at Alice's station we take an EPR state ρ_{aA} having zero mean and CM equal to

$$\mathbf{V} = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix}, \ \mathbf{Z} := \begin{pmatrix} 1 & \\ & -1 \end{pmatrix}. \quad (4)$$

By heterodyning mode a, Alice remotely prepares a coherent state $|\alpha\rangle$ on mode A, whose amplitude is modulated by a complex Gaussian with variance $\varphi = \mu - 1$. The outcome of the measurement $\tilde{\alpha}$ is related to the projected amplitude α by the relation

$$\tilde{\alpha} = \eta\alpha^*, \ \eta := (\mu+1)(\mu^2-1)^{-1/2}. \quad (5)$$

For large modulation $\mu \gg 1$ we have $\tilde{\alpha} \simeq \alpha^*$. It is important to note that the two variables α and $\tilde{\alpha}$ are equivalent from a information-theoretical point of view, in the sense that they share the same mutual information with any third variable.

On the other side, Bob's coherent state $|\beta\rangle$ can be prepared using another EPR state ρ_{bB} whose mode b is heterodyned with outcome $\tilde{\beta} = \eta\beta^*$ (with the limit $\tilde{\beta} \simeq \beta^*$ for $\mu \gg 1$). Again, we have that the outcome variable $\tilde{\beta}$ is informationally equivalent to β.

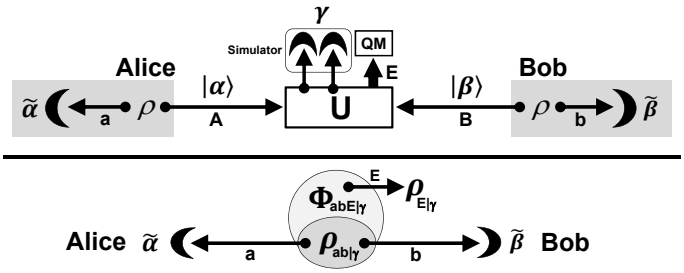

FIG. 7: (Top). Entanglement-based representation of the protocol, where Alice's and Bob's random coherent states are generated by local heterodyne detections on EPR states. Outcome variables $\tilde{\alpha}$ and $\tilde{\beta}$ are informationally-equivalent to the amplitudes α and β of the coherent states. (Bottom) Conditional scenario after Eve's detection with outcome γ.

In the top panel of Fig. 7 we see that, before the unitary U and the measurements, the global input state of Alice, Bob, and Eve is pure and Gaussian (Eve's ancillas are prepared in vacua). After U and before the measurements, their global output state is still pure, despite the fact that it could be non-Gaussian. Since local measurements commute, we can postpone Alice's and Bob's heterodyne detections after Eve's detection, whose outcome γ is obtained with probability $p(\gamma)$. Thus, we have the conditional scenario depicted in the bottom panel of Fig. 7, where Alice, Bob, and Eve share a conditional

state $\Phi_{abE|\gamma}$ with reduced states $\rho_{ab|\gamma}$ (for Alice and Bob) and $\rho_{E|\gamma}$ (for Eve). Since Eve performs homodyne detections, $\Phi_{abE|\gamma}$ is pure, so that $\rho_{ab|\gamma}$ and $\rho_{E|\gamma}$ have the same entropy

$$S(\rho_{ab|\gamma}) = S(\rho_{E|\gamma}). \tag{6}$$

In the conditional post-relay scheme of Fig. 7 (bottom panel), Alice encodes information by heterodyning her mode a with result $\tilde{\alpha}$. Since heterodyne is a rank-one measurement, it projects $\Phi_{abE|\gamma}$ into a pure state $\Phi_{bE|\gamma\tilde{\alpha}}$ for Bob and Eve, so that the reduced states $\rho_{b|\gamma\tilde{\alpha}}$ and $\rho_{E|\gamma\tilde{\alpha}}$ have the same entropy

$$S(\rho_{b|\gamma\tilde{\alpha}}) = S(\rho_{E|\gamma\tilde{\alpha}}). \tag{7}$$

As a result we have that, conditioned on γ, Eve's stolen information on Alice's variable $\tilde{\alpha}$ is upperbounded by the Holevo quantity

$$I_{E|\gamma} := S(\rho_{E|\gamma}) - S(\rho_{E|\gamma\tilde{\alpha}}) = S(\rho_{ab|\gamma}) - S(\rho_{b|\gamma\tilde{\alpha}}), \tag{8}$$

which is fully determined by the state $\rho_{ab|\gamma}$.

To retrieve Alice's encoding $\tilde{\alpha}$, Bob heterodynes his mode b whose output $\tilde{\beta}$ is optimally postprocessed. Conditioned on γ, Alice and Bob's mutual information is given by $I_{AB|\gamma} := I(\tilde{\alpha}, \tilde{\beta}|\gamma) = I(\alpha, \beta|\gamma)$, which is fully determined by $\rho_{ab|\gamma}$. As a result, the secret-key rate of the protocol is given by the average

$$R = \int d^2\gamma \; p(\gamma) R_{|\gamma}, \; R_{|\gamma} := I_{AB|\gamma} - I_{E|\gamma}. \tag{9}$$

This quantity only depends on the conditional state $\rho_{ab|\gamma}$ and the statistics of Eve's outcomes $p(\gamma)$.

B. Measurement-device independence and Gaussian optimality

Starting from the observed distribution $p(\alpha, \beta, \gamma) = p(\alpha, \beta|\gamma)p(\gamma)$, Alice and Bob reconstruct a joint attack as in the top panel of Fig. 7, which is optimal and compatible with their statistics. In particular, they compute the post-relay conditional state $\rho_{ab|\gamma}$ directly from the conditional probability $p(\alpha, \beta|\gamma)$.

Given $p(\alpha, \beta, \gamma)$, and therefore $p(\gamma)$ and $\rho_{ab|\gamma}$, the rate R is completely determined. This means that R remains exactly the same if we arbitrarily change U while preserving the observed statistics $p(\alpha, \beta, \gamma)$. In particular, we can change U in such a way that the simulator represents a properly-working relay. This can always be done by adding the identity $I = U_{\text{Bell}} U_{\text{Bell}}^{\dagger}$, where $U_{\text{Bell}}^{\dagger}$ is absorbed by U, while U_{Bell} converts the homodynes of the simulator into a Bell detection. Thus, compatibly with the observed data, an arbitrary joint attack U of the links and the relay can always be reduced to an attack of the links only, associated with a properly-working relay.

The next step is exploiting the optimality of Gaussian attacks for Gaussian protocols [S1, S2]. For any outcome γ, the conditional rate $R_{|\gamma}$ is minimized if we replace the pure state $\Phi_{abE|\gamma}$ with a pure Gaussian state $\Phi^{G}_{abE|\gamma}$ having the same mean value and CM. Note that, in the top panel of Fig. 7, this is equivalent to considering U to be a Gaussian unitary, therefore generating joint Gaussian statistics for the variables α, β and γ. Thus, Alice and Bob can always replace $p(\alpha, \beta, \gamma)$ with a Gaussian distribution $p_G(\alpha, \beta, \gamma)$ having the same first- and second-order statistical moments. Adopting this new distribution, they upperbound Eve's performance replacing her attack with a Gaussian attack against the links.

C. General computation of the secret-key rate

According to the previous analysis, Alice and Bob consider the worst-case scenario where the two links are subject to a Gaussian attack, while the relay is properly operated by Eve. In this case, for any outcome γ, the conditional Gaussian state $\rho_{ab|\gamma}$ has always the same CM $\mathbf{V}_{ab|\gamma}$ while its mean value varies with γ. As typical in Gaussian entanglement swapping [S3], this random shift in the first moments can be automatically compensated for by Bob's postprocessing.

As a result we have that $I_{AB|\gamma}$ depends only on the invariant CM $\mathbf{V}_{ab|\gamma}$, so that we can write

$$I_{AB} = I_{AB|\gamma} \tag{10}$$

for any γ. Similarly, the entropies in Eq. (8) depends only on the invariant CM $\mathbf{V}_{ab|\gamma}$, so that

$$I_{E} = I_{E|\gamma} \tag{11}$$

for any γ. As a result, the conditional rate $R_{|\gamma}$ is invariant and coincides with the actual (average) rate of the protocol, i.e., $R = R_{|\gamma}$ for any γ. Equivalently, we may write

$$R = I_{AB} - I_{E}. \tag{12}$$

Thus, we can theoretically compute the rate R from the quantum CM $\mathbf{V}_{ab|\gamma}$ of the post-relay state $\rho_{ab|\gamma}$.

Now it is important to note that this CM can always be determined by the parties during the data comparison at the end of the protocol. In particular, it can be derived from the second-order statistical moments of the observed data. In fact, from the empirical distribution $p(\alpha, \beta, \gamma)$ or its Gaussian version $p_G(\alpha, \beta, \gamma)$, Alice and Bob derive the relation matrix $\mathbf{\Gamma}(\alpha, \beta, \gamma)$ and the complex CM $\mathbf{V}(\alpha, \beta, \gamma)$ [S4]. Setting $\alpha = (q_A + ip_A)/2$ and $\beta = (q_B + ip_B)/2$, these matrices are equivalent to a real CM for the quadratures

$$\mathbf{V}(q_A, p_A, q_B, p_B, q_-, p_+) = \begin{pmatrix} \mathbf{V}_{A\oplus B} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{R} \end{pmatrix}, \tag{13}$$

where $\mathbf{V}_{A\oplus B} := \mathbf{V}(q_A, p_A) \oplus \mathbf{V}(q_B, p_B)$ is Alice and Bob's reduced CM, $\mathbf{R}$ is the CM of the outcomes at the relay,

and $\mathbf{C}$ accounts for the correlations. Given the outcome γ, the conditional CM of Alice and Bob can be computed by Gaussian elimination and reads

$$\mathbf{V}(q_A, p_A, q_B, p_B|\gamma) = \mathbf{V}_{A\oplus B} - \mathbf{C}\mathbf{R}^{-1}\mathbf{C}^T. \quad (14)$$

In the entanglement-based representation of the protocol, we can easily put the previous CM in terms of Alice's and Bob's measurement outcomes, respectively,

$$\tilde{\alpha} = (\tilde{q}_A + i\tilde{p}_A)/2, \quad \tilde{\beta} = (\tilde{q}_B + i\tilde{p}_B)/2. \quad (15)$$

In fact, we can write

$$\mathbf{V}(q_A, p_A, q_B, p_B|\gamma) = \eta^{-2}\mathbf{V}(\tilde{q}_A, \tilde{p}_A, \tilde{q}_B, \tilde{p}_B|\gamma), \quad (16)$$

where parameter η is defined in Eq. (5) and accounts for the fact that the modulation is finite. Finally, the connection with the quantum CM is given by

$$\mathbf{V}(\tilde{q}_A, \tilde{p}_A, \tilde{q}_B, \tilde{p}_B|\gamma) = \mathbf{V}_{ab|\gamma} + \mathbf{I}, \quad (17)$$

where $\mathbf{I}$ is the vacuum shot-noise introduced by the heterodyne detections. The latter relation can be derived modelling each heterodyne detector as a quantum-limited amplifier (with gain 2) followed by a balanced beam splitter (with vacuum environment) which is conjugately homodyned at the output ports (one in the position and the other in the momentum quadrature).

Note that for the specific computation of the conditional entropy of Eq. (7), which enters in Eve's Holevo information and therefore the rate, one has to derive the conditional quantum CM $\mathbf{V}_{b|\gamma\tilde{\alpha}}$ of Bob's state $\rho_{b|\gamma\tilde{\alpha}}$ after Alice's heterodyne detection with outcome $\tilde{\alpha}$. For this calculation, we write $\mathbf{V}_{ab|\gamma}$ in the block form

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \mathbf{a} & \mathbf{c} \\ \mathbf{c}^T & \mathbf{b} \end{pmatrix}, \quad (18)$$

and we apply the formula [S1]

$$\mathbf{V}_{b|\gamma\tilde{\alpha}} = \mathbf{b} - \mathbf{c}^T(\mathbf{a} + \mathbf{I})^{-1}\mathbf{c}, \quad (19)$$

or equivalently [S5]

$$\mathbf{V}_{b|\gamma\tilde{\alpha}} = \mathbf{b} - \zeta^{-1}\mathbf{c}^T(\mathbf{\Omega}\mathbf{a}\mathbf{\Omega}^T + \mathbf{I})\mathbf{c}, \quad (20)$$

where ζ is defined in terms of trace and determinant as $\zeta := \det(\mathbf{a}) + \mathrm{Tr}(\mathbf{a}) + 1$, and

$$\mathbf{\Omega} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \quad (21)$$

Alternatively, we may compute

$$\mathbf{V}_{b|\gamma\tilde{\alpha}} = \mathbf{V}(\tilde{q}_B, \tilde{p}_B|\gamma\tilde{\alpha}) - \mathbf{I}, \quad (22)$$

where $\mathbf{V}(\tilde{q}_B, \tilde{p}_B|\gamma\tilde{\alpha})$ comes from $\mathbf{V}(\tilde{q}_A, \tilde{p}_A, \tilde{q}_B, \tilde{p}_B|\gamma)$ after Gaussian elimination of Alice's outcome variables.

To derive an explicit formula for the secret-key rate, we consider a realistic form for the coherent Gaussian attack. The mathematical details of this attack are fully discussed in the next section. Then, in Sec. I E we will explicitly compute the analytical expression of the rate.

D. Realistic Gaussian attack against the links

Consider the scenario depicted in Fig. 8, which is the entanglement-based representation of our protocol subject to a realistic Gaussian attack against the two links. This two-mode Gaussian attack is characterized by two beam splitters with transmissivities τ_A (for Alice's link) and τ_B (for Bob's link). Using these beam splitters, Eve mixes the incoming modes, A and B, with two ancillary modes, E_1 and E_2, extracted from a reservoir of ancillas. After the beam splitters, the output ancillas, E_1' and E_2', are stored in a quantum memory (together with all the other ancillas in the reservoir).

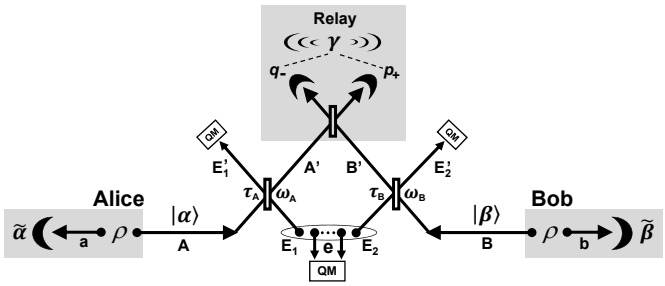

FIG. 8: Protocol in the entanglement-based representation. Continuous-variable Bell relay is correctly operated while a two-mode Gaussian attack is performed against the two quantum links (see text for more details).

The reduced state $\sigma_{E_1E_2}$ of E_1 and E_2 is Gaussian with zero mean-value and CM in the normal form

$$\mathbf{V}_{E_1E_2} = \begin{pmatrix} \omega_A\mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B\mathbf{I} \end{pmatrix}, \quad \begin{matrix} \mathbf{I} := \mathrm{diag}(1,1), \\ \mathbf{G} := \mathrm{diag}(g, g'). \end{matrix} \quad (23)$$

Here $\omega_A \geq 1$ is the variance of the thermal noise introduced by E_1 in Alice's link, while $\omega_B \geq 1$ is the variance of the thermal noise introduced by E_2 in Bob's link. The correlations between E_1 and E_2 are determined by the block $\mathbf{G}$ whose elements, g and g', must satisfy a set of *bona-fide* conditions [S6, S7]. Note that the previous normal form is very general since any two-mode CM can be put in this form by local Gaussian operations [S1].

For given values of thermal noise $\omega_A, \omega_B \geq 1$, Eve's CM $\mathbf{V}_{E_1E_2}$ is fully determined by the correlation parameters g and g', which can be represented as a point in a 'correlation plane'. To better describe this plane, we need to write the bona-fide conditions for g and g', which are derived by imposing the uncertainty principle [S6]

$$\mathbf{V}_{E_1E_2} > 0, \ \nu_-^2 \geq 1, \quad (24)$$

where ν_- is the least symplectic eigenvalue of $\mathbf{V}_{E_1E_2}$. In particular, we have [S1]

$$2\nu_-^2 = \Delta - \sqrt{\Delta^2 - 4\det\mathbf{V}_{E_1E_2}}, \quad (25)$$

where $\Delta = \omega_A^2 + \omega_B^2 + 2gg'$.

The positivity $\mathbf{V}_{E_1E_2} > 0$ provides the constraints

$$|g| < \sqrt{\omega_A \omega_B},\ |g'| < \sqrt{\omega_A \omega_B}, \tag{26}$$

while $\nu_-^2 \geq 1$ provides an inequality $f(\omega_A, \omega_B, g, g') \geq 1$ which is symmetric with respect to the origin and the bisector $g' = -g$. On the bisector $g' = -g$ we have that $f \geq 1$ corresponds to $|g'| \leq \phi$ where

$$\phi := \min\left\{\sqrt{(\omega_A - 1)(\omega_B + 1)}, \sqrt{(\omega_A + 1)(\omega_B - 1)}\right\}. \tag{27}$$

The previous bona-fide conditions must be satisfied by g and g' for any $\omega_A, \omega_B \geq 1$. They imply that the correlation plane is accessible only in a limited region around its origin, whose border is determined by ω_A and ω_B. A numerical example for $\omega_A = 5$ and $\omega_B = 2$ is provided in Fig. 9. The accessible region always forms a continuous and convex set, apart from the singular case $\omega_A = 1$ or $\omega_B = 1$, where it collapses into its origin $g' = g = 0$.

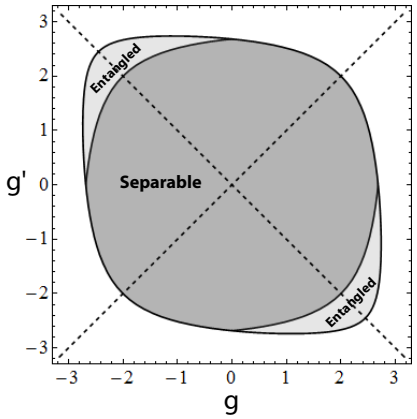

FIG. 9: Correlation plane (g, g') for $\omega_A = 5$ and $\omega_B = 2$. Points in the external white area are not accessible (having correlations too strong to be compatible with quantum mechanics). Accessible points (i.e., satisfying the bona-fide conditions) are represented by the delimited region, which is further divided in sub-regions. The inner darker area corresponds to separable attacks, while the two peripheral areas correspond to entangled attacks. The two dashed lines represent the two bisectors $g' = g$ and $g' = -g$.

The accessible region of the correlation plane can be further divided into sub-regions, corresponding to attacks performed with separable or entangled ancillas E_1 and E_2. In fact, we can easily write the separability condition for Eve's reduced state $\sigma_{E_1E_2}$ by considering the least partially-transposed symplectic eigenvalue $\tilde{\nu}_-$ of its CM $\mathbf{V}_{E_1E_2}$. This positive eigenvalue is determined by

$$2\tilde{\nu}_-^2 = \tilde{\Delta} - \sqrt{\tilde{\Delta}^2 - 4 \det \mathbf{V}_{E_1E_2}}, \tag{28}$$

where $\tilde{\Delta} = \omega_A^2 + \omega_B^2 - 2gg'$. Then, we have $\sigma_{E_1E_2}$ separable if and only if $\tilde{\nu}_-^2 \geq 1$. This corresponds to another inequality $\tilde{f}(\omega_A, \omega_B, g, g') \geq 1$ which is now symmetric with respect to the origin and the bisector $g' = g$. Thus, within the accessible region, we have an inner area of attacks performed with separable ancillas ($\tilde{\nu}_-^2 \geq 1$), that we call 'separable attacks', and two peripheral areas of attacks performed with entangled ancillas ($\tilde{\nu}_-^2 < 1$), that we call 'entangled attacks' (see Fig. 9).

Among the separable attacks, the simplest one is the origin of the plane, where Eve's state is a tensor product $\sigma_{E_1} \otimes \sigma_{E_2}$. This attack consists of two independent entangling cloners, i.e., two beam splitters mixing the travelling modes with two independent thermal modes, part of two EPR states. Apart from this singular case, all other separable attacks have correlated noise, with the two ancillary modes E_1 and E_2 possessing quantum correlations (non-zero quantum discord) and possibly entangled with extra ancillas $\mathbf{e}$ in the reservoir.

For the entangled attacks, it is essential to distinguish between the two peripheral regions. For attacks in the bottom-right region ($g > 0$ and $g' < 0$), Eve injects 'good' entanglement. She injects EPR correlations of the type $\hat{q}_{E_1} \approx \hat{q}_{E_2}$ and $\hat{p}_{E_1} \approx -\hat{p}_{E_2}$, helping the Bell detection (which projects on the same kind of correlations $\hat{q}_{A'} \approx \hat{q}_{B'}$ and $\hat{p}_{A'} \approx -\hat{p}_{B'}$). We call the 'positive EPR attack' the most entangled attack in this region, which is the bottom-right point with $g = \phi$ and $g' = -\phi$.

By contrast, for attacks in the top-left region ($g < 0$ and $g' > 0$), Eve injects 'bad' entanglement with EPR correlations of the type $\hat{q}_{E_1} \approx -\hat{q}_{E_2}$ and $\hat{p}_{E_1} \approx \hat{p}_{E_2}$. These correlations tend to destroy those established by the Bell detection. In particular, we call the 'negative EPR attack' the most entangled state $\sigma_{E_1E_2}$ in this region, which is the top-left point with $g = -\phi$ and $g' = \phi$.

E. Analytical derivation of the secret-key rate

Having completely characterized the description of the realistic Gaussian attack against the two links, we can now derive the corresponding secret-key rate of the protocol under such an attack. As previously discussed in Sec. I C, this rate is completely determined by the quantum CM $\mathbf{V}_{ab|\gamma}$ of Alice's and Bob's remote modes a and b after the action of the relay. The first step is therefore the computation of the post-relay CM $\mathbf{V}_{ab|\gamma}$ coming from the scenario in Fig. 8.

In Sec. I H we explicitly compute

$$\mathbf{V}_{ab|\gamma} = \begin{pmatrix} \mu\mathbf{I} & \mathbf{0} \\ \mathbf{0} & \mu\mathbf{I} \end{pmatrix} - (\mu^2 - 1)\times \\ \times \begin{pmatrix} \frac{\tau_A}{\theta} & 0 & -\frac{\sqrt{\tau_A\tau_B}}{\theta} & 0 \\ 0 & \frac{\tau_A}{\theta'} & 0 & \frac{\sqrt{\tau_A\tau_B}}{\theta'} \\ -\frac{\sqrt{\tau_A\tau_B}}{\theta} & 0 & \frac{\tau_B}{\theta} & 0 \\ 0 & \frac{\sqrt{\tau_A\tau_B}}{\theta'} & 0 & \frac{\tau_B}{\theta'} \end{pmatrix}, \tag{29}$$

where we have set

$$\theta := (\tau_A + \tau_B)\,\mu + \lambda,\ \theta' := (\tau_A + \tau_B)\,\mu + \lambda', \tag{30}$$

and the lambdas are defined as

$$\lambda := \kappa - ug > 0,\ \lambda' := \kappa + ug' > 0, \tag{31}$$

with

$$\kappa := (1-\tau_A)\omega_A + (1-\tau_B)\omega_B, \tag{32}$$

$$u := 2\sqrt{(1-\tau_A)(1-\tau_B)}. \tag{33}$$

In the limit of high modulation $\mu \gg 1$, the symplectic spectrum [S1] of $\mathbf{V}_{ab|\gamma}$ takes the asymptotic expressions

$$\{\nu_1, \nu_2\} = \left\{ \frac{|\tau_A - \tau_B|}{\tau_A + \tau_B}\mu,\ \frac{\sqrt{\lambda\lambda'}}{|\tau_A - \tau_B|} \right\} \quad \text{for } \tau_A \neq \tau_B, \tag{34}$$

and

$$\{\nu_1, \nu_2\} = \left\{ \sqrt{\frac{\lambda\mu}{2\tau_B}},\ \sqrt{\frac{\lambda'\mu}{2\tau_B}} \right\} \quad \text{for } \tau_A = \tau_B. \tag{35}$$

For the next calculations it is useful to compute the CMs of Bob's reduced state $\rho_{b|\gamma}$ and Bob's state $\rho_{b|\gamma\tilde{\alpha}}$ conditioned on Alice's detection. These CMs can easily be derived from $\mathbf{V}_{ab|\gamma}$. In particular, we have

$$\mathbf{V}_{b|\gamma} = \begin{pmatrix} \mu - \frac{(\mu^2-1)\tau_B}{\theta} & 0 \\ 0 & \mu - \frac{(\mu^2-1)\tau_B}{\theta'} \end{pmatrix}, \tag{36}$$

$$\mathbf{V}_{b|\gamma\tilde{\alpha}} = \begin{pmatrix} \mu - \frac{(\mu^2-1)\tau_B}{\tau_A+\tau_B\mu+\lambda} & 0 \\ 0 & \mu - \frac{(\mu^2-1)\tau_B}{\tau_A+\tau_B\mu+\lambda'} \end{pmatrix}, \tag{37}$$

with $\mathbf{V}_{b|\gamma\tilde{\alpha}}$ having the symplectic eigenvalue

$$\nu = \tau_B^{-1}\sqrt{(\tau_A+\lambda)(\tau_A+\lambda')} \ \text{ for } \mu \gg 1. \tag{38}$$

1. Alice and Bob's mutual information

Having determined the post-relay CM, we can now proceed with the derivation of the rate. First, let us compute the mutual information of Alice and Bob $I_{AB} = I(\tilde{\alpha}, \tilde{\beta}|\gamma)$. The outcomes $\tilde{\alpha}$ and $\tilde{\beta}$ of Alice's and Bob's detectors are associated with the classical CM given in Eq. (17). In particular, Bob's reduced CM is equal to

$$\mathbf{V}_{B|\gamma} := \mathbf{V}(\tilde{q}_B, \tilde{p}_B|\gamma) = \mathbf{V}_{b|\gamma} + \mathbf{I}. \tag{39}$$

Then, Bob's CM conditioned to Alice's outcome $\tilde{\alpha}$ is

$$\mathbf{V}_{B|\gamma\tilde{\alpha}} := \mathbf{V}(\tilde{q}_B, \tilde{p}_B|\gamma\tilde{\alpha}) = \mathbf{V}_{b|\gamma\tilde{\alpha}} + \mathbf{I}. \tag{40}$$

The previous CMs are all diagonal $\mathbf{V} = \mathrm{diag}(V^q, V^p)$. Since the two quadratures are modulated independently, the mutual information I_{AB} is given by the sum of the two terms, one for each quadrature. Explicitly, we have

$$I_{AB} = \frac{1}{2}\log_2 \frac{V^q_{B|\gamma}}{V^q_{B|\gamma\tilde{\alpha}}} + \frac{1}{2}\log_2 \frac{V^p_{B|\gamma}}{V^p_{B|\gamma\tilde{\alpha}}} = \frac{1}{2}\log_2 \Sigma, \tag{41}$$

where

$$\Sigma := \frac{1 + \det \mathbf{V}_{b|\gamma} + \mathrm{Tr}\mathbf{V}_{b|\gamma}}{1 + \det \mathbf{V}_{b|\gamma\tilde{\alpha}} + \mathrm{Tr}\mathbf{V}_{b|\gamma\tilde{\alpha}}}. \tag{42}$$

We can always re-write the mutual information in terms of a signal-to-noise ratio as

$$I_{AB} = \log_2 \frac{\mu}{\chi} = \log_2 \frac{\varphi+1}{\chi}, \tag{43}$$

where the equivalent noise $\chi = \mu\Sigma^{-1/2}$ can be computed from Σ, which in turn depends on the post-relay CM $\mathbf{V}_{ab|\gamma}$, known to the parties from the observed statistics $p(a, \beta|\gamma)$. For large modulation $\mu \gg 1$, we derive

$$\chi = \frac{\tau_A + \tau_B}{\tau_A\tau_B}\sqrt{(\tau_A+\tau_B+\lambda)(\tau_A+\tau_B+\lambda')}, \tag{44}$$

where the equivalent noise is expressed in terms of all parameters of the attack, i.e., $\chi = \chi(\tau_A, \tau_B, \omega_A, \omega_B, g, g')$.

2. Eve's Holevo information

In order to bound Eve's stolen information on Alice's outcome variable $\tilde{\alpha}$, we use the Holevo quantity

$$I_E = S(\rho_{ab|\gamma}) - S(\rho_{b|\gamma\tilde{\alpha}}). \tag{45}$$

The first entropy term $S(\rho_{ab|\gamma})$ can be computed from the symplectic spectrum $\{\nu_1, \nu_2\}$ of $\mathbf{V}_{ab|\gamma}$. In particular, we have

$$S(\rho_{ab|\gamma}) = h(\nu_1) + h(\nu_2), \tag{46}$$

where the h-function is defined as

$$h(x) := \left(\tfrac{x+1}{2}\right)\log_2\left(\tfrac{x+1}{2}\right) - \left(\tfrac{x-1}{2}\right)\log_2\left(\tfrac{x-1}{2}\right), \tag{47}$$

$$\simeq \log_2\left(\frac{ex}{2}\right) + O\left(\frac{1}{x}\right) \ \text{ for } x \gg 1. \tag{48}$$

For large modulation ($\mu \gg 1$), the spectrum $\{\nu_1, \nu_2\}$ is given by Eqs. (34) and (35). Correspondingly, we derive the following asymptotic formula for the entropy

$$S(\rho_{ab|\gamma}) = \begin{cases} S_{\neq} & \text{for } \tau_A \neq \tau_B, \\ S_{=} & \text{for } \tau_A = \tau_B, \end{cases} \tag{49}$$

where

$$S_{\neq} := h\left(\frac{\sqrt{\lambda\lambda'}}{|\tau_A - \tau_B|}\right) + \log_2\left[\frac{e|\tau_A - \tau_B|\mu}{2(\tau_A+\tau_B)}\right], \tag{50}$$

$$S_{=} := \log_2\left(\frac{e^2\sqrt{\lambda\lambda'}\mu}{8\tau_B}\right). \tag{51}$$

For the second entropy term in Eq. (45), we have $S(\rho_{b|\gamma\tilde{\alpha}}) = h(\nu)$, where the symplectic eigenvalue ν takes the asymptotic expression given in Eq. (38).

Here it is important to note that $S(\rho_{ab|\gamma})$ is continuous in $\tau_A = \tau_B$. In other words, we have

$$S_{\neq} \to S_{=}, \ \text{ for } \tau_A \to \tau_B. \tag{52}$$

This continuity is inherited by the Holevo information I_E in Eq. (45) and by the rate computed in the next section.

3. Asymptotic secret-key rate

Using the previous formulas for Alice and Bob's mutual information and Eve's Holevo information, we can derive the secret-key rate of the protocol $R = I_{AB} - I_E$ for large modulation $\mu \gg 1$. This rate is expressed in terms of all parameters of the attack $R = R(\tau_A, \tau_B, \omega_A, \omega_B, g, g')$. For $\tau_A \neq \tau_B$, we find

$$R = h(\nu) - h\left(\frac{\sqrt{\lambda\lambda'}}{|\tau_A - \tau_B|}\right) + \log_2\left[\frac{2(\tau_A+\tau_B)}{e|\tau_A-\tau_B|\chi}\right], \quad (53)$$

with continuous limit in $\tau_A = \tau_B := \tau$, where it becomes

$$R = h(\nu) + \log_2\left(\frac{8\tau}{e^2\chi\sqrt{\lambda\lambda'}}\right). \quad (54)$$

Here the lambda parameters λ and λ' are given in Eq. (31), the eigenvalue ν is expressed by Eq. (38), and the equivalent noise χ is given in Eq. (44).

F. Minimum secret-key rate

The general formula in Eq. (53) is given in terms of all parameters of the attack τ_A, τ_B, ω_A, ω_B, g, and g'. While τ_A and τ_B are easily accessible from the first-order moments, the remaining parameters could be inaccessible to the parties, since they generally mix in determining the CM $\mathbf{V}_{ab|\gamma}$ of Eq. (29). For this practical reason, it is important to express the rate in terms of fewer parameters.

1. Minimization of the rate at fixed thermal noise

Let us start by assuming that Alice and Bob only know the transmissivities (τ_A and τ_B) and the thermal noise affecting each link (ω_A and ω_B). Given these four parameters, we minimize the rate $R(\tau_A, \tau_B, \omega_A, \omega_B, g, g')$ of Eq. (53) over all physical values of the correlation parameters, i.e., over all accessible points in the correlation plane (g, g'). In our analysis, it is sufficient to assume $\tau_A \neq \tau_B$, since we can extend the result to the symmetric configuration $\tau_A = \tau_B$ by continuity.

First it is important to note that the rate R in Eq. (53) depends on the correlation parameters (g, g') only via the lambdas, λ and λ', specified by Eq. (31). Since R is invariant under permutation $\lambda \leftrightarrow \lambda'$, it is symmetric with respect to the bisector $g' = -g$. This symmetry is also shown in the numerical example given in Fig. 10.

In the correlation plane, the set of accessible points is a convex set and symmetric with respect to the bisector $g' = -g$. Combining this topology with the symmetry of the rate R allows us to restrict its minimization to the accessible points along the bisector $g' = -g$. Setting $g' = -g$ corresponds to setting $\lambda' = \lambda = \kappa + ug'$ in the rate of Eq. (53), which gives

$$R(g' = -g) = H(\tau_A, \tau_B, \lambda) + L(\tau_A, \tau_B, \lambda), \quad (55)$$

where

$$H(\tau_A, \tau_B, \lambda) := h\left(\frac{\tau_A+\lambda}{\tau_B}\right) - h\left(\frac{\lambda}{|\tau_A-\tau_B|}\right), \quad (56)$$

$$L(\tau_A, \tau_B, \lambda) := \log_2\left[\frac{2\tau_A\tau_B}{e|\tau_A-\tau_B|(\tau_A+\tau_B+\lambda)}\right]. \quad (57)$$

It is easy to check that H and L are minimized by maximizing λ which, in turn, corresponds to maximizing g'. As we know from Sec. I D, the maximal accessible value of g' along the bisector $g' = -g$ is given by ϕ in Eq. (27). Thus, at fixed transmissivities (τ_A and τ_B) and thermal noise (ω_A and ω_B), the optimal coherent attack is given by $g' = -g = \phi$, which is the extremal top-left point in the accessible region of the correlation plane. As already discussed in Sec. I D, this entangled attack is a 'negative EPR attack' where Eve injects EPR correlations in the links which tend to destroy the effect of the Bell detection. By contrast, H and L are maximized by minimizing g', whose minimum accessible value along the bisector $g' = -g$ is given by $-\phi$. Thus, the rate is maximum in the extremal bottom-right point of the accessible region, corresponding to the 'positive EPR attack', where Eve injects EPR correlations helping the Bell detection.

Assuming that Eve performs the optimal attack, i.e., the negative EPR attack, the minimum rate of our protocol is equal to

$$R(\tau_A, \tau_B, \omega_A, \omega_B) = h\left(\frac{\tau_A+\lambda_{\rm opt}}{\tau_B}\right) - h\left(\frac{\lambda_{\rm opt}}{|\tau_A-\tau_B|}\right) + \log_2\left[\frac{2\tau_A\tau_B}{e|\tau_A-\tau_B|(\tau_A+\tau_B+\lambda_{\rm opt})}\right], \quad (58)$$

where

$$\lambda_{\rm opt} := \kappa + u\phi, \quad (59)$$

with κ and u defined in Eqs. (32) and (33). This rate is continuous in $\tau_A = \tau_B := \tau$, where it becomes

$$R(\tau, \omega_A, \omega_B) = h\left(\frac{\tau+\lambda_{\rm opt}}{\tau}\right) + \log_2\left[\frac{4\tau^2}{e^2(2\tau+\lambda_{\rm opt})\lambda_{\rm opt}}\right]. \quad (60)$$

As evident from Fig. 10, the negative EPR attack clearly outperforms the collective entangling-cloner attack (corresponding to the origin of the plane $g' = g = 0$). From this point of view, the security analysis of our protocol is clearly more complex compared to previous literature on continuous-variable quantum cryptography.

2. Minimization of the rate at fixed equivalent noise

Despite the complexity of the protocol, it is remarkable that we can further simplify its rate by expressing it in terms of three parameters only. In fact, suppose that Alice and Bob only access the values of the transmissivities (τ_A and τ_B) and the equivalent noise χ. This minimal knowledge on the attack is always guaranteed. In fact, as

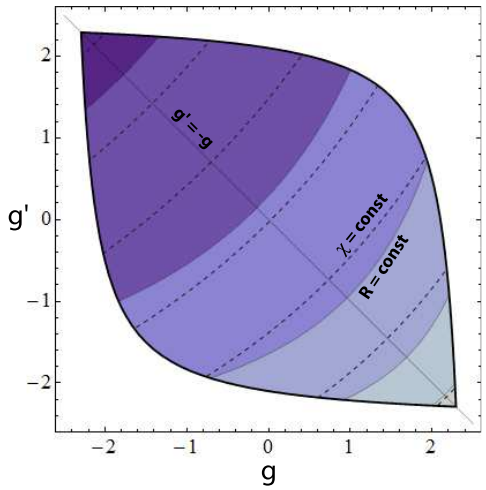

FIG. 10: **Minimization at fixed thermal noise**. The general rate R of Eq. (53) is plotted in the correlation plane (g, g') for $\tau_A = 0.9$, $\tau_B = 0.5$, and $\omega_A = \omega_B = 2.5$. The non-white area is the set of accessible points, which is convex and symmetric with respect to the bisector $g' = -g$. Within the accessible set, darker regions correspond to lower values of the rate. The rate is symmetric with respect to the bisector $g' = -g$, and decreasing towards the extremal top-left point of the accessible set (behavior is generic for any choice of the parameters τ_A, τ_B, ω_A and ω_B). **Mnimization at fixed equivalent noise**. We compare the iso-noise curves (χ=const) with the more concave iso-rate curves (R=const).

discussed in Sec. I E and specifically regarding Eq. (43), we have that the equivalent noise is uniquely determined by the post-relay CM $\mathbf{V}_{ab|\gamma}$ which is, in turn, reconstructed from the empirical statistics $p(\alpha, \beta|\gamma)$. Thus, given the three accessible parameters τ_A, τ_B and χ, we minimize the general rate R of Eq. (53), finding a simple formula for the minimum rate $R(\tau_A, \tau_B, \chi)$.

For this constrained minimization we can construct a Lagrangian and look for its critical points (procedure is involved and not reported here). More intuitively, we can find the minimum by directly comparing the rate and the equivalent noise on the correlation plane. On this plane, we plot the curves with the same rate R=const (iso-rate curves) and the curves with the same equivalent noise χ=const (iso-noise curves). As we can see from the numerical example in Fig. 10, the iso-rate curves are more concave than the iso-noise curves.

Combining this different concavity with the fact that the rate is decreasing from the bottom-right point to the top-left point of the accessible region, we find that the rate is minimized at the intersection of each iso-noise curve with the bisector $g' = -g$. In other words, moving along an iso-noise curve (χ=const) the rate is minimized at the point where $g' = -g$. Therefore we set $g' = -g$ in the rate $R(\tau_A, \tau_B, \omega_A, \omega_B, g, g')$ and we express the result in terms of the three basic parameters τ_A, τ_B and χ.

Given these parameters the minimum rate is equal to

$$R(\tau_A, \tau_B, \chi) = h\left(\tfrac{\tau_A \chi}{\tau_A+\tau_B} - 1\right) - h\left[\tfrac{\tau_A\tau_B\chi - (\tau_A+\tau_B)^2}{|\tau_A-\tau_B|(\tau_A+\tau_B)}\right] + \log_2\left[\frac{2(\tau_A+\tau_B)}{e|\tau_A-\tau_B|\chi}\right], \tag{61}$$

which is continuous in $\tau_A = \tau_B$, where it becomes

$$R(\chi) = h\left(\frac{\chi}{2} - 1\right) + \log_2\left[\frac{16}{e^2\chi(\chi-4)}\right]. \tag{62}$$

These latter two formulas represent our main theoretical result and coincide with Eqs. (2) and (3) of the main text.

We can always decompose the equivalent noise as

$$\chi = \chi_{\text{loss}}(\tau_A, \tau_B) + \varepsilon, \tag{63}$$

where

$$\chi_{\text{loss}}(\tau_A, \tau_B) := \chi|_{\omega_A=\omega_B=1} = \frac{2(\tau_A+\tau_B)}{\tau_A\tau_B} \tag{64}$$

is that part of the noise due to loss only, with the extra part ε known as the 'excess noise'. Adopting this decomposition of the noise, the rate of Eq. (61) can be re-written as $R = R(\tau_A, \tau_B, \varepsilon)$.

For the specific case $\varepsilon = 0$, we have a pure-loss attack of the links, where Eve's beam splitters mix the incoming modes with vacuum modes. The study of this simple attack is useful to estimate the maximum performance of the protocol (which clearly worsens for $\varepsilon > 0$). In a pure-loss attack, the minimum rate $R(\tau_A, \tau_B, 0)$ simplifies to

$$R(\tau_A, \tau_B) = h\left(\frac{2-\tau_B}{\tau_B}\right) - h\left(\frac{2-\tau_A-\tau_B}{|\tau_A-\tau_B|}\right) + \log_2\left(\frac{\tau_A\tau_B}{e|\tau_A-\tau_B|}\right), \tag{65}$$

which is continuous in $\tau_A = \tau_B := \tau$, where it becomes

$$R(\tau) = h\left(\frac{2-\tau}{\tau}\right) + \log_2\left[\frac{\tau^2}{e^2(1-\tau)}\right]. \tag{66}$$

One can easily check that Eq. (65) can also be achieved by specifying the previous rates of Eqs. (53) and (58) to the specific case of pure-loss ($\omega_A = \omega_B = 1$).

In the top panel of Fig. 11, we have plotted $R(\tau_A, \tau_B)$ as a function of the two transmissivities. We see that $R > 0$ occurs above a certain threshold which is asymmetric in the plane. In particular, for τ_A close to 1 we see that τ_B can be close to zero, identifying the optimal configuration of the protocol. Assuming standard optical fibres (0.2dB/km), this corresponds to having Alice close to the relay while Bob can be very far away as also shown in Fig. 4 in the main text. These results are proven to be robust with respect to the presence of excess noise $\varepsilon > 0$. This can be seen in the bottom panel of Fig. 11, where we plot $R(\tau_A, \tau_B, \varepsilon)$ for the high numerical value $\varepsilon = 0.1$.

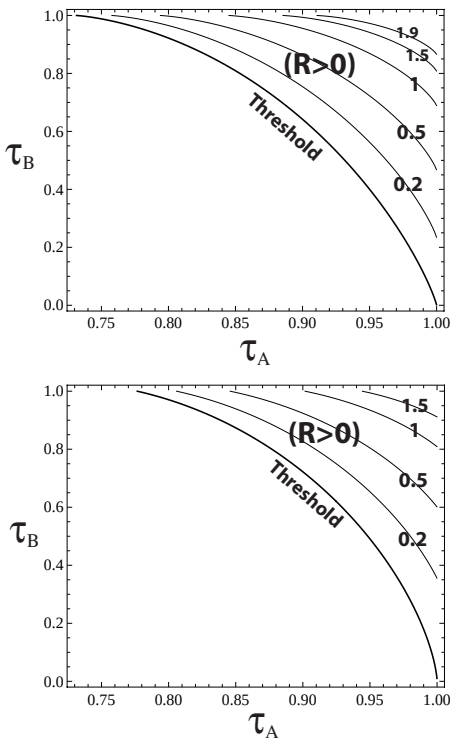

FIG. 11: Secret-key rate R (bits per relay use) as a function of the two transmissivities τ_A and τ_B. (Top) Rate $R(\tau_A, \tau_B)$ for a pure-loss attack ($\varepsilon = 0$). (Bottom) Rate $R(\tau_A, \tau_B, \varepsilon)$ for a coherent Gaussian attack with excess noise $\varepsilon = 0.1$.

G. Minimum rate in limit configurations

According to Fig. 11, the most interesting scenario is when the protocol is implemented in an asymmetric fashion with small loss in Alice's link ($\tau_A \simeq 1$). Therefore, let us analyze what happens in the limit for $\tau_A \to 1$. Assuming a fixed loss rate (e.g., 0.2dB/km), this corresponds to Alice approaching the relay (note that even if the Alice-relay distance becomes negligible, the relay must still be considered as a different device which is potentially operated by Eve). Taking the limit $\tau_A \to 1$ in Eq. (61), we find

$$R_{\tau_A \to 1} = h\left[\frac{1+(1-\tau_B)\omega_B}{\tau_B}\right] - h(\omega_B) + \log_2\left\{\frac{2\tau_B}{e(1-\tau_B)[1+\tau_B+(1-\tau_B)\omega_B]}\right\}. \quad (67)$$

This is a function of τ_B and ω_B only, as expected since the coherent Gaussian attack collapses into an entangling cloner attack affecting Bob's link only (with transmissivity τ_B and thermal noise ω_B).

It is important to note that the rate of Eq. (67) is identical to the reverse-reconcilation rate of a point-to-point 'no-switching' protocol from Alice to Bob which is based on random coherent states and heterodyne detection [S8] (see the Supplementary Information of Ref. [S9] for checking the asymptotic analytical expression of this rate). It is remarkable that the security performance of such a powerful protocol can be realized in the absence of a direct link between Alice and Bob by exploiting the intermediation of an untrusted relay in the proximity of Alice, i.e., the encoder of the secret information. Thanks to the equivalence with reverse reconciliation, we can achieve remarkably long distances for Bob. Ideally, if Bob's link were affected by pure loss only ($\omega_B = 1$), then we would have

$$R^{\rm loss}_{\tau_A \to 1} = h\left(\frac{2-\tau_B}{\tau_B}\right) + \log_2\left[\frac{\tau_B}{e(1-\tau_B)}\right], \quad (68)$$

which goes to zero only for $\tau_B \to 0$, corresponding to Bob being arbitrarily far from the relay.

We can also explain why the other asymmetric configuration with $\tau_B \simeq 1$ is not particularly profitable (at fixed loss rate this corresponds to Bob approaching the relay). Taking the limit $\tau_B \to 1$ in Eq. (61), we find

$$R_{\tau_B \to 1} = h\left[\tau_A + (1-\tau_A)\omega_A\right] - h(\omega_A) + \log_2\left\{\frac{2\tau_A}{e(1-\tau_A)[1+\tau_A+(1-\tau_A)\omega_A]}\right\}, \quad (69)$$

which depends on τ_A and ω_A only, as expected, since the attack must reduce to an entangling cloner attack versus Alice's link. Here it is important to note that Eq. (69) coincides with the direct-reconciliation rate of the point-to-point no-switching protocol [S8] (whose asymptotic analytical expression can be found in the Supplementary Information of Ref. [S9]). As we know this rate has a limited range. For instance, in the presence of pure loss ($\omega_A = 1$), we have

$$R^{\rm loss}_{\tau_B \to 1} = \log_2\left[\frac{\tau_A}{e(1-\tau_A)}\right], \quad (70)$$

which is zero at $\tau_A \simeq 0.73$, therefore limiting Alice's distance from the relay to about 6.8km in standard optical fibres (0.2dB/km).

It is clear that the symmetric configuration $\tau_A = \tau_B := \tau$ has a performance which must be somehow intermediate between the previous limit cases. More precisely the performance of the symmetric configuration is comparable with that of Bob approaching the relay. In fact, for pure-loss attacks ($\omega_A = \omega_B = 1$), we have the rate in Eq. (66), which goes to zero for $\tau \simeq 0.84$, therefore restricting Alice's and Bob's distances from the relay to about 3.8km in optical fibres (0.2dB/km). This means that the overall distance between Alice and Bob cannot exceed 7.6km when the relay is perfectly in the middle.

Finally, it is interesting to note how the Bell detection reverses the role of the two types of reconciliations. In fact, suppose to have an EPR source very close to Alice, who heterodynes one mode in order to encode the signal variable in the other mode being sent to Bob who is far away. In this scheme, Bob guessing Alice corresponds to direct reconciliation. If we now replace the EPR source with a relay performing a Bell detection on incoming modes, the situation is reversed and Bob guessing Alice becomes equivalent to reverse reconciliation.

H. Computation of the post-relay CM

In this technical section we explicitly compute the formula of Eq. (29) for the post-relay CM $\mathbf{V}_{ab|\gamma}$ corresponding to the scenario depicted in Fig. 8. At the input, Alice's modes a and A, Bob's modes b and B, and Eve's modes E_1 and E_2 are in a tensor-product state $\rho_{aA}\otimes\rho_{bB}\otimes\sigma_{E_1E_2}$, where $\rho_{aA}=\rho_{bB}=\rho$ is an EPR state with CM

$$\mathbf{V}(\mu)=\begin{pmatrix}\mu\mathbf{I} & \mu'\mathbf{Z}\\ \mu'\mathbf{Z} & \mu\mathbf{I}\end{pmatrix},\quad \mu':=\sqrt{\mu^2-1},\quad \mathbf{Z}:=\mathrm{diag}(1,-1), \tag{71}$$

and $\sigma_{E_1E_2}$ is Eve's zero-mean Gaussian state with CM $\mathbf{V}_{E_1E_2}$ in the normal form of Eq. (23). The global state is then a zero-mean Gaussian state with CM

$$\mathbf{V}_{aAbBE_1E_2}=\mathbf{V}(\mu)\oplus\mathbf{V}(\mu)\oplus\mathbf{V}_{E_1E_2}. \tag{72}$$

It is helpful to permute the modes so as to have the ordering $abAE_1E_2B$, where the upper-case modes are those transformed by the beam splitters. After reordering, the input CM has the explicit form

$$\mathbf{V}_{abAE_1E_2B}=\begin{pmatrix}\mu\mathbf{I} & \mathbf{0} & \mu'\mathbf{Z} & \mathbf{0} & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \mu\mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mu'\mathbf{Z}\\ \mu'\mathbf{Z} & \mathbf{0} & \mu\mathbf{I} & \mathbf{0} & \mathbf{0} & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \omega_A\mathbf{I} & \mathbf{G} & \mathbf{0}\\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{G} & \omega_B\mathbf{I} & \mathbf{0}\\ \mathbf{0} & \mu'\mathbf{Z} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mu\mathbf{I}\end{pmatrix}, \tag{73}$$

where $\mathbf{0}$ is the 2×2 zero matrix. Now the action of the two beam splitters with transmissivities τ_A and τ_B is described by the symplectic matrix

$$\mathbf{S}=\mathbf{I}\oplus\mathbf{I}\oplus\mathbf{S}(\tau_A)\oplus\mathbf{S}(\tau_B)^T, \tag{74}$$

where the identity matrices $\mathbf{I}\oplus\mathbf{I}$ act on the remote modes a and b, the beam splitter matrix

$$\mathbf{S}(\tau_A)=\begin{pmatrix}\sqrt{\tau_A}\mathbf{I} & \sqrt{1-\tau_A}\mathbf{I}\\ -\sqrt{1-\tau_A}\mathbf{I} & \sqrt{\tau_A}\mathbf{I}\end{pmatrix} \tag{75}$$

acts on modes A and E_1, and the transposed beam splitter matrix $\mathbf{S}(\tau_B)^T$ acts on modes E_2 and B.

The state describing the output modes $abA'E_1'E_2'B'$ after the beam splitters is a Gaussian state with zero mean and CM equal to

$$\mathbf{V}_{abA'E_1'E_2'B'}=\mathbf{S}\,\mathbf{V}_{abAE_1E_2B}\,\mathbf{S}^T. \tag{76}$$

After some algebra, we get

$$\mathbf{V}_{abA'E_1'E_2'B'}=\begin{pmatrix}\mathbf{V}_{ab} & \mathbf{W}_1 & \mathbf{W}_2\\ \mathbf{W}_1^T & \mathbf{V}_{A'E_1'} & \mathbf{W}_3\\ \mathbf{W}_2^T & \mathbf{W}_3^T & \mathbf{V}_{E_2'B'}\end{pmatrix}, \tag{77}$$

where the blocks along the diagonal correspond to the reduced CMs $\mathbf{V}_{ab}=\mu(\mathbf{I}\oplus\mathbf{I})$,

$$\mathbf{V}_{A'E_1'}=\begin{pmatrix}x_A\mathbf{I} & x_A''\mathbf{I}\\ x_A''\mathbf{I} & x_A'\mathbf{I}\end{pmatrix},\ \mathbf{V}_{E_2'B'}=\begin{pmatrix}x_B'\mathbf{I} & x_B''\mathbf{I}\\ x_B''\mathbf{I} & x_B\mathbf{I}\end{pmatrix}, \tag{78}$$

where we have set (for $k=A,B$)

$$x_k:=\tau_k\mu+(1-\tau_k)\omega_k, \tag{79}$$

$$x_k':=\tau_k\omega_k+(1-\tau_k)\mu, \tag{80}$$

$$x_k'':=\sqrt{\tau_k(1-\tau_k)}(\omega_k-\mu). \tag{81}$$

The off-diagonal blocks are given by

$$\mathbf{W}_1=\begin{pmatrix}\mu'\sqrt{\tau_A}\mathbf{Z} & -\mu'\sqrt{1-\tau_A}\mathbf{Z}\\ \mathbf{0} & \mathbf{0}\end{pmatrix}, \tag{82}$$

$$\mathbf{W}_2=\begin{pmatrix}\mathbf{0} & \mathbf{0}\\ -\mu'\sqrt{1-\tau_B}\mathbf{Z} & \mu'\sqrt{\tau_B}\mathbf{Z}\end{pmatrix}, \tag{83}$$

and

$$\mathbf{W}_3=\begin{pmatrix}\sqrt{(1-\tau_A)\tau_B}\mathbf{G} & \sqrt{(1-\tau_A)(1-\tau_B)}\mathbf{G}\\ \sqrt{\tau_A\tau_B}\mathbf{G} & \sqrt{\tau_A(1-\tau_B)}\mathbf{G}\end{pmatrix}. \tag{84}$$

Since we are interested in the output CM of Alice and Bob, we trace out E_1' and E_2', which corresponds to deleting the corresponding rows and columns in the CM of Eq. (77). As a result, we get the following reduced CM for modes $abA'B'$

$$\mathbf{V}_{abA'B'}=\begin{pmatrix}\mathbf{V}_{ab} & \mathbf{C}_1 & \mathbf{C}_2\\ \mathbf{C}_1^T & \mathbf{A} & \mathbf{D}\\ \mathbf{C}_2^T & \mathbf{D}^T & \mathbf{B}\end{pmatrix}, \tag{85}$$

where the various blocks are given by

$$\mathbf{A}=x_A\mathbf{I},\ \mathbf{B}=x_B\mathbf{I}, \tag{86}$$

$$\mathbf{D}=\sqrt{(1-\tau_A)(1-\tau_B)}\mathbf{G}, \tag{87}$$

and

$$\mathbf{C}_1=\begin{pmatrix}\mu'\sqrt{\tau_A}\mathbf{Z}\\ \mathbf{0}\end{pmatrix},\ \mathbf{C}_2=\begin{pmatrix}\mathbf{0}\\ \mu'\sqrt{\tau_B}\mathbf{Z}\end{pmatrix}. \tag{88}$$

From the CM of Eq. (85) we derive the CM $\mathbf{V}_{ab|\gamma}$ of the conditional remote state $\rho_{ab|\gamma}$ after the Bell measurement on modes A' and B'. For this derivation, we use the transformation rules for CMs under Bell-like measurements given in Ref. [S5]. From the blocks of the CM (85), we construct the following theta matrix

$$\mathbf{\Theta}:=\frac{1}{2}\left(\mathbf{ZAZ}+\mathbf{B}-\mathbf{ZD}-\mathbf{D}^T\mathbf{Z}\right). \tag{89}$$

After some simple algebra, we find

$$\mathbf{\Theta}=\frac{1}{2}\begin{pmatrix}\theta & 0\\ 0 & \theta'\end{pmatrix}, \tag{90}$$

whose diagonal elements are given in Eq. (30).

Then the conditional CM is given by the formula [S5]

$$\mathbf{V}_{ab|\gamma}=\mathbf{V}_{ab}-\frac{1}{2\det\mathbf{\Theta}}\sum_{i,j=1}^{2}\mathbf{C}_i(\mathbf{X}_i^T\mathbf{\Theta}\mathbf{X}_j)\mathbf{C}_j^T, \tag{91}$$

where

$$\mathbf{X}_1:=\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\ \mathbf{X}_2:=\begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}. \tag{92}$$

After some algebra, we find the expression in Eq. (29).

II. EXPERIMENTAL METHODS

In this section we start by providing a general description of the experimental setup, discussing the main optical elements involved in the implementation (Sec. II A). Then, in Sec. II B, we give a more detailed mathematical interpretation of the experiment, and we discuss the data post-processing together with the finite-size effects associated with the protocol.

A. General description of the optical setup

In our proof-of-principle experiment we used a highly stable laser at 1064nm which is split in equal portions and directed to the stations of Alice and Bob, providing them with a common local oscillator. In a future in-field implementation of the protocol, such a phase-locking of the beams can be achieved by atom-clock syncronization and classical communication between the parties. In general, the local oscillator could even be provided by the eavesdropper since does not contain any information about the encodings of Alice and Bob. Furthermore, it can be continuously monitored by the parties and suitably filtered to delete the presence of additional degrees of freedom (side-channel attacks [S10]).

At each of the stations (see Fig. 12), the laser beams are modulated using amplitude and phase electro-optical modulators that are fed by Gaussian modulated signals from independent electronic signal generators. The Gaussian modulations are white within the measurement bandwidth. Prior to modulation, the laser fields were polarized to a very high degree to ensure pure amplitude (phase) modulation produced by the amplitude (phase) modulator. Furthermore, the transverse profiles of the laser beams were made as large as possible in the modulator to ensure preservation of their Gaussian profiles.

At the relay, the two beams interfere at a balanced beam splitter with a visibility of 96% and their relative phase is actively controlled with a piezo mounted mirror to produce equally intense output beams. These beams are focused onto two balanced detectors and the resulting currents are subtracted and added in order to produce the difference of the amplitude quadratures and the sum of the phase quadratures, respectively. This method is a simple alternative to the standard eight-port measurement setup needed for the continuous-variable Bell detection and is enabled by the brightness of the carrier [S11]. As the subtraction and addition processes are performed in a software program, an imbalanced hardware-system can be compensated during the post-processing (See the next section for more details).

The measurements are carried out at the sideband frequency of 10.5MHz which is well separated from the carrier frequency thereby avoiding low frequency noise and thus ensuring quantum noise limited performance of the protocol. The power of the individual laser beams was

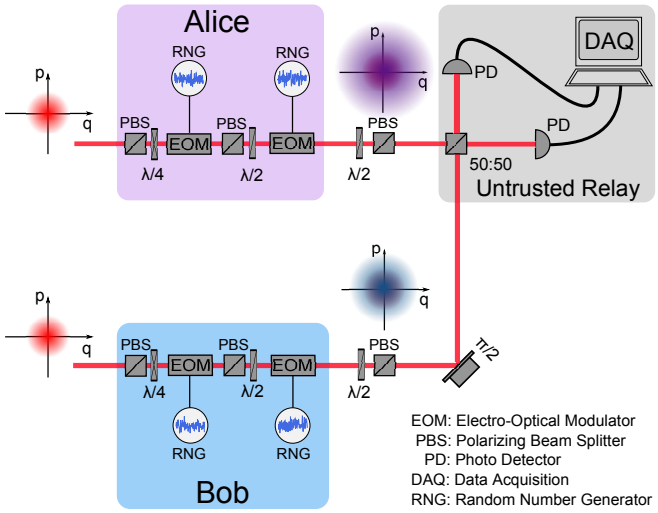

FIG. 12: Experimental setup (same as Fig. 5 in the main text). Alice and Bob apply amplitude and phase modulators to a pair of identical classical phase-locked bright coherent beams, providing a common local oscillator and coming from a highly stable laser (not shown). At the output, the two modes emerge randomly-displaced in the phase space according to a Gaussian distribution. In particular, Bob's modulation is suitably attenuated to simulate loss in his link. Bob's mode is then phase-shifted and merged with Alice's mode at the relay's balanced beam splitter. The two output ports are photodetected and processed to realize an equivalent continuous-variable Bell measurement.

1.4mW. The signal is mixed down to DC from 10.5MHz, low pass filtered at 100kHz and digitized with a sampling rate of 500kHz and 14bit resolution. Each data block consists of 10^6 data points corresponding to a measurement time of 2 seconds.

The modulation depth in Bob's link was reduced to simulate the transmission loss. A reduction in modulation is equivalent to a beam splitter induced transmission loss because both reduce the power in the sidebands. The difference is that a reduction in modulation depth keeps the power of the carrier (with respect to the sidebands) laser beam constant, which was experimentally convenient. This allows us to accurately simulate the transmission through the channels and thus test different communication realizations (see the next section for more details on this method).

B. Detailed mathematical description of the experiment and data post-processing

Consider the schematic of Fig. 12. The two input classical beams are identical and phase-locked, each providing a bright coherent state with amplitude iL ($L \gg 1$). Note that we have complete freedom in choosing the global phase of this oscillator, which is here set to π just for convenience of notation.

At the output of the modulators, Alice's and Bob's

annihilation operators can be written as $\hat{A} = iL + \hat{a}$ and $\hat{B} = iL + \hat{b}$, respectively. Before entering the second balanced beam splitter at the relay, Bob's mode is phase-shifted by $\pi/2$, so that the two output ports have roughly the same intensity. This is equivalent to transform Alice's mode as $\hat{A} \to i\hat{A}$ (since this is a relative shift, it can be mathematically applied to Alice or Bob). The output ports of the beam splitter are then described by the following annihilation operators

$$\hat{D}_0 = \frac{i\hat{A} + \hat{B}}{\sqrt{2}},\ \hat{D}_1 = \frac{i\hat{A} - \hat{B}}{\sqrt{2}}. \tag{93}$$

Each output port ($k = 0, 1$) is measured by a photodetector with photocurrent $i_k = c_k \hat{N}_k$, where $\hat{N}_k = \hat{D}_k^\dagger \hat{D}_k$ is the number operator, and c_k is an optical-to-current conversion factor. This factor is different for the two detectors, so that they have different levels of electronic shot-noise. To counterbalance this asymmetry, we can re-scale one of the currents by a real factor g. Thus, by re-scaling the currents and taking their sum and difference, we get

$$\Sigma_\pm := i_0 \pm g\ i_1 = c_0 \left(\hat{N}_0 \pm r \hat{N}_1 \right), \tag{94}$$

where $r := g c_1/c_0$. By expanding at the first order in the local oscillator L, we derive

$$\frac{\Sigma_+}{c_0} = (1+r)L^2 + \frac{L}{2}\left[(1-r)\hat{q}_- + (1+r)\hat{p}_+\right], \tag{95}$$

$$\frac{\Sigma_-}{c_0} = (1-r)L^2 + \frac{L}{2}\left[(1+r)\hat{q}_- + (1-r)\hat{p}_+\right]. \tag{96}$$

The next step is subtracting the offset of the local oscillator which is equivalent to subtracting the mean values $\langle \Sigma_\pm \rangle = c_0(1 \pm r)L^2$. The result is normalized dividing by the standard deviation of the vacuum fluctuations

$$\sigma_\pm = \sqrt{\langle \Sigma_\pm^2 \rangle_{\rm vac} - \langle \Sigma_\pm \rangle_{\rm vac}^2} = c_0 L \sqrt{\frac{1+r^2}{2}}. \tag{97}$$

Thus, we get

$$\frac{\Sigma_+ - \langle \Sigma_+ \rangle}{\sigma_+} = \hat{x}_{+r},\quad \frac{\Sigma_- - \langle \Sigma_- \rangle}{\sigma_-} = \hat{x}_{-r}, \tag{98}$$

where

$$\hat{x}_{+r} := \kappa_1 \hat{q}_- + \kappa_2 \hat{p}_+ \tag{99}$$

is a linear combination $\hat{q}_-$ and $\hat{p}_+$, with coefficients

$$\kappa_1 = \frac{1-r}{\sqrt{2(1+r^2)}},\ \kappa_2 = \frac{1+r}{\sqrt{2(1+r^2)}}. \tag{100}$$

We can rewrite the linear combination of Eq. (99) as

$$\hat{x}_{+r} = \frac{1-r}{1+r}\ \kappa_2 \hat{q}_- + \kappa_2 \hat{p}_+, \tag{101}$$

and include the factor κ_2 in Alice's and Bob's classical modulations. In fact, the quantum variables can always be decomposed as

$$\hat{q}_- = q_- + \hat{q}_-^{\rm vac},\ \hat{p}_+ = p_+ + \hat{p}_+^{\rm vac}, \tag{102}$$

where q_- and p_+ are the classical parts, with $\hat{q}_-^{\rm vac}$ and $\hat{p}_+^{\rm vac}$ accounting for vacuum noise. Then, we can write

$$\hat{x}_{+r} = \frac{1-r}{1+r} q_- + p_+ + \hat{\delta}_+^{\rm vac}, \tag{103}$$

where $\hat{\delta}_+^{\rm vac}$ is vacuum noise and the classical variables have been re-scaled as

$$\kappa_2 q_- \to q_-,\ \kappa_2 p_+ \to p_+. \tag{104}$$

This is equivalent to re-scaling Alice's and Bob's classical variables

$$\kappa_2 \begin{pmatrix} q_A \\ p_A \\ q_B \\ p_B \end{pmatrix} \to \begin{pmatrix} q_A \\ p_A \\ q_B \\ p_B \end{pmatrix}, \tag{105}$$

so that their new variables are Gaussianly-modulated with a re-scaled variance $\kappa_2^2 \varphi \to \varphi$. Similarly to Eq. (103), we derive

$$\hat{x}_{-r} = q_- + \frac{1-r}{1+r} p_+ + \hat{\delta}_-^{\rm vac}. \tag{106}$$

Thus, the outcome of the relay is generally given by the pair (x_{-r}, x_{+r}) or equivalently $\gamma_r := (x_{-r} + i x_{+r})/\sqrt{2}$, where r is a parameter which can be optimized. Note that, for $r = 1$, we have $\hat{x}_{+1} = \hat{p}_+$ and $\hat{x}_{-1} = \hat{q}_-$. In general, for the presence of quadrature asymmetries and q-p correlations (coming from the cross-talk between the amplitude and phase modulators), the optimal value of r may be different from 1, e.g., in the range $0.45 \div 0.75$ in our experiment. This optimization is a simple operation which enables us to counterbalance some of the technical imperfections in our setup. Similar optimizations could also be exploited in potential in-field implementations of the protocol (given an observed statistics, Alice and Bob can always assume an optimized relay and ascribe all the noise to the coherent attack of the links.)

In order to use Eqs. (103) and (106), we need to access the experimental values of Alice's and Bob's optical displacements $(q_A, p_A, q_B, p_B)^T$. Therefore we have to compute the electro-optical gains of the modulators, for both amplitude and phase (i.e., position and momentum on top of the bright local oscillator). These gains $\{t_1, t_2, t_3, t_4\}$ convert the applied electronic displacements $\{\mathcal{A}_q, \mathcal{B}_q, \mathcal{A}_p, \mathcal{B}_p\}$ into the optical quadrature displacements. For their computation, we minimize the following variances

$$\left\langle \left[\hat{x}_{-r} - \frac{t_1 \mathcal{A}_q - t_2 \mathcal{B}_q}{\sqrt{2}} \right]^2 \right\rangle, \tag{107}$$

$$\left\langle \left[\hat{x}_{+r} - \frac{t_3 \mathcal{A}_p + t_4 \mathcal{B}_p}{\sqrt{2}} \right]^2 \right\rangle. \tag{108}$$

Once these gains are known, we can experimentally determine the optical displacements of Alice and Bob as

$$q_A = t_1 \mathcal{A}_q, \; q_B = t_2 \mathcal{B}_q, \tag{109}$$

$$p_A = t_3 \mathcal{A}_p, \; p_B = t_4 \mathcal{B}_p. \tag{110}$$

The classical modulations in the optical quadratures are approximately equal, with a maximal variance of $\varphi \simeq 65$ vacuum-noise units. In order to simulate beam splitters in the links, we equivalently attenuate the classical modulations $\varphi_A = V(q_A) \simeq V(p_A)$ and $\varphi_B = V(q_B) \simeq V(p_B)$. In fact, an ensemble of Gaussian-modulated coherent states is described by an average state which is thermal with quantum variance $\mu = \varphi + 1$, where φ is the classical modulation and 1 is the variance of the vacuum noise. By sending a thermal state with such a variance through a beam splitter with transmissivity τ (in a vacuum environment), we get the output variance

$$V = \tau(\varphi + 1) + 1 - \tau = \tau\varphi + 1. \tag{111}$$

This is equivalent to removing the beam splitter and sending a thermal state with quantum variance $\tau\varphi + 1$, i.e., Gaussian-modulated coherent states with a reduced modulation $\tau\varphi$.

Thus, Bob's modulation is taken to be $\varphi_B = \tau_B \varphi$ with τ_B being the equivalent transmissivity of the beam splitter. We have considered several values of τ_B down to about 4×10^{-4}, corresponding to 34dB loss (equivalent to 170km in optical fibre at 0.2dB/km). Alice's modulation is fixed to be maximal $\varphi_A \simeq \varphi$, simulating the scenario where Alice's link has $\tau_A \simeq 1$ (small effects due to non-unit quantum efficiencies of the detectors and non-unit beam splitter visibility have been neglected by suitably re-scaling Alice's modulation). Note that, in a future real-time implementation of the protocol, Alice's transmissivity can indeed be very close to 1 by using photodiodes with high quantum efficiencies (∼98%).

Thus, in our experiment we realize the conditions

$$\hat{x}_{-r} \simeq \frac{q_A - \sqrt{\tau_B} q_B}{\sqrt{2}} + \frac{1-r}{1+r} \frac{p_A + \sqrt{\tau_B} p_B}{\sqrt{2}} + \hat{\delta}_-^{\rm vac}, \tag{112}$$

$$\hat{x}_{+r} \simeq \frac{1-r}{1+r} \frac{q_A - \sqrt{\tau_B} q_B}{\sqrt{2}} + \frac{p_A + \sqrt{\tau_B} p_B}{\sqrt{2}} + \hat{\delta}_+^{\rm vac}, \tag{113}$$

which connect Alice's amplitude $\alpha := (q_A + i p_A)/2$, Bob's amplitude $\beta := (q_B + i p_B)/2$, and the relay outcome $\gamma_r := (x_{-r} + i x_{+r})/\sqrt{2}$ under a pure-loss attack of Bob's link. One can easily check that, for $r = 1$, the previous Eqs. (112) and (113) become

$$\hat{q}_- \simeq \frac{q_A - \sqrt{\tau_B} q_B}{\sqrt{2}} + \hat{\delta}_-^{\rm vac}, \tag{114}$$

$$\hat{p}_+ \simeq \frac{p_A + \sqrt{\tau_B} p_B}{\sqrt{2}} + \hat{\delta}_+^{\rm vac}. \tag{115}$$

For any experimental value of τ_B, we have considered an optimized relay (with optimal r published) and collected 10^6 values of α, β and γ_r. The value of τ_B is accessible to Alice and Bob by computing and comparing the first moments of their data which must follow Eqs. (112) and (113). Their estimate is in good agreement with the applied attenuation. The parties can also derive the global classical CM $\mathbf{V}(q_A, p_A, q_B, p_B, x_{-r}, x_{+r})$ by comparing a subset of their data. Once this is known, they can derive the secret key rate of the protocol.

Before proceeding, let us first discuss the experimental finite-size effects involved in the estimate of the first- and second-order moments. As we can see from Fig. 13, the asymptotic values of the statistical moments are already reached after $\simeq 10^5$ rounds of the protocol (for the second-order moments we have plotted the scaled determinant of the global CM, i.e., $\det \mathbf{V}_n / \det \mathbf{V}_\infty$, where n is the variable number of rounds and $\infty = 10^6$). Thus, the parties rapidly reach the asymptotic regime, where the finite-size effects on the key rate can be neglected (see again Fig. 13 for the rate). Thus the parties just need to compare $\simeq 10^5$ points in order to estimate the asymptotic values of the statistical moments. Clearly, this represents a negligible subset of data in a real-time implementation of the protocol where the number of rounds can be $\gg 10^5$ (e.g., $> 10^9$ in Ref. [S12]).

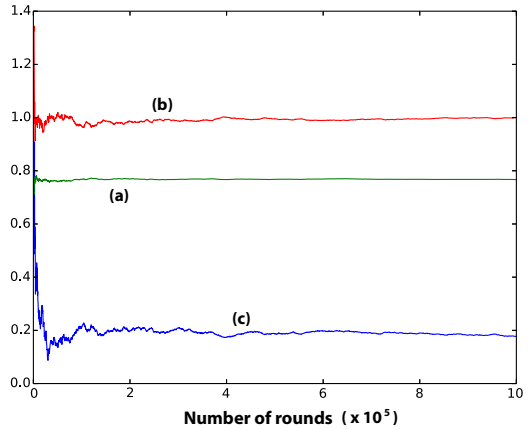

FIG. 13: As the number of rounds of the protocol increases up to 10^6, we plot Alice and Bob's estimate of the transmissivity τ_B (a), the estimate of the scaled determinant of the global CM $\mathbf{V}$ (b) and the estimate of the key rate of the protocol (c). Asymptotic values are quickly reached after about 10^5 experimental points. This behaviour is generic in r (here we have chosen $r = 1$) and for the various experimental points (here we have chosen $\tau_B \simeq 0.77$).

Let us now derive the experimental key rate from the global CM $\mathbf{V}(q_A, p_A, q_B, p_B, x_{-r}, x_{+r})$. The first step is to perform the Gaussian elimination of the relay variables in order to construct the conditional CM $\mathbf{V}_{\rm cond} := \mathbf{V}(q_A, p_A, q_B, p_B | \gamma_r)$ according to Eqs. (13) and (14). This conditional matrix has still some asymmetries in the quadratures plus residual q-p correlations. These imperfections can be counterbalanced by Alice and Bob by performing local rotations and re-scalings of their classical data α and β. By means of these local symplectic transformations, the conditional matrix is trans-

formed into a normal form

$$\mathbf{V}_{\rm cond} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix} \rightarrow \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix}, \tag{116}$$

where $a = \sqrt{\det \mathbf{A}}$, $b = \sqrt{\det \mathbf{B}}$ and c is determined by computing the other two symplectic invariants $\det \mathbf{V}$ and $\det \mathbf{A} + \det \mathbf{B} + 2 \det \mathbf{C}$.

Once Alice and Bob have symmetrized the conditional CM, they derive the quantum CM $\mathbf{V}_{ab|\gamma_r}$ in the equivalent entanglement-based representation of the protocol. According to Eq. (16) and (17), this is given by

$$\mathbf{V}_{ab|\gamma_r} = \eta^2 \mathbf{V}_{\rm cond} - \mathbf{I}, \tag{117}$$

where η is the parameter of Eq. (5) and accounts for the finite modulation ($\eta \simeq 1.01$ in the experiment, where $\eta = 1$ is the asymptotic regime of infinite modulation).

From $\mathbf{V}_{ab|\gamma_r}$ we can easily extract the reduced CM $\mathbf{V}_{b|\gamma_r}$ and compute the doubly-conditional CM $\mathbf{V}_{b|\gamma_r\tilde{\alpha}}$ via Eq. (19) or (20). These matrices provide Alice and Bob's mutual information I_{AB} according to Eqs. (41) and (42). Then, we compute Eve's Holevo information I_E using Eq. (45), where the entropies of $\rho_{ab|\gamma_r}$ and $\rho_{b|\gamma_r\tilde{\alpha}}$ are computed from the symplectic spectra of $\mathbf{V}_{ab|\gamma_r}$ and $\mathbf{V}_{b|\gamma_r\tilde{\alpha}}$, respectively. Finally, we can derive the experimental rate

$$R = \xi I_{AB} - I_E, \tag{118}$$

where ξ is the reconciliation efficiency, with ideal value $\xi = 1$ and current achievable value of $\xi \simeq 97\%$ [S13]. The corresponding rates are plotted in the main text and compared with the theoretical curves. According to these final results, our adjustment of the experimental imperfections is not perfect, with some residual noise affecting our data. Such noise affects the rate in the same way as a coherent Gaussian attack with excess noise $\varepsilon \lesssim 0.02$.

[S1] Weedbrook, C., Pirandola, S., Garcia-Patron, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H. & Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).

[S2] García-Patrón, R. & Cerf, N. J. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, **97**, 190503 (2006).

[S3] Pirandola, S., Vitali, D., Tombesi, P. & Lloyd, S. Macroscopic entanglement by entanglement swapping. *Phys. Rev. Lett.* **97**, 150403 (2006).

[S4] Picinbono, B. Second-order complex random vectors and normal distributions. *IEEE Trans. Sig. Proc.* **44**, 2637–2640 (1996).

[S5] Spedalieri, G., Ottaviani, C. & Pirandola, S. Covariance matrices under Bell-like detections. *Open Syst. Inf. Dyn.* **20**, 1350011 (2013).

[S6] Pirandola, S., Serafini, A. & Lloyd, S. Correlation matrices of two-mode bosonic systems. *Phys. Rev. A* ***79***, 052327 (2009).

[S7] Pirandola, S. Entanglement reactivation in separable environments. *New J. Phys.* **15**, 113046 (2013).

[S8] Weedbrook, C., Lance, A. M., Bowen, W. P., Symul, T., Ralph, T. C. & Lam, P. K. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).

[S9] Pirandola, S., Mancini, S., Lloyd, S. & Braunstein, S. L. Continuous-variable quantum cryptography with two-way quantum communication. *Nature Phys.* **4**, 726 (2008).

[S10] Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Phys. Rev. Lett.* **108**, 130502 (2012).

[S11] Niset, J., Acín, A., Andersen, U. L., Cerf, N. J., García-Patrón, R., Navascués, M., & Sabuncu, M. Superiority of entangled measurements over all local strategies for the estimation of product coherent states. *Phys. Rev. Lett.* **98**, 260404 (2007).

[S12] Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics* **7**, 378–381 (2013).

[S13] Jouguet, P., Kunz-Jacques, S., & Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **84**, 062317 (2011).