Master thesis: High-rate multipartite quantum secret sharing with continuous variables

Jacopo Angeletti

Quantum cryptography has undergone substantial growth and development within the multi-disciplinary field of quantum information in recent years. The field is constantly advancing with new protocols being developed, security measures being improved, and the first practical applications of these technologies being deployed in optical fibers and free space optical beams. In this paper, we present a comprehensive review of a cutting-edge metropolitan-scale protocol for continuous-variable quantum cryptography. The protocol allows an arbitrary number of users to send modulated coherent states to a relay, where a generalised Bell detection creates secure multipartite correlations. These correlations are then distilled into a shared secret key, providing a secure method for quantum secret-sharing. This novel approach to quantum cryptography has the potential to offer high-rate secure multipartite communication using readily available optical components, making it a promising advancement in the field.

Keywords: quantum information, quantum optics, quantum cryptography, continuous-variable, multipartite Bell detection

Tuesday 7$^{\text{th}}$ April, 2020

I. INTRODUCTION

Quantum key distribution (QKD) [1, 2] with continuous-variable (CV) systems [3] has garnered significant attention in recent years. The design of CV-based QKD protocols utilizing Gaussian quantum states of optical beams has proven to be particularly effective, and these states can now be easily produced in laboratory settings. The ideal implementation of QKD protocols that utilize CV systems [4, 5] and Gaussian states [6] has the potential to approach the PLOB bound [7, 8], which is the ultimate limit of point-to-point communication. These advancements demonstrate the exciting progress and potential for continued development in the field of QKD with CV systems. Recently, there has been a significant push towards an end-to-end approach that can be applied to network implementations [9–11]. This approach utilizes an intermediate relay as a means of communication, allowing parties to perform measurement-device-independent (MDI) QKD protocols [10, 12], even if the relay is untrusted. This development provides a solution that can greatly benefit network implementations and has garnered significant attention in the field.

We analyze a cutting-edge multipartite protocol for secure quantum secret-sharing (QSS) that utilizes CV systems and an MDI configuration. This protocol can be easily implemented using linear optics and provides a secure method for key distribution. In this protocol, an arbitrary number of users are divided into groups and send Gaussian-modulated coherent states to an untrusted relay. A generalized multipartite Bell detection is performed at the relay and the results are publicly broadcast. QSS enables the distribution of a secret key among all users, which requires their collaboration for validity. In the case of non-collaboration, a threshold behavior is manifested and allows for the detection of "dummy" users, leading to the potential abort of the protocol. This multipartite protocol based on CV systems and MDI configuration provides a promising solution for secure key distribution in a network setting.

Consider a configuration where users are distributed asymmetrically around a relay station and analyze the security of the protocol against collective attacks. In this scenario, we assume that Eve uses independent entangling cloners [7, 13] and analyze the asymptotic regime of many (ideally infinite) exchanged signals. The links connecting the parties to the relay are modeled as memory-less thermal-loss channels, with the assumption that users in the same ensemble share both common transmissivity and thermal noise. Under these realistic conditions, we demonstrate that the protocol is suitable for metropolitan-scale areas. For example, the ultimate limit for bipartite secure communication still allows for the establishment of a secret key between two groups in a noisy environment within a radius of 10 km.

The paper is organized as follows: in Sec. II, we describe the communication scheme. Sec. III A focuses on the analysis of bi-partitions of users for a thermal-loss channel. In Sec. III B, we examine two specific configurations, referred to as the *Y*- and *X*-schemes, which allow for secure secret-sharing among three and four groups, respectively. Finally, in Sec. IV, we summarize our findings and provide concluding remarks. To facilitate a deeper understanding of the protocol, the mathematical tools used in our analysis are provided in the appendices.

II. DESCRIPTION OF THE COMMUNICATION SCHEME

We provide the definition of a generic secret-sharing protocol as follows:

Definition 1 *An* (M, N)-*threshold scheme is a procedure for dividing a message into* N *pieces, called shadows or shares, such that no subset of fewer than* M *shadows can reveal the message, but any set of* M *shadows can be used to reconstruct it [14].*

To illustrate this concept, consider the scenario of Alice setting up a launch program for a nuclear warhead from a remote location. To ensure that the launch cannot be initiated by a single person, she divides the launch code into N parts, and distributes them among N individuals. These shares are encrypted and contain no information about the original launch code individually. However, if M individuals cooperate, they

Figure 1. (a) Illustration of a group of N users organized into M ensembles, each consisting of N_j users, where $j = \{1, \ldots, M\}$, such that $\sum_{j=1}^{M} N_j \leq N$. The possible presence of "dummy" users is represented in red. The ensembles are arranged at different distances from the relay, while the users within each ensemble are at equal distances from the relay (Note: the illustration may not be entirely accurate in terms of distances between ensembles and relay). (b) **(General)** Prepare and measure (PM) implementation of the QSS scheme for $N = 7$ users, with $N_1 = 3$ in group "1", and $N_2 = 4$ users in group "2". It may be generalised to an arbitrary number M of groups, each with a different number N_j of users users. Each user, referred to as "Bob," sends a Gaussian-modulated coherent state with amplitude $|\alpha_k\rangle$ to an untrusted relay through an optical link described by a thermal-loss channel Φ_j. At the relay, the incoming states undergo a generalised multipartite Bell detection, performed through a cascade of beamsplitters and homodyne detectors. The beamsplitters have transmissivities $T_1 = 1$ and $T_k = 1 - k^{-1}$ for $k = \{2, \ldots, N\}$, while the homodyne detectors measure either the $\hat{q}$ or the $\hat{p}$ quadrature, as described in the figure. The outcome, $\gamma := (p, q_2, \ldots, q_N)$ is broadcast to the Bobs, so that *a posteriori* correlations are created among their local variables $\alpha_1, \ldots, \alpha_N$. These correlations are used to extract a secret key for QSS. **(Attack)** Sample of the protocol in the EB representation, where each thermal-loss channel Φ_j is characterised by its transmissivity η_j and thermal noise $\omega_j = 2\bar{n}_j + 1$.

would be able to reconstruct the complete launch code. This makes it more challenging for any single person to gain unauthorized access, as they would need to collude with $M - 1$ others.

In order to perform a QSS protocol, consider an arbitrary number N of trusted users (referred to as "Bobs") arranged into M groups, with N_j users in each group, where $j = \{1, \ldots, M\}$. The sum of all users in the groups should not exceed N (see Fig. 1a), and when $\sum_{j=1}^{M} N_j = N$, we refer to this as the "full-house" case. The users send random Gaussian-modulated coherent states $|\alpha_k\rangle$ through a thermal-loss channel Φ_j to an untrusted relay, where a generalized multipartite Bell detection is performed, as depicted in Fig. 1b. The relay is modeled as an N-port interferometer consisting of N beam-splitters, with increasing transmittivities $T_1 = 1$ to $T_k = 1 - k^{-1}$ for $k = \{2, \ldots, N\}$, followed by N homodyne detections. The first output is measured in $\hat{p}$, while the rest are $\hat{q}$-homodyned, where $\hat{q}$ and $\hat{p}$ are the two quadrature operators of the optical mode such that $[\hat{q}, \hat{p}] = 2i$. The outcome $\gamma := (p, q_2, \ldots, q_N)$ is broadcast to all Bobs, who can then remove the local displacement caused by the measurements. Further mathematical details are provided in App. A.

The theoretical assessment of the protocol is performed in the entanglement-based (EB) representation. In this representation, each source of coherent states is represented by a two-mode squeezed vacuum (TMSV) state $\hat{\rho}_{AB}$, which undergoes heterodyne detection. The $\hat{B}$ modes are kept at each user's station, while the $\hat{A}$ modes are sent to the relay for detection.

As a result, each user is equipped with a TMSV state $\hat{\rho}_{AB}$ that has a zero mean and a covariance matrix (CM) that is equal to

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

where $\mathbf{Z} = \text{diag}\{1, -1\}$, $\mathbf{I} = \text{diag}\{1, 1\}$, $1 \leq \mu := \cosh 2r \in \mathbb{R}$ [15], and the modes are ordered as $\left(\hat{q}^A, \hat{p}^A, \hat{q}^B, \hat{p}^B\right)^T$. Here, r is the squeezing parameter. By heterodyning mode $\hat{B}$, each Bob remotely prepares a coherent state $|\beta\rangle$ on mode $\hat{A}$, the amplitude of which is modulated by a complex Gaussian with variance $\mu - 1$. For large modulation $\mu \gg 1$, the outcome of the measurement $\tilde{\beta} \simeq \alpha^*$ is approximately equal to the projected amplitude α. The CM of the TMSV state $\hat{\rho}_{AB}$ Eq. (1), upon the action of the channel Φ_j, undergoes the transformation

$$\mathbf{V}'_{AB} = \begin{pmatrix} x_j\mathbf{I} & z_j\mathbf{Z} \\ z_j\mathbf{Z} & y\mathbf{I} \end{pmatrix}, \quad (2)$$

with $j = \{1, \ldots, M\}$. Here, each thermal-loss channel Φ_j is characterized by its transmissivity η_j and thermal noise ω_j, such that

$$\begin{aligned} x_j &= \eta_j\mu + \left(1 - \eta_j\right)\omega_j, \\ y &= \mu, \\ z_j &= \sqrt{\eta_j\left(\mu^2 - 1\right)}. \end{aligned} \quad (3)$$

Figure 2. Unitary entanglement localisation in M-symmetric states. Within each group, users cooperate to concentrate the entanglement they share, and we can describe the situation from the point of view of M "super users," which are the M groups of users.

After the Bell measurement and communication of the outcome γ, the modes $\hat{\mathbf{B}} := \hat{B}_1 \cdots \hat{B}_N$ are projected onto a symmetric N-mode Gaussian state (see also App. B). The users are divided into M groups, each consisting of N_j members, and the global state is represented by $\rho_{\mathbf{M}|\gamma}$, where $\hat{\mathbf{M}} := \hat{N}_1 \cdots \hat{N}_M$ represents all the members of the M groups. The members of each group can apply local operations (LOs) [16] on $\rho_{\mathbf{M}|\gamma}$ to establish a common secret key among the M groups. These local Gaussian operations concentrate the quantum correlations of all the Bobs, transforming $\rho_{\mathbf{M}|\gamma}$ into an effective M-mode Gaussian state $\rho_{M|\gamma}$ with CM [17] [18]

$$\mathbf{V}_{M|\gamma} = \begin{pmatrix} \mathbf{\Gamma}_{11} & \mathbf{\Gamma}_{12} & \cdots & \mathbf{\Gamma}_{1M} \\ \mathbf{\Gamma}_{21} & \mathbf{\Gamma}_{22} & \cdots & \mathbf{\Gamma}_{2M} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{\Gamma}_{M1} & \mathbf{\Gamma}_{M2} & \cdots & \mathbf{\Gamma}_{MM} \end{pmatrix}, \tag{4}$$

where [19]

$$\mathbf{\Gamma}_{ij} = y\mathbf{I}\,\delta_{ij}$$
$$- z_i z_j \mathrm{diag}\left(\frac{\delta_{ij} \sum_{k \neq i} N_k \mathfrak{X}^{(ki)} - \left(1 - \delta_{ij}\right) \mathfrak{X}^{(ij)}}{\sum_{k \neq i} N_k \mathfrak{X}^{(i)}}, \frac{\sqrt{N_i N_j}}{\sum_{k=1}^{M} N_k x_k} \right), \tag{5}$$

with δ_{ij} the Kronecker delta, and

$$\mathfrak{X}^{(\alpha\beta)} := \prod_{k \neq \alpha \neq \beta} x_k. \tag{6}$$

As a result, we can consider the situation from the perspective of M aggregated entities, commonly referred to as "super users," which correspond to the M groups into which the users are divided. This is shown in Fig. 2. For more information on this process, refer to App. C.

We consider the practical limitations that arise during the implementation of the multipartite Bell detection. The presence of inefficiencies in the detectors is accounted for by including detector efficiencies $\tau < 1$ in the homodyne measurements. This is achieved through the use of N beam splitters with transmissivity τ. In CV-Bell detections, it is possible to attain high efficiencies at both optical and telecom frequencies, both with and without fiber components. Despite the technical difficulties, homodyne detection can reach detection efficiencies of up to 90% [13, 20, 21].

To account for the finite effects due to a limited number of exchanged signals between the parties, we must consider the reconciliation efficiency ξ of the classical codes used for error correction and privacy amplification [1, 2]. Despite being crucial for extracting a secret key, this process typically has an efficiency $\xi < 1$, with typical values ranging from $\xi \simeq 0.95 \div 0.985$ [22–27]. In addition to this, there may be other imperfections that arise from the relay, such as the asymmetric behavior of the interferometer beamsplitters [11]. However, this case is nontrivial and requires numerical solutions, and is therefore not considered in this analysis.

Assuming asymptotic security and infinite Gaussian modulation [28], the secret-key rate of the protocol against collective attacks is simply given by [1]

$$R = \xi I_{\mathbf{B}|\gamma} - \chi_{E|\gamma}. \tag{7}$$

For practical purposes, the secret-key rate must be optimized over the modulation parameter μ, as outlined in App. D. To analyze the potential performance of the protocol, we will focus on scenarios that are suitable for experimental testing, by considering the cases with $M = \{2, 3, 4\}$.

III. RESULTS

A. Bipartite system

In a QSS session, users are divided into $M = 2$ groups, referred to as group "1" and group "2", with group "2" positioned deeper [29] in the interferometer and serving as the decoder [30] (see also App. E). As shown in Fig. 3, the performance of the protocol is evaluated in terms of the secret-key rate, measured in bits per channel use, as a function of the distance d_1 between group "1" and the relay (measured in kilometers for a standard optical fiber with 0.2 dB/km attenuation). The relay is fixed at a distance of $d_2 = 0$ km from group "2". The notation used is the following

Definition 2 *A splitting of the kind "X/Y" means that X% (Y%) of all users belongs to group "1" ("2").*

In Fig. 3, we compare the optimal rate for different channel types (thermal- and pure-loss) and detection efficiencies, with group "2" fixed at the relay and group "1" at varying distances. The parameters of the thermal-loss channel are detailed in the figure caption. Our Gaussian QSS scheme achieves outstanding performance compared to qubit-based protocols, with secret key rates that are at least three orders of magnitude higher [31], over comparable distances, for which one has $\lesssim 10^{-4}$ bit/use at $\lesssim 25$ km. If symmetric configuration was limited to 3.8 km, our apparatus can reach a maximum distance of 170 km in standard optical fibers, with a high key rate of 2×10^{-4} bit/use. With a clock of 25 MHz, this corresponds to a key rate of the order of 2.5 Mbits/sec for all users.

Figure 3. Secret-key rates (in bits per use) for two optimally distributed groups, as a function of the distance d_1 (in km, for a standard optical fiber) of group "1", with group "2" fixed at the relay ($d_2 = 0$ km). The different curves correspond to different parameter settings: black ($\omega_1 = \omega_2 = \tau = 1$), dashed green ($\omega_1 = 1$, $\omega_2 = 1.1$, $\tau = 1$), red ($\omega_1 = \omega_2 = 1$, $\tau = 0.98$), dashed purple ($\omega_1 = 1$, $\omega_2 = 1.1$, $\tau = 0.98$), orange ($\omega_1 = 1.1$, $\omega_2 = 1 = \tau = 1$), dashed blue ($\omega_1 = \omega_2 = 1.1$, $\tau = 1$), yellow ($\omega_1 = 1.1$, $\omega_2 = 1$, $\tau = 0.98$), and dashed gray ($\omega_1 = \omega_2 = 1.1$, $\tau = 0.98$). The performances of the protocol, whether ideal (black and orange curves) or not (red and yellow curves), are not significantly affected by the presence of noise in the nearest group (dashed green, blue, purple, and gray curves). However, in the case of thermal noise corresponding to $\omega_1 = 1.1$ SNU and a detection efficiency of $\tau = 98\%$, the performance is reduced by about 150%.

The optimal bipartition corresponds to the "full-house" case and symmetric splitting, resulting in the same best (ideal) performance as standard CV-MDI-QKD [7, 12] in its asymmetric configuration (black curve). This is possible because the state $\rho_{2|\gamma}$ is independent from the number of users N. Our results show that, while imperfections and noise do have a general destructive effect, they do not appreciably affect the performance of the protocol (solid and dashed line coincide). However, the presence of thermal noise with $\omega_1 = 1.1$ SNU and a detection efficiency of $\tau = 98\%$ reduces the performance by about 150%. These results highlight the feasibility of high-rate secure CV-MDI-QKD QSS in a noisy environment at a metropolitan scale.

1. Secret-key rate versus group distance

In this study, we examine the behavior of the secret-key rate with respect to the distance of one of the two groups, while the other is fixed. We vary the distance $d_i = \{0.1\,\text{km},\ 1\,\text{km},\ 10\,\text{km}\}$ of one of the groups from the relay. We focus on the full-house case for different splittings, including 50/50, 5/95, and 1/99. The 50/50 splitting is also analyzed in a noisy environment.

The trends [32] in the secret-key rate behavior with respect to the distance of a group are presented in Fig. 4. Our analysis shows that for a pure-loss channel, the performance is worse

Figure 4. performance of the protocol in terms of secret-key rate (in bits per use) as a function of the distance of one of the groups (in km, for a standard optical fiber), with the distance of the other group fixed at $d_i = 0.1$ km. Figures a and b differ in which group is fixed. The different curves correspond to different splitting ratios: 50/50 (red, black, green, and purple), 5/95 (blue), and 1/99 (gray). We also consider different amounts of noise added to the optimal 50/50 configuration, with noise parameters of $\omega_1 = \omega_2 = 1$ (red, blue, and gray), $\omega_1 = 1$, $\omega_2 = 1.1$ (black), $\omega_1 = 1.1$, $\omega_2 = 1$ (purple), and $\omega_1 = \omega_2 = 1.1$ (green). The plots are invariant with respect to asymmetrical splittings when there is no injection of noise, implying no depth effects induced by the relay. The best performance is achieved for the optimal 50/50 splitting, with the deepest group in the interferometer closest to the relay, resulting in an improvement of a factor of 10 compared to the symmetric protocol [11]. The ultimate limit for bipartite secure communication still allows for the establishment of a secret key between two groups at a metropolitan scale within a radius of $d_2 = 10$ km (not shown). Noise is more tolerable in the nearest group, where the performance is not significantly affected.

when the splittings are extreme and does not vary [33] with asymmetrical splittings. This indicates that there are no depth effects induced by the relay. Despite this, we are pleased to find that the ultimate limit for bipartite secure communication still allows for the establishment of a secret key between two groups within a radius of 10 km in a metropolitan scale (not shown). When studying the impact of noise, we observe that in the case of asymmetrical noise [34], the group closer to the relay can tolerate more noise in its link, and the performance is not significantly affected. At present, reasonable values of excess noise are in the range of $\epsilon = 0.04 \div 0.05$ SNU [35], which express the incredible tolerance of our protocol to noise, despite the conversion from excess noise to thermal noise ω not being immediate.

Finally, Fig. 5 further (see Fig. **??**) illustrates the impact

of distance on the secret-key rate when considering non-ideal reconciliation efficiency ($\xi \leq 1$). As expected, the rate decrease as the distance increases, and the impact of imperfect reconciliation becomes more pronounced. The results clearly demonstrate the need for efficient reconciliation to achieve high secret-key rates over large distances.

Figure 5. Secret-key rates (bits per use) are plotted against the distance d_1 (in km, for a standard optical fiber) of the superficial group "1" in a two-group setup, where group "2" is fixed at a distance of $d_2 = 0.1$ km. The groups are optimally distributed in a 50/50 ratio. The figure shows the impact of reconciliation efficiency on the secret-key rates, with different curves representing different values of reconciliation efficiencies. Moving from right to left, the values are ξ = 1, 0.985, 0.98, 0.95, and 0.90. As expected, the secret-key rate decreases with decreasing reconciliation efficiency. The results highlight the importance of high reconciliation efficiency to achieve a higher secret-key rate in quantum key distribution protocols.

2. Threshold behaviour

The results of this study, depicted in Fig. 6, showcase the threshold behavior characteristic of QSS. As depicted, when one or more users do not cooperate, the performance drops significantly, which allows for easy detection and potential termination of the session.

Our study focuses on determining the maximum distance achievable by one group of users, d_j^{max} [36], as a function of the number of users N, while keeping the distance of another group fixed at d_i. Three different types of user bipartitions were considered. As previously stated, the optimal split of 50/50 (represented by orange in the figure) has a performance that does not depend on N. Additionally, we analyze the cases where one "dummy" user is present in each group, leading to two scenarios: $N_1 = N/2 - 1$, $N_2 = N/2$ (purple) and $N_1 = N/2$, $N_2 = N/2 - 1$ (blue).

We also considered the scenario where two dummy users are present, resulting in three possible combinations: $N_1 = N_2 = N/2 - 1$ (red), $N_1 = N/2 - 2$, $N_2 = N/2$ (brown), or $N_1 = N/2$, $N_2 = N/2 - 2$ (pink). Our analysis shows that, regardless of the user group positioning, the worst effect occurs when users of the shallowest group do not cooperate, implying possible depth effects.

Figure 6. Maximum fiber distance for the QSS protocol, plotted for three different types of bipartitions of the users. The optimal 50/50 splitting (orange curves) exhibits performance that is independent of N. We consider the scenario with one dummy Bob per group, i.e., $N_1 = N/2 - 1$ and $N_2 = N/2$ (purple curves), or vice versa, $N_1 = N/2$ and $N_2 = N/2 - 1$ (blue), and two dummy Bobs, $N_1 = N_2 = N/2 - 1$ (red), or $N_1 = N/2 - 2$ and $N_2 = N/2$ (brown), or vice versa, $N_1 = N/2$ and $N_2 = N/2 - 2$ (pink). The protocol performance is always the worst when the users in the shallowest group do not cooperate. In (a), we compare the performance with the corresponding pure-loss channel (gray). In (b), we consider the case of reconciliation efficiency $\xi = 0.985$ for the worst-case scenario of one dummy Bob in group "1". Any configuration of two dummy users produces a negative rate. The introduction of reconciliation efficiency lowers the curves and makes the threshold behavior more pronounced when compared with the ideal $\xi = 1$ case (gray).

The introduction of reconciliation efficiency has a compressing effect on the rate, making the threshold behavior even more pronounced, as can be seen in Fig. 6(b).

B. M-partite systems: Y- and X-schemes

We present a study of a specific configuration in which there are $M = 3$ groups, each with $N_j = N/M$ users and a pure-loss channel with equal excess noise, $\omega_j = 1$ for $j = \{1, 2, 3\}$, resulting in an optimal M-partition. The details of this setup are discussed in App. F. In the Y-scheme configuration, the third group, located farthest from the relay, is placed at a distance of d_3, while the first and second groups are positioned at an equal distance $d_{1/2}$ from the relay. This configuration is depicted in Fig. 7a. Additionally, the relay can be configured to act as a switch, connecting two groups at a time, as shown in Fig. 7b.

The impact of the distance $d_{1/2}$ of the shallowest group on

Figure 7. Schematic diagram of a *Y*-scheme with three groups. Group "3" is the deepest in the interferometer, located at a distance of d_3 from the relay, while groups 1" and "2" are equidistant from the relay at a distance of $d_{1/2}$. (b) The relay can also function as a switch, allowing the two superficial groups to communicate directly without passing through the deepest group.

Figure 8. Secret-key rate (in bits per use) as a function of the distance (in kilometers, for standard optical fiber) at which two groups are placed from the relay, while the deepest group in the interferometer is fixed at a distance d_{deep}, with $deep = \{2, 3\}$. The red, blue, and black curves correspond to distances d_3 of 100 m, 50 m, and 10 m, respectively. The secret key rate is robust to changes in the distance d_3. Operating the relay as a switch yields a threefold improvement. The inset shows that the performance worsens when going from two to three groups. Specifically, we compare the red curve with $M = 2$, $N_j = N/2$ (green) and $M = 2$, $N_1 = 2N/3$, $N_2 = N/3$ (black).

the secret-key rate can be seen in Fig. 8, where the fixed distance of the deepest group, $d_3 = \{10\,\text{m}, 50\,\text{m}, 100\,\text{m}\}$, is kept constant. The two sets of curves in the figure represent two different relay configurations, with the right set representing the switch case, which enhances the performance by a factor of nearly three.

The inset provides a visual comparison to highlight the scaling. When considering an analogous two-group scenario, with the deepest group, i.e., group "2", located $d_2 = 100\,\text{m}$ from the relay, and varying the distance d_1 of the other group, secure communication at a distance of nearly 60 km can be achieved even with a non-optimal split of $N_1 = 2N/3$ and $N_2 = N/3$. However, adding a third group results in a drastic drop in performance that stabilizes immediately afterwards (if other groups are to be added). In a *Y*-scheme with an op-

Figure 9. Comparison of the secret-key rate (bit/use) for a non-ideal tripartite *Y*-scheme (red), a switch configuration (blue), and the ideal case (gray), corresponding to Fig. 8.

timal three-partition, the restriction is to approximately 1 km, while four groups permit secure communication up to approximately 600 m. Finally, Fig. 9 presents the results of the same scenario as Fig. 8 but with non-ideal Bell detection. Fig. 8

Figure 10. The *Y*-scheme and *X*-scheme are two ways to arrange four groups for secure key distribution.

demonstrates the robustness of the secret-key rate to changes in d_3 for both operational modes of the relay. The scalability of the scheme is further proven by the extension to four groups in the *Y*-scheme set-up shown in Fig. 10. The deepest group (group "4") is located at a distance d_4 from the relay, while the other three groups ("1", "2", and "3") are positioned at an equal distance $d_{1/2/3}$ from the relay. In addition, we analyze another configuration, known as the *X*-scheme, in which the users are distributed with an optimal *M*-partition of the form $N_j = N/M$, where $M = 4$. In this configuration, groups "1" and "2" are positioned at a distance $d_{1/2}$ from the relay, while groups "3" and "4" are positioned at a distance $d_{3/4}$ from the relay (as shown in Fig. 10). The secret-key rate of the protocol as a function of the distance $d_{1/2}$ of the first two groups, with the other distances $d_{3/4}$ fixed, is shown in Fig. 11. As the best protocol performance is achieved when the deepest group(s) in the interferometer is (are) located closer to the relay, we fix their distance. When distributed in a *X*-scheme (represented by green curves), the four groups perform better (by approximately less than 15%) than they would in a *Y*-scheme (represented by red curves). This is because the larger the number

Figure 11. Secret-key rate (bit/use) as a function of the distance (in km, for standard optical fiber) between the relay and the deepest group in the interferometer, for different distances between the other two groups and two fixed values of the deepest group's distance: d_{deep} = 100 m (red), 50 m (blue), and 10 m (black), corresponding to depths $deep$ = {4, 3/4}, respectively. The X-scheme (green) outperforms the Y-scheme (red) by less than 15%. The robustness to changes in d_{deep} is similar for both schemes.

of users closer to the relay, the better the performance.

IV. CONCLUSIONS

We have presented a novel multipartite CV-MDI-QKD protocol that enables secure quantum secret sharing among an arbitrary number of users. This protocol builds upon the asymmetric configuration from previous works [9, 11] and extends the capabilities of standard CV-MDI-QKD [7, 12]. Our analysis focuses on the asymptotic security of the protocol, ignoring finite-size effects and assuming individual uncorrelated attacks. Despite these limitations, the results are promising, especially considering the high level of excess thermal noise we have used in our analysis, which is even higher than what has been achieved experimentally [35]. Moreover, the challenges associated with modeling a correlated attack make this a highly nontrivial task both theoretically and computationally.

The performance of a M-partite CV-MDI-QKD protocol with $M > 2$ groups has been analyzed in this study. To simplify the analysis, two specific configurations, the Y- and X-schemes, have been considered. The results show that the "switch" variant of the Y-scheme leads to improved performance. The protocol also demonstrates robustness to changes in the distance of the deepest group in the interferometer, providing a foundation for building a network of nodes.

In conclusion, it is important to keep in mind that the security of the presented protocol is only proven in the asymptotic limit of many exchanged signals and does not take into account finite-size effects. Further research is needed to improve the security and performance of the protocol. This includes the study of multipartite Bell detections, which have been limited to only a few users so far [37, 38]. Alternatives

such as a squeezed state protocol or a thermal-state protocol in the THz frequency range [39], as well as discrete modulation [40] [1, 41, 42], may lead to improved results. Additionally, exploring other set-ups, such as smaller groups connected with two-by-two Bell-like detections, could help extend the study to more complex networks and clusters of networks. The potential for improvement in this field is vast and provides ample opportunities for future research.

Appendix A: Action of the interferometer

The relay station in our model is represented by the N-port interferometer outlined in Sec. II. This interferometer operates on the travelling modes $\hat{A}$ and is described by the symplectic linear transformation [11] given by

$$
\begin{aligned}
\hat{A}_1 &\to A_1 = \frac{1}{\sqrt{N}} \sum_{j=1}^{N} \hat{A}_j, \\
\hat{A}_k &\to A_k = \frac{1}{\sqrt{k(k-1)}} \left[(k-1)\,\hat{A}_k - \sum_{i=1}^{k-1} \hat{A}_i \right] \\
&\quad \text{for } k = \{2, \ldots, N\}.
\end{aligned} \tag{A1}
$$

For clarity, we will use A instead of $\hat{A}$ to represent the travelling modes after they have undergone the transformation of the interferometer.

1. Bipartite system

To provide further clarity, let us consider the case where there are only two groups ($M = 2$). After the interferometer has acted, the global input state is described by the CM

$$
\mathbf{V_B} = \left(\begin{array}{c|c} y\,\boldsymbol{I}_{2N} & \boldsymbol{\Upsilon} \\ \hline \boldsymbol{\Upsilon}^T & \boldsymbol{\Xi} \end{array} \right), \tag{A2}
$$

where, for the sake of calculation simplicity, the order of the modes has been changed to $\left\{ \hat{B}_1, \ldots, \hat{B}_N, A_1, \ldots, A_N \right\}$, with $\hat{B}_j = \left(\hat{q}_j^B, \hat{p}_j^B \right)^T$ and $A_j = \left(q_j^A, p_j^A \right)^T$. Note that in this case, the absence of the hat symbol distinguishes the modes before and after the interferometer. In general, for the case $M = 2$, the entries of the matrices $\boldsymbol{\Upsilon}$ and $\boldsymbol{\Xi}$ can be calculated using Eq. (A5). where the value of $\star = \{1, 2\}$ in the expression depends on the group, and with $\Lambda_{a,b} := ax_1 + bx_2$. It is noteworthy that, with a proper rearrangement of the modes, the matrix $\boldsymbol{\Upsilon}$ is upper-triangular. To give a concrete example, let us consider the case where $N = 5$, $N_1 = 2$, and $N_2 = 3$. This scenario is depicted by the block matrices

$$
\boldsymbol{\Upsilon} = \begin{pmatrix}
\frac{z_1}{\sqrt{5}} & -\frac{z_1}{\sqrt{2}} & -\frac{z_1}{\sqrt{6}} & -\frac{z_1}{2\sqrt{3}} & -\frac{z_1}{2\sqrt{5}} \\
\frac{z_1}{\sqrt{5}} & \frac{z_1}{\sqrt{2}} & -\frac{z_1}{\sqrt{6}} & -\frac{z_1}{2\sqrt{3}} & -\frac{z_1}{2\sqrt{5}} \\
\frac{z_2}{\sqrt{5}} & 0 & \sqrt{\frac{2}{3}}z_2 & -\frac{z_2}{2\sqrt{3}} & -\frac{z_2}{2\sqrt{5}} \\
\frac{z_2}{\sqrt{5}} & 0 & 0 & \frac{\sqrt{3}}{2}z_2 & -\frac{z_2}{2\sqrt{5}} \\
\frac{z_2}{\sqrt{5}} & 0 & 0 & 0 & \frac{2z_2}{\sqrt{5}}
\end{pmatrix} \otimes \mathbf{Z}, \tag{A3}
$$

$$\mathbf{\Xi} = \begin{pmatrix} \frac{\Lambda_{2,3}}{5} & 0 & -\sqrt{\frac{2}{15}}\Lambda_{1,-1} & -\frac{\Lambda_{1,-1}}{\sqrt{15}} & -\frac{\Lambda_{1,-1}}{5} \\ 0 & \Lambda_{1,0} & 0 & 0 & 0 \\ -\sqrt{\frac{2}{15}}\Lambda_{1,-1} & 0 & \frac{\Lambda_{1,2}}{3} & \frac{\Lambda_{1,-1}}{3\sqrt{2}} & \frac{\Lambda_{1,-1}}{\sqrt{30}} \\ -\frac{\Lambda_{1,-1}}{\sqrt{15}} & 0 & \frac{\Lambda_{1,-1}}{3\sqrt{2}} & \frac{\Lambda_{1,5}}{6} & \frac{\Lambda_{1,-1}}{2\sqrt{15}} \\ -\frac{\Lambda_{1,-1}}{5} & 0 & \frac{\Lambda_{1,-1}}{\sqrt{30}} & \frac{\Lambda_{1,-1}}{2\sqrt{15}} & \frac{\Lambda_{1,9}}{10} \end{pmatrix} \otimes \mathbf{I}. \tag{A4}$$

$$\mathbf{\Upsilon} = \begin{pmatrix} \frac{z_1}{\sqrt{N}} & -\frac{z_1}{\sqrt{2}} & \cdots & -\frac{z_1}{\sqrt{j(j-1)}} & \cdots & -\frac{z_1}{\sqrt{k(k-1)}} & \cdots & -\frac{z_1}{\sqrt{N(N-1)}} \\ \vdots & \frac{z_1}{\sqrt{2}} & \cdots & \cdots & \cdots & \cdots & \cdots & -\frac{z_1}{\sqrt{N(N-1)}} \\ \frac{z_1}{\sqrt{N}} & 0 & \ddots & \cdots & \cdots & \cdots & \cdots & \vdots \\ \frac{z_2}{\sqrt{N}} & 0 & \cdots & \sqrt{\frac{j-1}{j}}z_2 & \cdots & \cdots & \cdots & -\frac{z_2}{\sqrt{N(N-1)}} \\ \vdots & \vdots & \cdots & 0 & \ddots & \cdots & \cdots & -\frac{z_2}{\sqrt{N(N-1)}} \\ \vdots & \vdots & \cdots & \vdots & 0 & \sqrt{\frac{k-1}{k}}z_2 & \cdots & \vdots \\ \vdots & 0 & \cdots & \cdots & \cdots & 0 & \ddots & -\frac{z_2}{\sqrt{N(N-1)}} \\ \frac{z_2}{\sqrt{N}} & 0 & \cdots & 0 & \cdots & \cdots & 0 & \sqrt{\frac{N-1}{N}}z_2 \end{pmatrix} \otimes \mathbf{Z}, \tag{A5}$$

$$\mathbf{\Upsilon}\begin{cases} \langle \hat{B}_i A_j \rangle = 0, & 1 \neq i > j, \\ \langle \hat{B}_m A_1 \rangle = \frac{z_\star}{\sqrt{N}}, & \forall m, \\ \langle \hat{B}_l A_k \rangle = -\frac{z_\star}{\sqrt{k(k-1)}}, & 1 \neq l < k, \\ \langle \hat{B}_k A_k \rangle = \sqrt{\frac{k-1}{k}}z_\star, & k \geq 2, \end{cases}$$

$$\mathbf{\Xi}\begin{cases} \langle A_1^2 \rangle = \frac{\Lambda_{N_1,N_2}}{N}, \\ \langle A_k^2 \rangle = \frac{\Lambda_{2,k(k-1)-2}}{k(k-1)}, & k > 2, \\ \langle A_2 A_j \rangle = 0, & \forall j \neq 2 \\ \langle A_1 A_k \rangle = -2\frac{\Lambda_{1,-1}}{\sqrt{Nk(k-1)}}, & k > 2, \\ \langle A_l A_k \rangle = 2\frac{\Lambda_{1,-1}}{\sqrt{l(l-1)k(k-1)}}, & l, k > 2, \end{cases}$$

Appendix B: Generalised multipartite Bell detection

To perform the multipartite Bell detection, $N - 1$ homodyne detections in the $\hat{q}$-quadrature and one homodyne detection in the $\hat{p}$-quadrature are carried out. Using the example in Eq. (A2), in the scenario with $N = 5$, $N_1 = 2$, and $N_2 = 3$, the resulting conditional global input state is described as

$$\mathbf{V}_{\mathbf{B}|\gamma} = \begin{pmatrix} A & C & E & E & E \\ C & A & E & E & E \\ E & E & B & D & D \\ E & E & D & B & D \\ E & E & D & D & B \end{pmatrix}. \tag{B1}$$

where

$$\mathbf{A} = y\mathbf{I} - \begin{pmatrix} \frac{1}{x_1}\frac{\Lambda_{3,1}}{\Lambda_{3,2}} & 0 \\ 0 & \frac{1}{\Lambda_{2,3}} \end{pmatrix}z_1^2,$$

$$\mathbf{B} = y\mathbf{I} - \begin{pmatrix} \frac{2}{x_2}\frac{\Lambda_{1,1}}{\Lambda_{3,2}} & 0 \\ 0 & \frac{1}{\Lambda_{2,3}} \end{pmatrix}z_2^2,$$

$$\mathbf{C} = \begin{pmatrix} \frac{x_2}{x_1}\frac{1}{\Lambda_{3,2}} & 0 \\ 0 & -\frac{1}{\Lambda_{2,3}} \end{pmatrix}z_1^2, \tag{B2}$$

$$\mathbf{D} = \begin{pmatrix} \frac{x_1}{x_2}\frac{1}{\Lambda_{3,2}} & 0 \\ 0 & -\frac{1}{\Lambda_{2,3}} \end{pmatrix}z_2^2,$$

$$\mathbf{E} = \begin{pmatrix} \frac{1}{\Lambda_{3,2}} & 0 \\ 0 & -\frac{1}{\Lambda_{2,3}} \end{pmatrix}z_1 z_2.$$

Appendix C: Unitary entanglement localisation of M-symmetric states

Eq. (B1) displays a distinctive symmetry that remains consistent for any value of M, making it possible to simplify our problem. To demonstrate this simplification, let us examine one quadrature (the same reasoning can be applied to the other). As a straightforward application of linear algebra [18], let us consider a $N \times N$ matrix of the form

$$
\begin{aligned}
\mathbf{W}_{N_j} &:= \left(d_j - c_j\right) \mathbf{I}_{N_j} + N_j c_j \mathbf{P}_{N_j} \\
&= \begin{pmatrix}
d_j & c_j & c_j & \cdots & c_j \\
c_j & d_j & c_j & \ddots & c_j \\
c_j & c_j & d_j & \ddots & c_j \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
c_j & c_j & c_j & c_j & d_j
\end{pmatrix},
\end{aligned} \tag{C1}
$$

where $\mathbf{P}_{N_j}$ denotes the projection matrix onto the vector $v_{N_j} = N_j^{-1/2} (1, 1, \ldots, 1)^T$ [43]. With the above Eq. (C1), it is straightforward to see that the matrix is diagonal in the basis defined by v_{N_j} and $N_j - 1$ orthogonal vectors, that is

$$
\begin{aligned}
\mathbf{W}'_{N_j} &= \mathbf{R}_{N_j}^{-1} \mathbf{W}_{N_j} \mathbf{R}_{N_j} \\
&= \begin{pmatrix}
d_j - c_j & 0 & 0 & \cdots & 0 \\
0 & d_j - c_j & 0 & \ddots & 0 \\
0 & 0 & d_j - c_j & \ddots & 0 \\
\vdots & \ddots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & 0 & d_j + \left(N_j - 1\right) c_j
\end{pmatrix}.
\end{aligned} \tag{C2}
$$

The matrix $\mathbf{R}_{N_j}$ is the rotation that diagonalizes the matrix, which can be obtained from the basis of eigenvectors $\{e_k\}_{k=1}^{N_j}$ of the matrix itself. It is given by $\mathbf{R}_{N_j} = N_j^{-1/2} \left(e_1, \ldots, e_{N_j}\right)^T$. We define

Definition 3 *An M-symmetric state is a multi-partite state of $\sum_{j=1}^{M} N_j$ modes characterized by its CM $\mathbf{V_M}$. The state is constructed by incorporating diagonal blocks,*

$$
\mathbf{O}_{N_j N_j} = \left(d_j - c_j\right) \mathbf{I}_{N_j} + N_j c_j \mathbf{P}_{N_j} \equiv \mathbf{W}_{N_j}, \tag{C3}
$$

with the same symmetry as $\mathbf{W}_{N_j}$, and off-diagonal blocks,

$$
\mathbf{O}_{N_i N_j} \equiv \mathbf{P}_{f_{ij}^{-1}} \quad (i \neq j), \tag{C4}
$$

which are proportional to $\mathbf{P}_{N_j}$ and have all elements equal to f_{ij}.

For clarity, we present an example of a

$$
\mathbf{V_3} = \begin{pmatrix}
\mathbf{W}_{N_1} & \mathbf{P}_{f_{12}^{-1}} & \mathbf{P}_{f_{13}^{-1}} \\
\mathbf{P}_{f_{12}^{-1}} & \mathbf{W}_{N_2} & \mathbf{P}_{f_{23}^{-1}} \\
\mathbf{P}_{f_{13}^{-1}} & \mathbf{P}_{f_{23}^{-1}} & \mathbf{W}_{N_3}
\end{pmatrix}. \tag{C5}
$$

As previously stated, Eq. (B1) is an example of a particular $\mathbf{V_2}$. By applying the same reasoning as in Eq. (C2), we can find the transformed CM of a general M-symmetric state, as

$$
\mathbf{V}'_{\mathbf{M}} = \bigoplus_{i=1}^{M} \mathbf{R}_{N_i}^{-1} \mathbf{V_M} \bigoplus_{j=1}^{M} \mathbf{R}_{N_j}, \tag{C6}
$$

whose blocks are therefore simply given by

$$
\mathbf{O}'_{N_i N_j} = \mathbf{R}_{N_i}^{-1} \mathbf{O}_{N_i N_j} \mathbf{R}_{N_j}. \tag{C7}
$$

Thus, the transformed CM $\mathbf{V}'\mathbf{M}$ describes an effective state of M modes, since $\left(\sum_{j=1}^{M} N_j\right) - M$ of them are thermal (or vacuum) states that are uncorrelated with each other [as seen in Eq. (C9)]. The effective M-mode state is described by

$$
\mathbf{O}'_{N_i N_j} = [d_i + (N_i - 1) c_i] \delta_{ij} + \left(1 - \delta_{ij}\right) f_{ij} \sqrt{N_i N_j}. \tag{C8}
$$

For example, we provide a transformed

$$
\mathbf{V}'_2 = \begin{pmatrix}
d_1 - c_1 & 0 & \ddots & 0 & 0 & 0 & 0 & 0 \\
0 & d_1 - c_1 & \ddots & 0 & 0 & 0 & 0 & 0 \\
\vdots & \ddots & \ddots & \vdots & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \boxed{d_1 + (N_1 - 1) c_1 \quad\quad f_{12} \sqrt{N_1 N_2}} & 0 & 0 & 0 \\
0 & 0 & 0 & \boxed{f_{12} \sqrt{N_1 N_2} \quad\quad d_2 + (N_2 - 1) c_2} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \vdots & \ddots & \ddots & \vdots \\
0 & 0 & 0 & 0 & 0 & \ddots & d_2 - c_2 & 0 \\
0 & 0 & 0 & 0 & 0 & \ddots & 0 & d_2 - c_2
\end{pmatrix}, \tag{C9}
$$

and therefore $\mathbf{V}_2'$ corresponds N_1+N_2-2 uncorrelated thermal modes, while the effective 2-mode state is described by

$$\mathbf{V}_2' = \left(\begin{array}{|cc|} \hline d_1 + (N_1 - 1)\,c_1 & f_{12}\,\sqrt{N_1 N_2} \\ f_{12}\,\sqrt{N_1 N_2} & d_2 + (N_2 - 1)\,c_2 \\ \hline \end{array} \right). \qquad \text{(C10)}$$

By induction and following the above reasoning, the general post-reduction CM of the effective M-mode state is given by Eqs. 4 and 5 in the main text. To clarify these expressions, let us consider the case of

$$\mathbf{V}_{3|\gamma} = \begin{pmatrix} \boldsymbol{\Gamma}_{11} & \boldsymbol{\Gamma}_{12} & \boldsymbol{\Gamma}_{13} \\ \boldsymbol{\Gamma}_{12} & \boldsymbol{\Gamma}_{22} & \boldsymbol{\Gamma}_{23} \\ \boldsymbol{\Gamma}_{13} & \boldsymbol{\Gamma}_{23} & \boldsymbol{\Gamma}_{33} \end{pmatrix}. \qquad \text{(C11)}$$

where

$$\begin{aligned}
\boldsymbol{\Gamma}_{11} &= y\mathbf{I} - \begin{pmatrix} \frac{N_3 x_2 + N_2 x_3}{\Theta_q} & 0 \\ 0 & \frac{N_1}{\Theta_p} \end{pmatrix} z_1^2, \\[4pt]
\boldsymbol{\Gamma}_{22} &= y\mathbf{I} - \begin{pmatrix} \frac{N_3 x_1 + N_1 x_3}{\Theta_q} & 0 \\ 0 & \frac{N_2}{\Theta_p} \end{pmatrix} z_2^2, \\[4pt]
\boldsymbol{\Gamma}_{33} &= y\mathbf{I} - \begin{pmatrix} \frac{\Lambda_{N_2,N_1}}{\Theta_q} & 0 \\ 0 & \frac{N_3}{\Theta_p} \end{pmatrix} z_3^2, \\[4pt]
\boldsymbol{\Gamma}_{12} &= \sqrt{N_1 N_2} \begin{pmatrix} \frac{x_3}{\Theta_q} & 0 \\ 0 & -\frac{1}{\Theta_p} \end{pmatrix} z_1 z_2, \\[4pt]
\boldsymbol{\Gamma}_{13} &= \sqrt{N_1 N_3} \begin{pmatrix} \frac{x_2}{\Theta_q} & 0 \\ 0 & -\frac{1}{\Theta_p} \end{pmatrix} z_1 z_3, \\[4pt]
\boldsymbol{\Gamma}_{23} &= \sqrt{N_2 N_3} \begin{pmatrix} \frac{x_1}{\Theta_q} & 0 \\ 0 & -\frac{1}{\Theta_p} \end{pmatrix} z_2 z_3,
\end{aligned} \qquad \text{(C12)}$$

with $\Theta_q := N_1 x_2 x_3 + cyclics$ and $\Theta_p := \sum_{j=1}^{3} N_j x_j$. The change in labeling is made to facilitate comprehension [see Eqs. C12 and 5].

Appendix D: Secret-key rate

Before the action of the eavesdropper and the measurements, the global input state that describes the parties (the Bobs) and the eavesdropper (Eve) is pure and Gaussian. After her action and before the measurements, the global output state is still pure, although it may be non-Gaussian. The local measurements commute, so we can defer the Bobs' heterodyne detections until after Eve's measurement. As a result, the Bobs and Eve share a pure conditional state $\hat{\rho}_{\mathbf{B}E|\gamma}$, where we label the local modes as $\hat{\mathbf{B}} := \hat{B}_1 \cdots \hat{B}_N$. The reduced states for the Bobs and Eve are $\hat{\rho}_{\mathbf{B}|\gamma}$ and $\hat{\rho}_{\mathbf{B}E|\gamma}$, respectively. Since the conditional state is pure, the von Neumann entropies S of the subsystems are equal, meaning

$$S\left(\hat{\rho}_{\mathbf{B}|\gamma}\right) = S\left(\hat{\rho}_{E|\gamma}\right). \qquad \text{(D1)}$$

Analogously, in the conditional post-relay scheme, the action of the Bobs projects $\hat{\rho}_{\mathbf{B}E|\gamma}$ into a pure [44] state $\hat{\rho}_{\mathbf{B}E|\gamma\tilde{\beta}^{(N)}}$, yielding to

$$S\left(\hat{\rho}_{\mathbf{B}|\gamma\tilde{\beta}^{(N)}}\right) = S\left(\hat{\rho}_{E|\gamma\tilde{\beta}^{(N)}}\right). \qquad \text{(D2)}$$

As a consequence, the amount of information that Eve can obtain about Bobs' variables $\tilde{\beta}^{(N)} := \{\tilde{\beta}_j\}_{j=1}^{N}$, conditioned on γ, is upper-bounded by her Holevo quantity

$$\begin{aligned}
\chi_{E|\gamma} &= S\left(\hat{\rho}_{E|\gamma}\right) - S\left(\hat{\rho}_{E|\gamma\tilde{\beta}^{(N)}}\right) \\
&= S\left(\hat{\rho}_{\mathbf{B}|\gamma}\right) - S\left(\hat{\rho}_{\mathbf{B}|\gamma\tilde{\beta}^{(N)}}\right),
\end{aligned} \qquad \text{(D3)}$$

which is fully determined by the conditional state $\hat{\rho}_{\mathbf{B}|\gamma}$. Indeed, assuming asymptotic security and infinite Gaussian modulation, the secret-key rate of the protocol can then be expressed as

$$R = \xi I_{\mathbf{B}|\gamma} - \chi_{E|\gamma}, \qquad \text{(D4)}$$

where $\xi < 1$ is the reconciliation efficiency. It is worth noting that, even though $\sum_{j=1}^{M} N_j < N$, Eve still has a purification of the global state due to the assumption of all trusted users, and as a result, the secret-key rate is covariant [45] [11].

Appendix E: Bipartite system

In the QSS protocol, the parties are divided into $M = 2$ groups, and the effective two-mode CM can be obtained following the methods presented in Refs. [11]. Using the same notation, the resulting CM is given by

$$\mathbf{V}_{2|\gamma} = \begin{pmatrix} \boldsymbol{\Delta}_1 & \boldsymbol{\Gamma}' \\ \boldsymbol{\Gamma}' & \boldsymbol{\Delta}_2 \end{pmatrix}, \qquad \text{(E1)}$$

where, for $l = \{1, 2\}$, one explicitly has

$$\begin{aligned}
\boldsymbol{\Delta}_l &= y - \mathrm{diag}\left(\frac{(N - N_l)\,z_l^2}{\Lambda_{N-N_1, N-N_2}}, \frac{N_l z_l^2}{\Lambda_{N-N_2, N-N_1}} \right), \\[4pt]
\boldsymbol{\Gamma}' &= z_1 z_2 \sqrt{N_1 N_2}\, \mathrm{diag}\left(\frac{1}{\Lambda_{N-N_1, N-N_2}}, -\frac{1}{\Lambda_{N-N_2, N-N_1}} \right),
\end{aligned} \qquad \text{(E2)}$$

and again $\Lambda_{a,b} := ax_1 + bx_2$. One may compute the symplectic eigenvalues of the CM Eq. (E1) as [6]

$$\nu_\pm = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4\left\|\mathbf{V}_{2|\gamma}\right\|}}{2}}, \qquad \text{(E3)}$$

where $\Delta = \|\boldsymbol{\Delta}_1\| + \|\boldsymbol{\Delta}_2\| + 2\left\|\boldsymbol{\Gamma}'\right\|$ and $\|\cdot\|$ indicates the determinant. However, it is not known beforehand if the rate will be asymptotically maximum or if there exists an optimal modulation value μ that maximizes it. Our analysis shows that there is an optimal modulation in the full-house case, where all users participate. Additionally, we also study the asymptotic trends for large modulation values in the full-house (FH)

scenario and find that

$$\nu_+^{(FH)} \to |\eta_1 - \eta_2| \sqrt{\frac{N_1 N_2}{\mathcal{N}_{12} \widetilde{\mathcal{N}}_{12}}} \, \mu,$$

$$\nu_-^{(FH)} \to \frac{1}{|\eta_1 - \eta_2|} \sqrt{\frac{\lambda_{12} \widetilde{\lambda}_{12}}{N_1 N_2}}, \tag{E4}$$

with

$$\begin{aligned}
\lambda_{ij} &:= N_i \omega_j \left(1 - \eta_j\right) + N_j \omega_i \left(1 - \eta_i\right), \\
\widetilde{\lambda}_{ij} &:= N_i \omega_i \left(1 - \eta_i\right) + N_j \omega_j \left(1 - \eta_j\right), \\
\mathcal{N}_{ij} &:= N_i \eta_j + N_j \eta_i, \\
\widetilde{\mathcal{N}}_{ij} &:= N_i \eta_i + N_j \eta_j,
\end{aligned} \tag{E5}$$

which are all symmetrical with respect to the interchange of indices i and j. The removable discontinuity $\eta_1 = \eta_2$ does not represent a problem, as we will prove in the next Sec. E 1.

1. Conditioning: Heterodyne Detection

Assuming group "2" serves as the decoder, the conditional CM after local heterodyne detection of Eq. (E1) is calcalated as [6]

$$\mathbf{V}_{1|\gamma 2} = \mathbf{\Delta}_1 - \mathbf{\Gamma}' \left(\mathbf{I} + \mathbf{\Delta}_2\right)^{-1} \mathbf{\Gamma}'^{\mathrm{T}}, \tag{E6}$$

which is diagonal and therefore its symplectic eigenvalue can be obtained by the symplectic invariance of its determinant, that is

$$\nu_N^{SS} = \sqrt{\|\mathbf{V}_{1|\gamma 2}\|}. \tag{E7}$$

Specifically, in the FH limit, the symplectic eigenvalue is given by

$$\nu_N^{SS} \to \frac{1}{\eta_1} \sqrt{\frac{\left(\lambda_{12} + N_1 \eta_2\right)\left(\widetilde{\lambda}_{12} + N_2 \eta_2\right)}{N_1 N_2}}. \tag{E8}$$

Having the total and conditional symplectic spectra [Eqs. (E4) and (E8), respectively], the Holevo quantity using as

$$\chi = h(\nu_+) + h(\nu_-) - h\left(\nu_N^{SS}\right), \tag{E9}$$

where the *entropic function* h is defined as

$$h(\nu) := \frac{\nu + 1}{2} \log_2\left(\frac{\nu + 1}{2}\right) - \frac{\nu - 1}{2} \log_2\left(\frac{\nu - 1}{2}\right). \tag{E10}$$

The function is equal to zero for the vacuum noise $h(1) = 0$ and asymptotically approaches

$$h(\nu) = \log_2 \frac{e}{2} \nu + O\left(\nu^{-1}\right). \tag{E11}$$

The continuity of the Holevo quantity χ in the transition from the asymmetrical to the symmetrical configuration, i.e., in

$\{\eta_1 = \eta_2, \omega_1 = \omega_2\}$, must be verified. This can be done by comparing their respective symplectic eigenvalues in the FH case. When $\eta_1 = \eta_2 := \eta$ and $\omega_1 = \omega_2 := \omega$, the following holds

$$\begin{aligned}
\nu_\pm^{(FH)} &\to \sqrt{y\left(y - \frac{z^2}{x}\right)} \\
&= \sqrt{\frac{\left[(1 - \eta)\mu\omega + \eta\right]\mu}{(1 - \eta)\omega + \eta\mu}},
\end{aligned} \tag{E12}$$

in agreement with Refs. [11]. The same continuity holds for ν_N^{SS}, which converges to

$$\nu_N^{SS} \to \sqrt{\frac{\tau_{12}\tau_{21}}{\widetilde{\tau}_{12}\widetilde{\tau}_{21}}}, \tag{E13}$$

where we define

$$\begin{aligned}
\tau_{ij} &:= \eta\left(N_i + N_j\mu\right) + N\omega\left(1 - \eta\right)\mu \\
\widetilde{\tau}_{ij} &:= \eta\left(N_i + N_j\eta\mu\right) + N\omega\left(1 - \eta\right).
\end{aligned} \tag{E14}$$

2. Mutual Information

The mutual information can be expressed compactly as [12]

$$I = \frac{1}{2} \log_2 \Sigma, \tag{E15}$$

where we make the assumption that group "2" serves as the decoder, allowing us to write

$$\Sigma = \frac{1 + \|\mathbf{\Delta}_1\| + \mathrm{Tr}\{\mathbf{\Delta}_1\}}{1 + \|\mathbf{V}_{1|\gamma 2}\| + \mathrm{Tr}\{\mathbf{V}_{1|\gamma 2}\}}, \tag{E16}$$

with $\mathbf{\Delta}_1$ and $\mathbf{V}_{1|\gamma 2}$ defined in Eqs. (E1) and (E6), respectively. A closer examination of the denominator $\sigma_n := 1 + \|\mathbf{V}_{1|\gamma 2}\| + \mathrm{Tr}\{\mathbf{V}_{1|\gamma 2}\}$ reveals

$$\sigma_n \to$$

$$\frac{\eta_2\left(\eta_1 + \eta_2\right)N\left(N - N_1 - N_2\right)^2\mu^2}{\left(N - N_1\right)\left[N\left(\eta_1 + \eta_2\right) - \mathcal{N}_{12}\right]\left[\left(N - N_2\right)\left(\eta_1 + \eta_2\right) - N_1\eta_2\right]}. \tag{E17}$$

The (quadratic) dependence on the modulation μ highlights the importance of identifying an optimal value of μ to maximize the secure communication performance. In contrast, in the FH case, there is no such dependence, as

$$\sigma_n^{(FH)} \to \frac{\left(\lambda_{12} + \mathcal{N}_{12}\right)\left(\widetilde{\lambda}_{12} + \widetilde{\mathcal{N}}_{12}\right)}{N_1 N_2 \eta_1^2}. \tag{E18}$$

This suggests that for a bipartite system, there is a direct relationship between full-house and asymptotic behavior. Whenever all users cooperate, the rate is maximized for high values of modulation $\mu \gg 1$. On the other hand, as soon as one or more users do not cooperate, there exists an optimal modulation value that maximizes the rate.

3. Secret-key rate

In a thermal-loss channel with asymptotic security, the secret-key rate against collective attacks can be obtained using Eq. (7), assuming perfect reconciliation ($\xi = 1$) and utilizing an infinite Gaussian modulation as

$$R = \frac{1}{2} \log_2 \Sigma - h(\nu_+) - h(\nu_-) + h\left(\nu_N^{SS}\right). \qquad \text{(E19)}$$

One may determine its FH asymptotic limit, resulting in

$$
\begin{aligned}
R^{asy} = {}& \log_2 \left(\frac{2\eta_1\eta_2}{e\,|\eta_1 - \eta_2|} \sqrt{\frac{N_1 N_2}{(\lambda_{12} + \mathcal{N}_{12})\left(\widetilde{\lambda}_{12} + \widetilde{\mathcal{N}}_{12}\right)}} \right) \\
& - h\left(\frac{1}{|\eta_1 - \eta_2|} \sqrt{\frac{\lambda_{12}\widetilde{\lambda}_{12}}{N_1 N_2}} \right) \\
& + h\left[\frac{1}{\eta_1} \sqrt{\frac{(\lambda_{12} + N_1\eta_2)\left(\widetilde{\lambda}_{12} + N_2\eta_2\right)}{N_1 N_2}} \right].
\end{aligned}
\qquad \text{(E20)}
$$

The asymmetric configuration, when ideal conditions are met, enables secure long-distance communication. In particular, for $\eta_2 = 1$ (which corresponds to a distance of $0\,\text{km}$ for the second user), the secret-key rate expression in Eq. (E20) simplifies to

$$
\begin{aligned}
R^{asy}(\eta_2 = 1) = {}& \log_2 \left(\frac{2\eta_1}{e(1 - \eta_1)} \sqrt{\frac{N_1 N_2}{\{N_1 + N_2\,[\omega_1(1 - \eta_1) + \eta_1]\}\{N_2 + N_1\,[\omega_1(1 - \eta_1) + \eta_1]\}}} \right) \\
& - h(\omega_1) + h\left\{ \frac{1}{\eta_1} \sqrt{\frac{[N_1 + N_2\omega_1(1 - \eta_1)][N_2 + N_1\omega_1(1 - \eta_1)]}{N_1 N_2}} \right\}.
\end{aligned}
\qquad \text{(E21)}
$$

Under the condition that group "1" has pure-loss links ($\omega_1 = 1$), Eq. (E20) can be further simplified to

$$
\begin{aligned}
R^{asy}(\eta_2 = 1, \omega_1 = 1) = {}& \log_2 \left[\frac{\eta_1}{e(1 - \eta_1)} \frac{\sqrt{N_1 N_2}}{N} \right] \\
& + h\left\{ \frac{1}{\eta_1} \sqrt{\frac{[N_1 + N_2(1 - \eta_1)][N_2 + N_1(1 - \eta_1)]}{N_1 N_2}} \right\}.
\end{aligned}
\qquad \text{(E22)}
$$

The rate Eq. (E20) is based on the assumption of infinite use of the relay channel. However, this can be closely approximated after a large but finite number of rounds, as demonstrated in Fig. 12. The fast convergence of the rate expressed in Eq. (E19) to its asymptotic value is particularly noteworthy. Additionally, it is observed that the configurations "X/Y" and "Y/X" show the same behavior, indicating that there are no depth effects introduced by the relay. Furthermore, when $N_1 + N_2 < N$, there exists an optimal modulation value μ that maximizes the rate, as confirmed by Fig. 13 in the case of a pure-loss channel with $\omega_1 = \omega_2 = 1$.

4. Non-ideal Bell detector

In the bipartite asymmetrical scenario, the transformation rule Eq. (E2) is represented as

$$
\begin{aligned}
(N - N_1)\,x_1 + (N - N_2)\,x_2 & \\
\mapsto (N - N_1)\,x_1 + (N - N_2)\,x_2 &+ N\frac{1 - \tau}{\tau}, \\
(N - N_2)\,x_1 + (N - N_1)\,x_2 & \\
\mapsto (N - N_2)\,x_1 + (N - N_1)\,x_2 &+ N\frac{1 - \tau}{\tau}.
\end{aligned}
\qquad \text{(E23)}
$$

This generalizes the results from Refs. [9, 37, 46]. Furthermore, in the case of a FH scenario, with $N_1 + N_2 = N$, Eq. (E23) simplifies to

$$x_j \mapsto x_j + \frac{1 - \tau}{\tau}, \qquad j = \{1, 2\}. \qquad \text{(E24)}$$

One can then generalize Eq. (E20) by following the approach presented in Ref. [37] and applying the transformations from Eq. (E24). Although Eq. (E20) is not expressed in terms of x_j, y, and z_j, but rather in terms of the channel parameters η_j,

Figure 12. The solid curves show the secret-key rate (bit/use) as a function of modulation μ, obtained from Eq. (E19), for different splittings of the signal in the full-house configuration, where Alice sends signals to all four users. The dotted curves represent the asymptotic rate Eq. (E20) for large values of μ. Moving from top to bottom, the splitting ratios are 50/50, 5/95, and 1/991. The distances and thermal noises are fixed to $d_1 = 1$ km, $d_2 = 0.1$ km, and $\omega_1 = \omega_2 = 1$ SNU. The figure shows that the optimal modulation for maximizing the rate is always large, independent of the splitting, and that the performance is symmetric with respect to the 'X/Y" and "Y/X" splittings.

Figure 13. The secret-key rate (bit/use) as a function of the modulation μ (SNU) for a pure-loss channel (i.e., $\omega_1 = \omega_2 = 1$) exhibits the presence of an optimal μ for dummy users, regardless of the distance of the groups from the relay. The curves show the performance of different "asymmetries" in the 50/50 splitting. The blue curve corresponds to the optimal 50/50 case, which has the same trend shown in Fig. 12. Other parameters are $d_1 = 1$ km and $d_2 = 0.01$ km.

ω_j, and the modulation μ, making this substitution non-trivial, after developing the usual analysis, it can be shown that, in the FH case, the asymptotic non-ideal secret-key rate for two

groups with a thermal-loss channel is given by

$$R^{asy} = \log_2\left(\frac{2\tau\eta_1\eta_2}{e\,|\eta_1 - \eta_2|}\sqrt{\frac{N_1 N_2}{L_{12}L_{21}}}\right) - h\left(\frac{1}{\tau\,|\eta_1 - \eta_2|}\sqrt{\frac{S_{12}S_{21}}{N_1 N_2}}\right)$$
$$+ h\left(\frac{1}{\tau\eta_1}\sqrt{\frac{R_{12}R_{21}}{N_1 N_2}}\right),$$

$$(E25)$$

where

$$S_{ij} = N_i\left[1 - \tau + \tau\omega_1\left(1 - \eta_1\right)\right]$$
$$+ N_j\left[1 - \tau + \tau\omega_2\left(1 - \eta_2\right)\right],$$
$$R_{ij} = N_i\left[1 - \tau + \tau\omega_1\left(1 - \eta_1\right)\right]$$
$$+ N_j\left[1 - \tau\left(1 - \eta_2\right) + \tau\omega_2\left(1 - \eta_2\right)\right],$$
$$L_{ij} = N_i\left[1 - \tau\left(1 - \eta_1\right) + \tau\omega_1\left(1 - \eta_1\right)\right]$$
$$+ N_j\left[1 - \tau\left(1 - \eta_2\right) + \tau\omega_2\left(1 - \eta_2\right)\right].$$
$$(E26)$$

Appendix F: *M*-partite systems: *Y*- and *X*-schemes

The standard procedure is followed when analyzing the security of a system with more than two groups. However, when dealing with multiple groups, it is important to pay attention to the rate. The smallest possible secret-key rate is obtained by subtracting the maximum Holevo quantity χ from the minimum mutual information I between any two groups. This is because the rate between different groups can vary and a potential eavesdropper may attack the group with the lower rate. To consider the worst-case scenario, we need to take the lowest possible rate into account.

To optimize the system, we must first find the symplectic eigenspectrum of $\mathbf{V}_{M|\gamma}$ [see Eq. (4)]. The conditioning of the system can then be performed in M different ways and we need to find the method that maximizes the Holevo quantity or minimizes the conditional von Neumann entropy S_{cond}. To do this, we perform local heterodyne detection on $\mathbf{V}_{M|\gamma}$ and find the group that is furthest from the relay, as this group will result in the minimum conditional entropy [47].

For the switch to function correctly, we must consider all combinations of two groups and perform a heterodyne measurement. They are characterised by the $\binom{M}{2}$ $\mathbf{V}_{yz}s$ 4×4 matrices built from $\mathbf{V}_{M|\gamma}$ with the blocks $\mathbf{\Gamma}_{yy}$, $\mathbf{\Gamma}_{zz}$, and $\mathbf{\Gamma}_{yz}$ of the groups "Y" and "Z" of interest, with $y, z = \{1, \ldots, M\}$. The minimum is still obtained by measuring the group that is furthest from the relay.

The correct mutual information Eq. (E15) can be determined by considering all the $M(M-1)/2$ Σ-matrices two-by-two. In the tripartite case, we label $\Sigma_{xy|\zeta}$ such that $\mathbf{\Gamma}_{xx}$ is the numerator block and $\mathbf{V}_{y|\zeta}$ the denominator one. Given that the groups are $d_x \geq d_y \geq d_z$ from the relay, the minimum mutual information is obtained by considering groups "Z" and "X" and conditioning the measurement on group "Y". The secret-key rate is then given by Eq. (7) after optimizing the modulation μ.

[1] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Advances in Optics and Photonics **12**, 1012 (2020).

[2] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).

[3] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: Principle, security and implementations," Entropy **17**, 6072–6092 (2015).

[4] S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513–577 (2005).

[5] A. Serafini, *Quantum Continuous Variables: A Primer of Theoretical Methods* (CRC Press, 2017).

[6] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621–669 (2012).

[7] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," Nature Communications **8**, 15043 (2017).

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

[9] C. Ottaviani, C. Lupo, A. Ferraro, M. Paternostro, and S. Pirandola, "Multipartite entanglement swapping and mechanical cluster states," Phys. Rev. A **99**, 030301 (2019).

[10] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, "Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration," Phys. Rev. A **91**, 022320 (2015).

[11] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, "Modular network for high-rate quantum conferencing," Communications Physics **2**, 118 (2019).

[12] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," Nature Photonics **9**, 397–402 (2015).

[13] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238–241 (2003).

[14] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," Phys. Rev. A **59**, 1829–1834 (1999).

[15] We sometimes omit that μ and ω are in SNU for simplicity of notation. This is also due to the fact that it is usually not possible to carry out a dimensional check in this field.

[16] In the EB representation, these LOs can be implemented by means of suitable interferometers, one on each side. These passive LOs can be available also at the post-processing stage, after the action of the relay, for the equivalent PM description.

[17] Across the M-partition, plus a tensor product of thermal states for the remaining modes.

[18] A. Serafini, G. Adesso, and F. Illuminati, "Unitarily localizable entanglement of gaussian states," Phys. Rev. A **71**, 032349 (2005).

[19] The index k always runs from 1 to M, but we explicitly show it only once for cleanliness.

[20] E. S. Polzik, J. Carri, and H. J. Kimble, "Spectroscopy with squeezed light," Phys. Rev. Lett. **68**, 3020–3023 (1992).

[21] T. C. Zhang, K. W. Goh, C. W. Chou, P. Lodahl, and H. J. Kimble, "Quantum teleportation of light beams," Phys. Rev. A **67**, 033802 (2003).

[22] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," Phys. Rev. A **77**, 042325 (2008).

[23] D. Lin, D. Huang, P. Huang, J. Peng, and G. Zeng, "High performance reconciliation for continuous-variable quantum key distribution with ldpc code," International Journal of Quantum Information **13**, 1550010 (2015), https://doi.org/10.1142/S0219749915500100.

[24] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography," npj Quantum Information **4**, 21 (2018), arXiv:1702.07740 [quant-ph].

[25] X. Wang, Y. Zhang, S. Yu, B. Xu, Z. Li, and H. Guo, "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution," Quantum Info. Comput. **17**, 1123–1134 (2017).

[26] X. Wang, Y. Zhang, S. Yu, and H. Guo, "High speed error correction for continuous-variable quantum key distribution with multi-edge type ldpc code," Scientific Reports **8**, 10543 (2018).

[27] T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, C. Pacher, R. Werner, and R. Schnabel, "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," Nature Communications **6**, 8795 (2015).

[28] In order to reach the optimal and asymptotic performances provided by the infinite-dimensional Hilbert space.

[29] Consisting the interferometer of a cascade of beam splitters T_k, we may define a user depth. A user, whose channel is characterised by T_i, is deeper than another $\left(T_j\right)$ if $i > j$.

[30] We are actually inverting the roles of encoder and decoder between the groups with respect to Refs. [7, 12]. This will end up with a trivial and irrelevant exchange of roles between Alice and Bob.

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

[32] We decide just to expose the results concerning 0.1 km being the others totally analogous.

[33] A protocol is invariant with respect to asymmetrical splittings if they lead to the same result.

[34] That is, when only one of the two groups is affected by noise (we exclude the case in which both are, clearly the worst possible scenario).

[35] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li, X. Zhang, Z. Zheng, B. Chu, X. Gao, N. Meng, W. Cai, Z. Wang, G. Wang, S. Yu, and H. Guo, "Continuous-variable qkd over 50 km commercial fiber," Quantum Science and Technology **4**, 035006 (2019).

[36] We omit the superscript max in the figures for simplicity of sketching.

[37] G. Spedalieri, C. Ottaviani, and S. Pirandola, "Covariance matrices under bell-like detections," Open Systems & Information Dynamics **20**, 1350011 (2013).

[38] Y. Wu, J. Zhou, X. Gong, Y. Guo, Z.-M. Zhang, and G. He, "Continuous-variable measurement-device-independent multipartite quantum communication," Phys. Rev. A **93**, 022325 (2016).

[39] It is attractive for the potential boosting of data rate of wireless communication.

[40] In order to exploit advantage distillation and post-selection pro-
tocols, allowing to improve the achievable distance (paying a
price in terms of the key-rate per use of the protocol), one may
substitute the Gaussian modulation of the signal states with a
discrete one.

[41] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs,
"Continuous variable quantum cryptography: Beating the 3 db
loss limit," Phys. Rev. Lett. **89**, 167901 (2002).

[42] A. Leverrier and P. Grangier, "Unconditional security proof
of long-distance continuous-variable quantum key distribution

with discrete modulation," Phys. Rev. Lett. **102**, 180504 (2009).

[43] It is the matrix with all elements equal to N_j^{-1}.

[44] This occurs because heterodyne detection is a rank-1 measure-
ment, hence the purity.

[45] In the sense that preserves Eq. (7) in form.

[46] R. Van Meter, *Quantum Networking* (John Wiley & Sons,
Hoboken, 2014).

[47] This behaviour does not depend on the modulation μ. In case
there are more equidistant groups further away from the relay,
it makes no difference which group is considered.