






Please cite the Published Version

Fletcher, Alasdair I, Harney, Cillian, Ghalaii, Masoud , Papanastasiou, Panagiotis , Mountogiannakis, Alexandros , Spedalieri, Gaetana, Hajomer, Adnan A E , Gehring, Tobias and Pirandola, Stefano  (2025) An overview of CV-MDI-QKD. Reports on Progress in Physics, 88. 084001 ISSN 0034-4885

DOI: <https://doi.org/10.1088/1361-6633/adf4f4>

Publisher: IOP Publishing

Version: Accepted Version

Downloaded from: <https://e-space.mmu.ac.uk/641877/>

Usage rights:  [Creative Commons: Attribution 4.0](https://creativecommons.org/licenses/by/4.0/)

Additional Information: This is an Author Accepted Manuscript of an article published in Reports on Progress in Physics by IOP.

Enquiries:

If you have questions about this document, contact openresearch@mmu.ac.uk. Please include the URL of the record in e-space. If you believe that your, or a third party's rights have been compromised through this document please see our Take Down policy (available from <https://www.mmu.ac.uk/library/using-the-library/policies-and-guidelines>)

An Overview of CV-MDI-QKD

Alasdair I. Fletcher,^{1,2} Cillian Harney,^{1,2} Masoud Ghalaii,³ Panagiotis Papanastasiou,^{1,2,4} Alexandros Mountogiannakis,² Gaetana Spedalieri,¹ Adnan A. E. Hajomer,⁵ Tobias Gehring,⁵ and Stefano Pirandola^{1,*}

¹*Department of Computer Science, University of York, York YO10 5GH, United Kingdom*

²*nodeQ, 71-75 Shelton Street, London WC2H 9JQ, United Kingdom*

³*Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M1 5GD, United Kingdom*

⁴*Department of Physics, University of York, York YO10 5DD, United Kingdom*

⁵*Department of Physics, Technical University of Denmark, 2800 Kongens Lyngby, Denmark*

As quantum key distribution (QKD) emerges as a robust defense against quantum computer threats, significant advancements have been realized by researchers. A pivotal focus has been the development of protocols that not only simplify hardware implementation, such as the use of continuous-variable (CV) systems, but also eliminate the necessity for trusted nodes, as seen with the measurement-device-independent (MDI) approach. This paper delves into the integration of these methodologies in the CV-MDI-QKD protocol, offering an in-depth exploration of its evolution, primary characteristics, and the latest advancements in both theory and experiment.

I. INTRODUCTION

Four decades have passed since quantum-secure communications were introduced [1, 2]. Besides quantum key distribution (QKD) [3], we have also witnessed the birth of other quantum-secure technologies, including quantum random number generators [4–11], quantum conferencing or secret-sharing [12–18], quantum digital signatures [19–26], quantum bit commitment [27–31], and secure quantum computing [32–36], to name a few. These outstanding endeavours are contributing to the future quantum internet [37–41].

There exist two major classes of QKD, i.e., discrete-variable (DV) and continuous-variable (CV) protocols. The former class exploits quantum resources with finite degrees of freedom, e.g., polarization qubits, and contains the BB84 [1], E91 [42], B92 [43] and six-state [44] protocols. In contrast, CV-QKD encodes information into quadratures of light [45] representing the so-called ‘continuous variables’. CV-QKD forms a distinct class of communication strategies including those which are based on squeezed states [46–48], coherent states [49, 50], and noisy/thermal states either in optical [51–54] or non-optical [55, 56] regimes. Other techniques continue to be explored involving no-switching [57], discrete modulation [58], and two-way [59] CV-QKD protocols. It is also worth to mention hybrid protocols where both DV and CV components are exploited [60–63].

All QKD protocols mentioned above are endowed with their own unique properties, and their success is based upon several salient features. This includes (i) their underlying trade-off between rate and transmission distance, (ii) their strength of security, and (iii) their feasibility of practical deployment. The theoretical and experimental evolution of QKD over the years has aimed to accelerate progress in each of these directions, with several critical milestones being reached along the way.

To address (i), one such milestone was the derivation of the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound [64] which establishes the exact fundamental trade-off between

communication rate and distance. This limit puts an upper bound on all point-to-point implementations of QKD. Namely, for a lossy bosonic channel, which could underlie models of optical-fibre and free-space channels, two users cannot distribute more than the secret key capacity of the link $-\log_2(1 - \tau)$, where τ quantifies channel’s loss. The PLOB bound provides a guide for all point-to-point QKD protocols, outlining an optimal performance level that can guide future protocol/experimental designs.

The PLOB bound also emphasises the critical inability of repeaterless, high-rate quantum communication over long-distance channels [64, 65]. However, realistic communication networks would consist of many interconnected nodes, and parties would not rely merely on direct links. Hence, this innate weakness can be compensated by additional infrastructure in the form of repeaters and quantum networks. With the addition of intermediate stations, distance limitations can be circumvented and high-rates restored. Indeed, the PLOB bound has more recently been extended to derive end-to-end capacities of quantum-safe networks [66, 67]. These results derive critical bounds on the performance of repeater-assisted QKD protocols, motivating advances within this domain.

Nevertheless, the development of repeater-assisted protocols invites further questions. In Refs. [66, 67], the end-to-end capacities are shown to be achievable by assuming either trusted QKD repeaters or entanglement-based repeaters. In a practical QKD network, it would be ideal to use repeaters simultaneously *untrusted*, so they could still be usable even if compromised by an attacker, and *not based on entanglement distribution*, so they can be more easily deployed in realistic technological environments. To address (ii) and (iii) simultaneously, the first step done in this direction was the introduction of measurement device independent (MDI) QKD [68–71] showing that QKD is still possible in a single-hop chain where Alice and Bob connects to an untrusted, and entanglement-free, repeater. More recently, the MDI idea was extended to design the twin-field QKD protocol [72, 73], which can also exceed the PLOB bound.

Soon after the introduction of the MDI protocol, a CV version was designed and experimentally realized [74, 75]. CV-MDI-QKD aims to achieve the same features as DV-MDI-

* Corresponding author; stefano.pirandola@york.ac.uk

QKD while ensuring much higher key rates at short distances. Many works followed proposing other studies, variants and improvements. Following Ref. [74], CV-MDI-QKD was also investigated in Refs. [76, 77] with some inaccuracies. Several works implemented techniques based on photon subtraction [78, 79], noiseless linear amplifiers [80], phase-sensitive amplifiers [81], and in free-space settings [82]. Attempts have been made on the encoding side by replacing coherent states with squeezed or thermal states [83–85], and replacing Gaussian modulation with discrete modulation or dual-phase modulation [86, 87].

Early works that assumed the asymptotic rates with many uses of the communication links have been extended to the composable and finite-size framework [88, 89] which significantly strengthen the security analysis of such protocols for practical deployment. Post-selection strategies for CV-MDI-QKD have also been recently investigated [90] which can help to extend transmission distances. Furthermore, investigations have been carried out concerning how CV-MDI-QKD protocols can be integrated into more complex networking domains with more than two users [16, 91] and more intermediate, untrusted nodes [92].

This review is structured as follows. In Sec. II we provide a schematic overview of the protocol. In Sec. III, we discuss the secret key rate of CV-MDI-QKD based on Gaussian modulation and its post-selection variant. In Sec. IV, we review finite-size and composability. In Sec. V, we weigh up quantum network complexity, including CV-MDI-QKD star and three-node networks. In Sec. VI we discuss the main experimental implementations of CV-MDI-QKD. We summarize our manuscript in Sec. VII.

II. FEATURES OF THE PROTOCOL

The basic protocol for CV-MDI-QKD [74, 75] is sketched in Fig. 1. The steps are as follows:

a. In the so-called entanglement-based (EB) representation, Alice and Bob each heterodyne one mode of a two-mode squeezed vacuum (TMSV) state while transmitting the other mode. This is equivalent to a prepare-and-measure (P&M) scheme, where they prepare a coherent state and modulate its amplitude via a bi-variate Gaussian distribution. It is assumed that the labs of Alice and Bob are secure so the loss and noise within them are trusted.

b. Alice and Bob send their Gaussian-modulated coherent states $|\alpha\rangle$ and $|\beta\rangle$ to the relay through quantum channels that could be, e.g., optical fibres or free-space links. These channels can be simulated via beam splitters with transmissivities τ_A and τ_B . The eavesdropper (Eve) can attack the links by overlapping one mode of her TMSV states at the beam splitters. This ‘entangling-cloner attack’ represents the most relevant Gaussian attack. See the next section for more details.

c. At the relay, Charlie uses a CV Bell measurement to perform a joint detection. This step includes overlapping signals received from Alice and Bob’s station on a balanced beam splitter and homodyning both outlet beams. Precisely, Charlie measures orthogonal quadratures q and p obtaining q_- and

p_+ , respectively. The resultant complex value $\gamma = q_- + ip_+$ is then broadcast to Alice and Bob. The outcome γ establishes a-posteriori correlations between the variables of the parties. Consequently, knowing γ allows each party to infer the variable of the other party through post-processing.

d. Alice and Bob post-process their measured/modulation data along with the corresponding relay outcomes, with the effect of correlating their data. Next, the post-processing includes channel parameter estimation (PE), error correction (EC), and privacy amplification (PA). These operations will provide the final secret shared key.

III. SECURITY ANALYSIS

The two end users, Alice and Bob, each have access to independent, identical zero-mean bi-variate Gaussian distributions with the same variance $\mu - 1$ (assumed to be large). From these distributions, they draw two amplitude values α and β therefore preparing Gaussian-modulated coherent states $|\alpha\rangle$ and $|\beta\rangle$ respectively (see prepare-and-measure description in Fig. 1). These two states are sent to a central detection station, which is in principle controlled by Eve. Operated correctly, the station performs a Bell detection in which the states are combined on a balanced beamsplitter and undergo conjugate homodyne detections. The results of these measurements are combined into a single complex variable γ which is publicly broadcast. It is clear that initially the mutual information $I(\alpha : \beta) = 0$ since the coherent states are prepared from independent Gaussian distributions. However after the announcement of γ , Alice and Bob are able to decode each other’s variable and thus $I(\alpha : \beta|\gamma) > 0$. Despite having access to γ , Eve is unable to infer the parties’ variables, i.e., $I(E : \alpha) = I(E : \beta) = 0$. Eve is therefore forced to attack the channels or alter the operation of the relay, both of which may be detected by Alice and Bob in post-processing.

Let us now consider the same protocol in the equivalent entanglement-based representation [3]. A detailed discussion of the formulation can be found in the supplementary information of [75]. Alice begins with a two-mode squeezed vacuum (TMSV) Φ_{aA} , a zero mean Gaussian state with covariance matrix given by [45]:

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

where $\mathbf{Z} = \text{diag}(1, -1)$. Mode a undergoes heterodyne detection, projecting the travelling mode A into the coherent state $|\alpha\rangle$, the modulation of which is in one-to-one correspondence with the measurement outcome $\tilde{\alpha}$. In the limit of large modulation $\mu \rightarrow \infty$, we have $\alpha = \tilde{\alpha}^*$. The one-to-one correspondence between α and $\tilde{\alpha}$ renders the two variables informationally equivalent. Symmetric description holds for Bob. Alice’s and Bob’s modes A and B are sent to the central relay for Bell detection and, by the commutation of local measurements, Alice’s and Bob’s heterodyne detections of their retained modes a and b may be delayed until the end of the protocol. The protocol can thus be seen as an entanglement

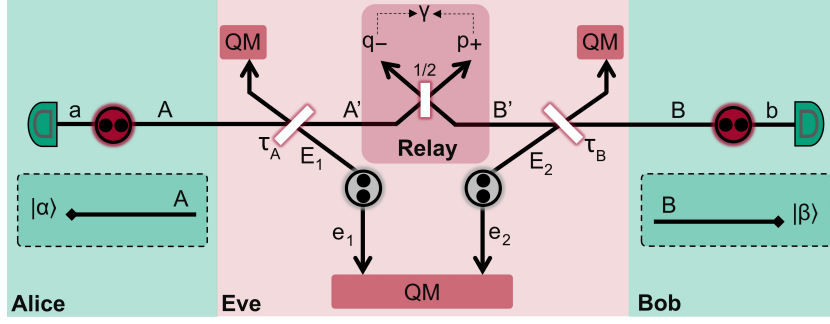


FIG. 1. **Schematic of CV-MDI-QKD.** In the entanglement-based description, Alice and Bob transmit one mode (A and B) of their TMSV states, denoted by red circles. In the equivalent and practical prepare-and-measure description (dashed boxes), Alice and Bob directly send Gaussian-modulated coherent states to the relay. Eve has a pair of TMSV states, denoted by grey circles. Her modes E_1 and E_2 are made to interact with Alice and Bob's signal modes via beam splitters of transmissivities τ_A and τ_B , respectively (each of these interactions corresponds to an 'entangling cloner'). Eve's output modes after the beamsplitters and her retained modes (e_1 and e_2) are stored in a quantum memory (QM) for collective measurement at the end of the protocol (this is known as a 'collective attack'). Alice's and Bob's output modes A' and B' are mixed in a $1/2$ beam splitter at the relay, whose outputs are subsequently measured using two conjugate homodyne detections with outcomes q_- and p_+ , respectively. These real outcomes form a single complex value γ that is publicly broadcast.

swapping protocol, generating an entangled Gaussian state between Alice's and Bob's retained modes by the Bell detection of the transmitted modes. The entanglement-based representation is a useful mathematical tool for studying the security of the protocol but also provides a potential version of it that can prevent side-channel attacks on state preparation [68].

A. Gaussian attacks and asymptotic key rate

Eve's most general attack strategy against an MDI protocol can always be reduced to the case in which the detector is operated correctly and Eve attacks the incoming links [75]. Failing to undertake detections or measuring other observables can always be detected by the parties in post-processing [68]. Moreover, the most powerful collective attack that Eve may undertake to eavesdrop on a Gaussian CV protocol is a Gaussian attack [93]. Alice and Bob therefore assume the worst-case scenario where all the pure loss and thermal noise can be attributed to Eve performing such an optimal Gaussian attack on the incoming links. Such an attack may be modeled as mixing Alice and Bob's incoming states with Eve's ancillary states E_1 and E_2 at beam splitters of transmissivity τ_1 and τ_2 respectively. The reduced state $\hat{\rho}_{E_1 E_2}$ is a correlated thermal state with zero mean and covariance matrix given by:

$$V_{E_1 E_2} = \begin{pmatrix} \omega_A \mathbf{I} & \mathbf{G} \\ \mathbf{G} & \omega_B \mathbf{I} \end{pmatrix} \quad (2)$$

where $\mathbf{G} = \text{diag}(g, g')$ such that g and g' are correlation parameters and ω_A and ω_B are the thermal variances introduced into each incoming link. For simplicity, one can study the case of $g' = g = 0$, which corresponds to the dilation into a pair of independent entangling cloners as depicted in Fig. 1. (We assume this case in the numerical plots of this paper).

We may compute the mutual information between Alice and Bob's variables $I_{AB} := I(\alpha : \beta)$ while Eve's total stolen

information I_E is upper bounded by using the Holevo information. In the asymptotic limit of an infinite number of protocol rounds, the rate takes the form $R = I_{AB} - I_E$, so that Alice and Bob share on average R secret bits per use of the relay. Note that the rate above is a simplified asymptotic formula that also assumes unit reconciliation efficiency (i.e., perfect error correction during data post-processing).

In the symmetric configuration, Alice and Bob are equidistant from the relay. In this case, the rate-distance scaling is shown in Fig. 2. The distance is calculated by assuming the parties connected to the relay by fibre optic links with a loss of 0.2 dB/km. That is the transmissivity of the beamsplitters used in Eve's attack may be given by $\tau_i = 10^{-0.02d_i}$ where d_i is the distance in kilometers of the links to Eve.

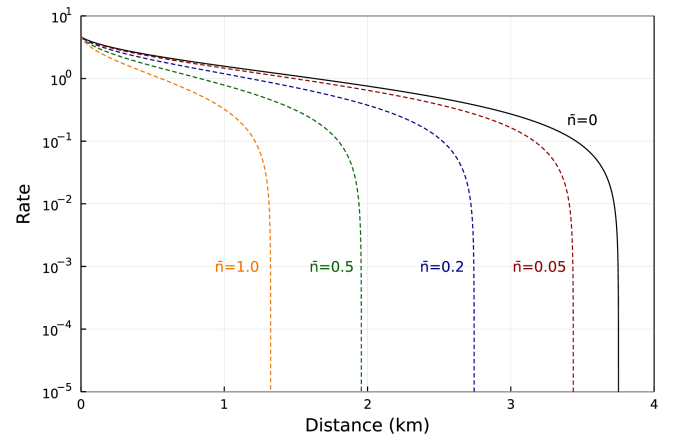


FIG. 2. Asymptotic key rate (bits/use) of the symmetric CV-MDI-QKD protocol versus fibre distance (0.2dB/km) for various values of thermal noise \tilde{n} affecting each link. The solid black line indicates the rate under pure loss. All rates are optimized with large modulation. Unit reconciliation and perfect detection efficiency are assumed. Figure adapted from Ref. [94].

In the symmetric configuration, the protocol can achieve high rates at short distances (~ 1 bit per use) and is robust against thermal noise. However, the maximum distance where a positive rate can be maintained is limited. Under pure loss, a positive rate can only be kept for ≤ 4 km.

In Fig. 3 we show the rate-distance scaling in the asymmetric configuration, where we assume that Alice is the encoder and Bob the decoder (this means that Bob needs to guess Alice's variable). If we fix the distance of Alice at 5m from the relay, we can see that Bob can be very far. The distance scaling is much improved in this configuration, enabling communication at over 100km between the two end parties. Indeed, it is shown in Ref. [75], that if Bob's channel is affected by pure loss only, in the limit $\tau_A \rightarrow 1$ (Alice brought arbitrarily close to the relay) that the rate only goes to zero for $\tau_B \rightarrow 0$, which represents Bob arbitrarily far away.

The reverse scenario in which Bob's position is fixed close to the relay is substantially less effective. Even with $\tau_B \rightarrow 1$ and pure loss in Alice's channel, a positive rate can only be maintained to 6.8km. This difference of performance is related to the distinction between direct and reverse reconciliation in CV QKD. In the limit $\tau_A \rightarrow 1$ in which Alice (the encoder) approaches the relay, we recover a point-to-point no-switching protocol in reverse reconciliation. Conversely, with $\tau_B \rightarrow 1$ (decoder close to the relay), we have a point-to-point no-switching protocol in direct reconciliation.

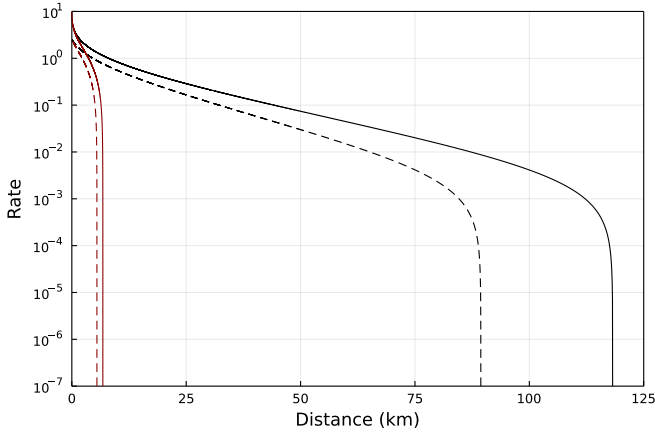


FIG. 3. Asymptotic key rate (bits/use) of CV-MDI-QKD in the asymmetric configuration versus fibre distance (0.2dB/km) between Alice and Bob. Black lines refer to Alice at a fixed distance of 5m from the relay, while Bob is at a variable fibre distance. The red lines represent the opposite scenario in which Bob's is fixed at 5m from the relay and Alice's fibre distance is allowed to vary. Solid lines indicate the rates under pure loss and the dashed with thermal noise equal to $\bar{n} = 0.05$. All rates are optimized with large modulation and perfect detection efficiency is assumed. Figure adapted from Ref. [94].

B. Post-selection

The distance of CV-MDI-QKD may be improved by introducing post-selection techniques. Post-selection was first utilized in QKD in Ref. [95] to overcome the apparent 3dB loss

limit for CV QKD implied by beam-splitting attacks. Such technique exploits the fact that, even beyond 3dB, there are regions in the parameter space in which Alice and Bob's mutual information exceeds Eve's Holevo information and hence the rate is positive. By announcing the absolute values of the quadratures of their prepared coherent states, Alice and Bob can determine such regions in post-selection and keep only the most favourable instances of the protocol. They may then attempt reconciliation on the signs of the quadratures to produce a secure key. This technique improves the distance of CV QKD at the cost of reducing its rate at short ranges.

Ref. [90] introduced post-selection for CV-MDI-QKD. In the prepare-and-measure formalism, Alice and Bob again prepare coherent states and each has access to zero-mean bivariate Gaussian distributions, from which they draw two real variables for the values of the displacement of the q and p quadratures of the coherent states they will prepare. They encode the magnitude of their value for the q displacement as Q_A and Q_B and the sign of the value as κ_A and κ_B . Similarly, the absolute values drawn for the p displacements are encoded as P_A and P_B , and the signs as κ'_A and κ'_B . Thus, Alice and Bob prepare the coherent states $|\alpha = \frac{1}{2}(\kappa_A Q_A + i\kappa'_A P_A)\rangle$ and $|\beta = \frac{1}{2}(\kappa_B Q_B + i\kappa'_B P_B)\rangle$, respectively.

These coherent states are sent to the relay as before and the measurement outcome $\gamma = \gamma_q + i\gamma_p$ is again announced publicly (where we have set $\gamma_q = q_-$ and $\gamma_p = p_+$). After the protocol ends, the parties undertake basis reconciliation to agree whether to use the q or p quadrature for each round of the protocol. If the q quadrature is chosen, Alice and Bob reveal their values of $Q_A, Q_B, \kappa'_A P_A$ and $\kappa'_B P_B$ and will attempt to reconcile the signs κ_A and κ_B . Alternatively if the p quadrature is chosen, Alice and Bob reveal $\kappa_A Q_A, \kappa_B Q_B, P_A$ and P_B and attempt to reconcile the signs κ'_A and κ'_B .

Under phase-insensitive collective Gaussian attacks (such as the typical case of a collective attack based on two entangling cloners), the two quadratures are perturbed symmetrically and remain uncorrelated. For this reason, we shall consider only the use of the q quadrature. The measurement yields the distribution $p(\gamma_q | \kappa_A, \kappa_B, Q_A, Q_B)$ (note we have implicitly removed conditioning from variables on which there is no dependence) from which Bayes' theorem may be used to calculate $p(\kappa_A | \kappa_B, Q_A, Q_B, \gamma_q)$ and $p(\kappa_B | \kappa_A, Q_A, Q_B, \gamma_q)$ and hence determine the single point mutual information $\tilde{I}(\kappa_A : \kappa_B | Q_A, Q_B, \gamma_q)$. Similarly we can the single point Holevo information $\tilde{\chi}(E : \kappa_A | Q_A, Q_B, \gamma_q)$ and the single-point rate

$$\begin{aligned} \tilde{R}(Q_A, Q_B, \gamma_q) &= \tilde{I}(\kappa_A : \kappa_B | Q_A, Q_B, \gamma_q) \\ &\quad - \tilde{\chi}(E : \kappa_A | Q_A, Q_B, \gamma_q), \end{aligned} \quad (3)$$

which is a rate conditioned on the values of the announced variables Q_A, Q_B and the measurement outcome γ_q . By applying post-selection, Alice and Bob only select instances of the protocol when the single point rate is positive. Hence the overall postselected rate is given by:

$$\int \max[\tilde{R}(Q_A, Q_B, \gamma_q), 0] p(Q_A, Q_B, \gamma_q) dQ d\gamma_q. \quad (4)$$

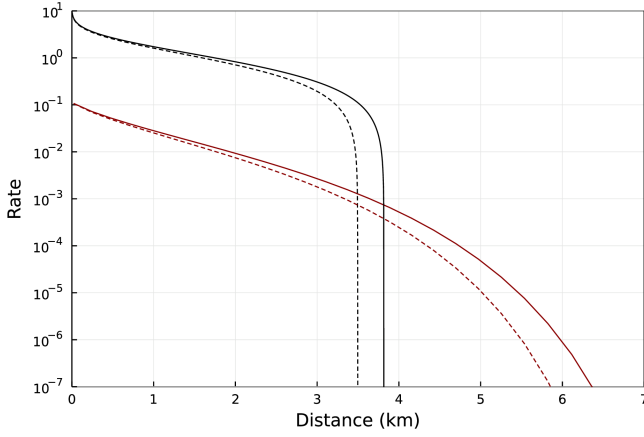


FIG. 4. Comparative rate-distance performance of CV-MDI-QKD with and without post-selection in the symmetric configuration. The black lines indicate the original CV-MDI-QKD protocol [75] and the red the equivalent protocol with post-selection [90]. Solid lines are the rates under pure loss and dashed lines refer to thermal noise equal to $\bar{n} = 0.05$ thermal photons. All the rates (bits/use) are optimized over the modulation of the prepared coherent states and assume perfect reconciliation and detection efficiency. Figure adapted from Ref. [94].

Alternatively, denoting the region in parameter space in which the single point rate is positive as Γ we may write the post-selected rate as:

$$R = \int_{\Gamma} p(Q_A, Q_B, \gamma_q) \tilde{R}(Q_A, Q_B, \gamma) dQ d\gamma_q. \quad (5)$$

The rate-distance performance of the two equivalent protocols with and without post-selection are compared in Fig. 4. We see the trade-off between the improved long-distance performance of the post-selected protocol and the reduction in the rate at short distances more akin to DV-MDI-QKD. The post-selected protocol is more robust in the symmetric configuration, able to maintain a positive key rate out to 6km.

IV. COMPOSABLE FINITE-SIZE SECURITY

Composable finite-size security of CV-MDI-QKD was initially studied in Refs. [96, 97] and later extended to free-space scenarios in Ref. [82], including satellite implementations. Finite-size means that we consider a finite number of signals exchanged in the protocol, which automatically leads to the use of estimators for evaluating channel parameters. Composability means that there is a security parameter associated with the protocol that quantifies its distance from an ideal implementation. This is called ‘epsilon’ security and combines the failure probabilities of data-processing steps (PE, EC, and PA).

The most rigorous formula for the composable finite-size key rate of the basic, Gaussian-modulated version of CV-MDI-QKD can be derived using the tools developed in Ref. [98] for the security of general CV-QKD protocols. Here we use these tools to provide an improved formulation.

Assume that Alice and Bob run a long session composed of n_{bks} blocks, each block having N points. A point corresponds to a single protocol run, where the parties transmit a pair of coherent states to the relay and extract two correlated classical values from the process. We set $N = n + m$, where m points of the block are used for PE while the remaining n points contribute to key generation. Also assume that, in post-processing, the variables are digitalized into d bits per letter. Then we have the following imperfections to consider:

- Up to an error probability ϵ_{pe} , Alice and Bob construct n_{pe} worst-case estimators for the channel parameters (transmissivity and thermal noise of each link).
- Up to an error probability ϵ_{ent} , Alice and Bob estimate the entropy of the key.
- Up to a failure probability $1 - p_{\text{ec}}$, EC is successful and, up to an error probability ϵ_{cor} , called ‘epsilon correctness’, the resulting corrected block is the same for Alice and Bob, so they have two identical string of bits.
- Up to an error probability ϵ_{sec} , called ‘epsilon secrecy’, PA is successful. This means that Alice’s and Bob’s strings are compressed into shorter strings that are completely decoupled from Eve. In turn, one may decompose $\epsilon_{\text{sec}} = \epsilon_s + \epsilon_h$, where ϵ_s is known as smoothing parameter and ϵ_h as hashing parameter.

The protocol has total epsilon security $n_{\text{bks}}\epsilon$, where

$$\epsilon \leq \epsilon_{\text{cor}} + \epsilon_s + \epsilon_h + \epsilon_{\text{ent}} + n_{\text{pe}}\epsilon_{\text{pe}}. \quad (6)$$

Assuming collective Gaussian attacks, the key rate is upper bounded by [see Eq. (68) of [98]]

$$R \leq \frac{p_{\text{ec}}[n\hat{R}_{\infty}^{\text{pe}} - n\delta_{\text{ent}} - \sqrt{n}\delta_{\text{aep}} + \theta]}{N}, \quad (7)$$

where

$$\delta_{\text{ent}} = \log_2(n) \sqrt{2n^{-1} \ln(2/\epsilon_{\text{ent}})}, \quad (8)$$

$$\delta_{\text{aep}} \simeq 4 \log_2 \left(2^{d/2} + 2 \right) \sqrt{\log_2(2/\epsilon_s^2)}, \quad (9)$$

$$\theta := \log_2(2c_h^2\epsilon_{\text{cor}}), \quad (10)$$

and $\hat{R}_{\infty}^{\text{pe}}$ is the asymptotic key rate computed from PE.

It is in the specific expression of $\hat{R}_{\infty}^{\text{pe}}$ that enters the features of the CV-MDI-QKD protocol. In particular, this is given by

$$\hat{R}_{\infty}^{\text{pe}} = \hat{\xi} \hat{I}_{AB} - [I_E]_{\text{wc}}, \quad (11)$$

where the various terms depend on estimators and worst-case estimators of $n_{\text{pe}} = 3$ parameters: the link transmissivities, τ_A and τ_B , and the total excess noise [97, Eq. (10)]. For an uncorrelated two-mode attack with two independent entangling cloners ($g' = g = 0$), the total excess noise takes the form

$$\Xi = \frac{1}{2} (\tau_A \zeta_A + \tau_B \zeta_B), \quad (12)$$

where $\zeta_k := (1 - \tau_k)(\omega_k - 1)/\tau$ is the excess noise of an individual link $k = A$ (Alice-relay) or B (Bob-relay).

The mutual information \hat{I}_{AB} is calculated from the estimators $\hat{\tau}_A$, $\hat{\tau}_B$, and $\hat{\Xi}$, while Eve's Holevo information $[I_E]_{wc}$ is computed from the worst-case estimators τ_A^{wc} , τ_B^{wc} , and Ξ_{wc} . In the presence of a stable configuration, these values can be computed over $n_{bks}m$ points (see Ref. [97] for more details on their explicit expressions). In addition, the error reconciliation efficiency is given by

$$\hat{\xi} = \frac{\hat{H}_{key} - n^{-1}\text{leak}_{ec}}{\hat{I}_{AB}}, \quad (13)$$

where \hat{H}_{key} is the estimated Shannon entropy of the raw key (see, for example, [89, Eqs.(46) and (47)]) and leak_{ec} upper-bounds the bits of information leaked during EC.

In Fig. 5, we show the composable-secure key rate of the CV-MDI-QKD protocol in the symmetric and asymmetric configurations. We can see how the requirement for composable security takes a toll in terms of achievable distance by comparing the results with those in Fig. 3. For example, in the asymmetric configuration, the asymptotic key rate stretches up to about 100 km, while this distance is reduced to about 25 km for the composable key rate.

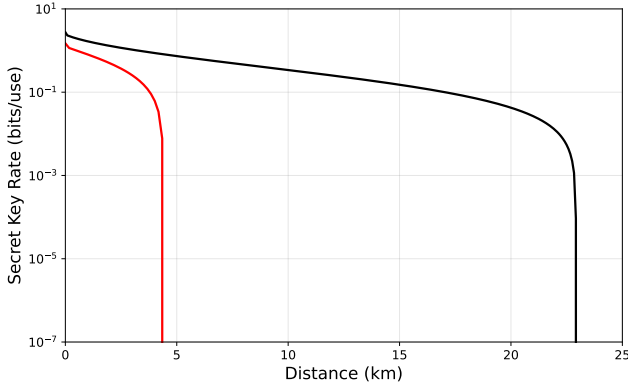


FIG. 5. Composable-secure secret key rate (bits/use) of the symmetric (red line) and asymmetric (black line) CV-MDI-QKD protocol versus fibre distance with standard loss-rate 0.2dB/km (the distance in the plot is the sum of the fibre distance of the two links). The distance of Alice from the relay is 5m for the asymmetric configuration. The values of the excess noise for the two individual links are $\zeta_A = \zeta_B = 0.01$ and we assume the two-mode uncorrelated attack ($g' = g = 0$). We have set $\hat{\xi} = 0.98$, $p_{ec} = 0.95$, $d = 14$ and a block size of $N = 10^7$. The electronic noise and detection efficiency of the relay are set to $u_{el} = 0.01$ and $\eta_{eff} = 0.98$. All epsilon parameters are individually set to 2^{-32} , while the PE ratio and the modulation variance are optimized. See Ref. [97] for details about all the parameters.

V. NETWORK COMPLEXITY

In this section, we discuss how CV-MDI-QKD can be extended to network scenarios. First, we consider an extension

to a star network with an arbitrary number of users. We then consider the specific case of a 3-node star network, for which we introduce the technique of post-selection, with the aim of improving the distribution distance from the central relay.

A. CV-MDI-QKD star network

Let us consider how CV-MDI-QKD can be extended from the bipartite case to N users. Since MDI-QKD invariably requires the use of a central untrusted relay, it is natural to consider a star network topology in which each of the N users connects to a single central relay. This approach is made possible by means of a generalized Bell detection at the central relay which creates shared correlations that can be post-processed into a secure key common to all parties ('key conferencing'). Overall, a CV-MDI-QKD network is a specific example of a Gaussian quantum network with untrusted relays, as generally modeled in Ref. [92].

The structure of the relay for CV-MDI-QKD is depicted in Fig. 6. Each party prepares coherent states $|\alpha_i\rangle$ which are sent through thermal-loss channels to the detector relay. The detector consists of a cascade of $N - 1$ beamsplitters of increasing transmissivity. Each output mode on the left of the diagram undergoes homodyne detection in the q quadrature and the final mode at the bottom is homodyned in the p quadrature. The results of the measurements are announced publicly.

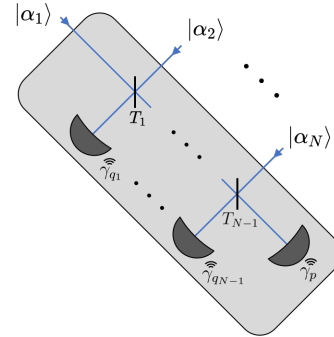


FIG. 6. Structure of the detector relay for CV-MDI-QKD conferencing. Figure adapted from Ref. [16].

The rates achieved by the star network module for various numbers of end users and amounts of thermal noise are shown in Fig. 7. The users are all equidistant to the central relay (symmetric configuration) and the rates shown are optimized for the maximum distance at which they maintain a positive key rate. There is a fundamental trade-off between the number of users and the maximum distance at which a positive key rate may be maintained. More precisely, from Fig. 3b of Ref. [16], we see a $\simeq 2/N$ scaling for the maximum radius in km of the star network in terms of the number of users N .

Due to the limitations of linear optics, it is important to remark that similar designs for multi-partite MDI-QKD cannot be implemented with discrete variables. A detailed discussion may be found in the supplementary information of Ref. [16]. Finally, it is also worth to mention that a squeezed version

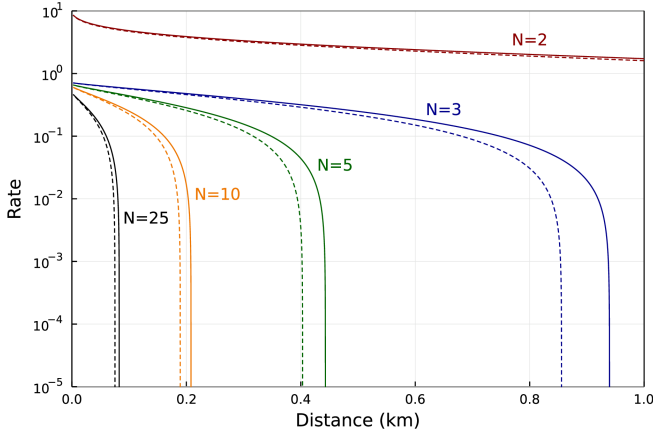


FIG. 7. Rate (bits/use) of a CV-MDI-QKD star network in the symmetric configuration as a function of the fibre distance of each user from the central relay. The variances of the Gaussian distributions used to modulate the coherent states are selected to optimize the maximum distance at which a positive secret key rate can be maintained. Solid lines represent the rate under pure loss ($\bar{n} = 0$) and the dashed lines under non-zero thermal noise ($\bar{n} = 0.05$). Figure adapted from Ref. [94].

of multi-partite CV-MDI-QKD can achieve higher rates than the standard version with coherent states. As discussed in Ref. [16, Supp. Note 4], higher rates may be achieved if the parties perform the protocol in an entanglement-based configuration where they use TMSV states, sending one mode to the relay while retaining the other. After the generalized Bell detection is performed, they would then apply conditional local squeezing operations to their kept modes before measuring them with heterodyne detection.

B. CV-MDI-QKD 3-node star network with post-selection

As with the two user case, post-selection techniques may be applied to such a setup to improve the long distance performance of the star network module. In particular, the 3 end user case has been recently investigated [91]. In this protocol the 3 parties prepare states of the form $|\frac{1}{2}(\kappa_A Q_i + i\kappa'_i P_i)\rangle$ again having drawn q_i and p_i from a zero mean Gaussian and encoding the signs as κ_i and κ'_i and the magnitudes as Q_i and P_i . The structure of the detector is the same as the star network described in Section V A with one key change: The detector is randomly switched between performing $N - 1$ q homodyne detections and 1 p homodyne detection and $N - 1$ p homodyne detections and 1 q homodyne detection. This second configuration is shown in the schematic in Fig. 8. The chosen configuration is publicly announced after the detections.

As in Section III B the postselected rate may be computed by performing an integral over the region Γ where the single point rate \tilde{R} is positive:

$$R = \int_{\Gamma} p(\mathbf{Q}, \gamma_q) \tilde{R}(\mathbf{Q}, \gamma_p) d\mathbf{Q} d\gamma_q \quad (14)$$

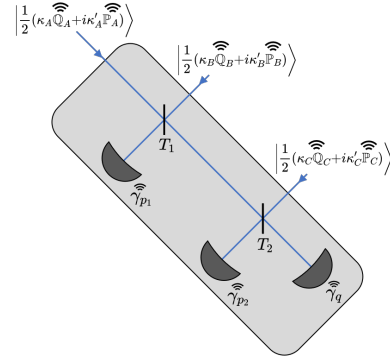


FIG. 8. 3-user CV-MDI-QKD star network in post-selection. Two beamsplitters mix input modes with transmissivities $T_1 = \frac{1}{2}$ and $T_2 = \frac{2}{3}$. The states undergo two p homodyne detections and one q homodyne detection. In this case, the parties will attempt reconciliation between $\kappa_A, \kappa_B, \kappa_C$. The other orientation is physically equivalent to Fig. 6, in which the parties attempt reconciliation on $\kappa'_A, \kappa'_B, \kappa'_C$. In both cases at the end of the protocol all the end users publicly broadcast the magnitudes of the quadratures of their prepared states. Figure adapted from Ref. [91].

where we have collected $\mathbf{Q} = (Q_A, Q_B, Q_C)$. The results are shown in Fig. 9, comparing the postselected and non-postselected protocols under pure loss. We see the same reduction in the rate at short distances but improved long-distance performance. The numerical difficulty in performing the high dimensional integral in Eq. (14) limits the analysis to pure loss attacks but the work provides proof of principle that such post-selection techniques may be applied to multi-party CV-MDI-QKD conferencing.

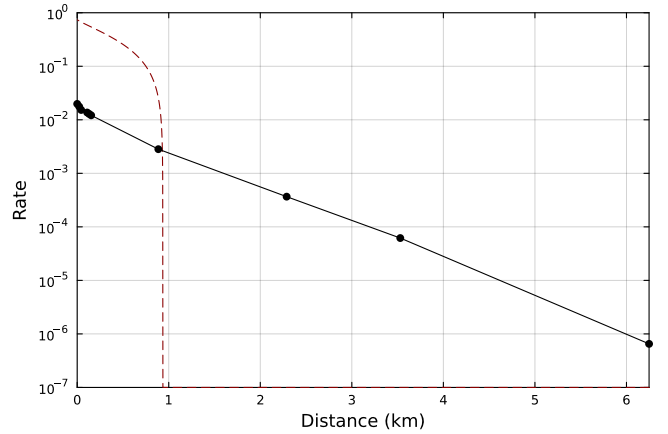


FIG. 9. Rate of the 3-user CV-MDI-QKD network in post-selection assuming the symmetric configuration (all parties equidistant from the central relay). The key rate (bits/use) is plotted versus fibre distance of each party assuming perfect detector efficiency and unit variance for the Gaussian modulations. For comparison, we show the rate of an equivalent 3-party star network without post-selection [16] and optimized parameters (red dashed line). In this plot, the links are all pure-loss channels. Figure adapted from Ref. [91].

VI. EXPERIMENTAL CV-MDI-QKD

CV-MDI-QKD enhances security by eliminating side-channel vulnerabilities on detection. This security benefit comes at the expense of increased implementation complexity compared to one-way CV-QKD. Consequently, despite significant progress in theory, only a few experimental demonstrations of CV-MDI-QKD have been reported, as summarized in Table I.

In 2015, the earliest proof-of-concept demonstration of CV-MDI-QKD was performed using a free-space optical setup, as illustrated in Fig. 10(a) [75]. In this experiment, coherent states were generated by modulating a continuous-wave laser at 1064 nm with amplitude and phase modulators driven by Gaussian noise. Phase synchronization between Alice's and Bob's signals was achieved using piezoelectric transducers. The CV Bell measurement was implemented using a balanced beam splitter combined with homodyne detectors measuring orthogonal quadratures. The setup achieved a secret key rate of 0.1 bits per relay use under emulated channel losses of 2% for Alice and 60% for Bob, assuming a reconciliation efficiency of 97%. While this work showed the fundamental viability of CV-MDI-QKD, it did not incorporate essential practical features like fibre-optic transmission, independent laser sources at Alice's and Bob's stations operating at telecommunication wavelengths, and clock synchronization between the transmitters, making it unsuitable for practical deployment.

A more practical CV-MDI-QKD implementation was demonstrated in 2022 [99], as illustrated in Fig. 10(b). This system employed a 10 km standard single-mode fibre (SMF) channel and independent CW lasers operating at the telecom wavelength of 1550 nm. The two lasers were frequency-locked by sending part of Alice's laser through a fibre channel to Bob's station, which interfered with a portion of Bob's laser. The interference result was then fed as an error signal to the phase-locked loop. The system used a 50 ns pulse carved at a repetition rate of 500 kHz. The pulses were split into quantum pulses modulated by cascaded amplitude and phase modulators, pilot pulses used as LO (coming from Bob's station) and phase-reference pulses (coming from Alice's station) to compensate for the fast phase drift between the LO and Alice's signal. The quantum and pilot pulses were time and polarization multiplexed at Alice's and Bob's stations using a combination of polarizing beam splitter, delay line, and Faraday mirror before transmitting them through SMF. At the relay, the quantum and the pilot pulses were first demultiplexed. To estimate the fast phase drift, heterodyne detection was performed by tapping off part of the LO pulses and interfering them with the reference pulses in a 90-degree optical hybrid measuring the amplitude quadrature X_R and the phase quadrature P_R . The measurement outcomes were then used to estimate the fast phase drift for each signal pulse as $\Delta\theta = \tan^{-1}(P_R/X_R)$. As for the slow phase drift estimation, Alice and Bob used another set of phase-calibration pulses, which were different from the phase-reference pulses. After estimating the total phase drift, Alice and Bob applied quadrature remapping to their data. With this frequency and phase locking system, a low excess noise of 0.0045 SNU was

achieved, enabling a key rate of 0.19 bit per relay use at an error correction efficiency of 97%. This work demonstrated the feasibility of building a CV-MDI-QKD system over fibre channels. However, the complexity of the experiment is rather high. For instance, a separate heterodyne receiver is required to implement the complex frequency and phase locking system, and because it is a pulsed system, an additional amplitude modulator is required for pulse carving. The combination of polarization and time multiplexing also adds another fold of complexity. Moreover, the experiment does not take into account how to synchronize distant transmitters.

The development of the next generation of CV-MDI-QKD systems focuses on simplifying the system structure and increasing the repetition rate. Figure 10(c) shows a recent experiment towards this goal [100]. In this experiment, the frequency and phase locking system, as well as pulse carving were removed. This is done by sharing a 1550 nm CW laser between the communication parties with a low noise amplifier (LN AMP) deployed at Bob's station to avoid frequency locking. Besides, the pulse carving was replaced by digital pulse shaping using a root-raised cosine filter. This allowed the transmitters to operate at a symbol rate of 5 MBaud, which is one order of magnitude larger than the previous demonstration [75, 99]. Furthermore, the CV Bell detection was realized without phase locking utilizing a new relay structure leveraging the concept of a polarization-based 90-degree hybrid. The quantum efficiency of the relay was 94%. Combining this structure with digital signal processing (DSP), the propagation delay and phase drift were estimated using reference symbols. The system generated keys at a rate of 0.12 bit per relay use over channel loss of 2 dB, assuming an information reconciliation efficiency of 97%.

The coexistence of CV-MDI-QKD with classical communication channels is pivotal for real-world adoption. A recent system design has addressed this issue, taking into account practical aspects such as clock synchronization and the utilization of SMF channels [101]. In this system, an asymmetric network configuration was employed, with the relay being co-located at Alice's station, as shown in Fig. 10(D). Both senders, Alice and Bob, utilized the same DSP module for quantum state preparation, following the approach in Ref. [100]. To achieve synchronization between Alice's and Bob's stations, a 10 MHz reference clock was utilized at Bob's station to generate an optical clock at 1310 nm, which co-propagated with the quantum signal to Alice's station. Furthermore, real-time phase locking was integrated into the system to lock two independent lasers, eliminating the need for an additional fibre channel as described in Ref. [99]. This significantly simplifies the system structure, making it more suitable for practical adoption. The system operated at a symbol rate of 20 MBaud and demonstrated key generation in finite-size regimes. This resulted in a two-order-of-magnitude improvement in the key rate compared to previous demonstrations [75, 99].

Despite these advances, further improvements are possible. For instance, enhanced DSP techniques could eliminate the need for explicit laser phase locking and clock synchronization. However, the achieved symbol rates in CV-MDI-QKD

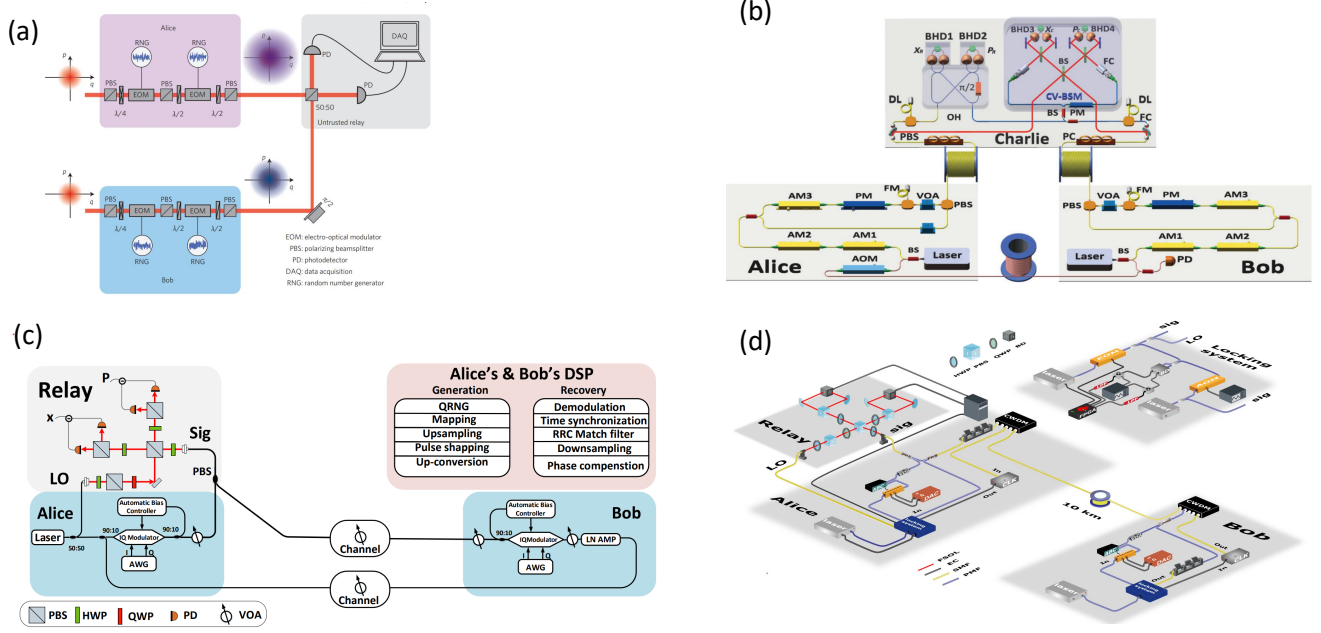


FIG. 10. Experimental CV-MDI-QKD based on Gaussian-modulated coherent states. (a) [75] (b) [99] (c) [100] (d) [101]. BS: beam splitter; AM: amplitude modulator; AOM: acousto-optic modulator; PM: phase modulator; FM: Faraday mirror; VOA: variable optical attenuator; PBS: polarizing beam splitter; PD: photodetector; PC: polarization controller; FC, fibre collimator; DL: delay line; AWG: arbitrary waveform generator; HWP: Half-wave plate; QWP: quarter-wave plate; BHD: balanced homodyne detector; DAC: Digital-to-analog converter; ABC: Automatic bias controller; CWDM: Coarse Wavelength division multiplexing; FPGA: Field-programmable gate array. Figures adapted from Refs. [75], [99], [100], and [101].

TABLE I. Comparison of Experimental Parameters in Recent CV-MDI-QKD Demonstrations

Ref.	Configuration	channel type	loss	repetition rate	key rate, bits/relay use	Security
[75]	asymmetric	Free space	4 dB	100 kHz	0.1	Asymptotic
[99]	asymmetric	Fiber	2.02 dB	500 kHz	0.19	Asymptotic
[100]	asymmetric	VOA	2 dB	5 MHz	0.12	Asymptotic
[101]	asymmetric	Fiber	2.5 dB	20 MHz	0.13	Finite-size

still lag behind the state-of-the-art in prepare-and-measure coherent-state QKD systems [102]. This limitation arises primarily from two factors: (1) bandwidth constraints in the high-efficiency relay, particularly in the readout electronics of balanced homodyne detectors, which often rely on discrete components with parasitic limitations that restrict both speed and noise performance; and (2) the stringent timing requirements at the relay beam splitter. Unlike one-way protocols, CV-MDI-QKD requires precise temporal overlap of optical pulses from independent sources. As the symbol rate increases and pulse durations shorten, synchronization becomes more challenging, directly impacting the interference visibility and system performance.

VII. CONCLUSIONS

CV-MDI-QKD amalgamates two groundbreaking concepts within QKD: the techniques of CV-QKD and MDI-QKD. On

the one hand, this approach streamlines quantum hardware, enabling the use of non-single-level coherent-state sources and room-temperature homodyne or heterodyne detectors. On the other, it establishes single-hop end-to-end encryption, where Alice and Bob extract a secret key even when the middle party is untrusted, i.e., potentially operated by an eavesdropper. In this short review, we have discussed the features of this protocol, its state-of-art in terms of security proofs, and experimental implementations.

While the promise of CV-MDI-QKD is very appealing for the entire field of quantum cryptography, its robustness to practical loss affects its performance in the symmetric configuration where Alice and Bob are approximately equidistant from the central relay. Besides the early development of the asymmetric version of the protocol, efforts have been directed to develop variants, e.g., based on post-selection, that would allow to mitigate this fragility and reach better distances when operated symmetrically.

The overall scope of this short review is to boost further

research in this area. The main theoretical goals are: (i) develop a symmetric variant able to further increase the distance of both parties from the central relay; and (ii) develop a multipartite network variant for quantum conferencing able to mitigate the $O(1/N)$ radius scaling with respect to the number of users N . From an experimental perspective there are several avenues for exploration: (i) developing a simpler system that is hardware-agnostic and phase-locking free; (ii) increasing the system's repetition rate; and (iii) integrating photonics and electronics components of the relay and transmitters.

CV-MDI-QKD presents a promising solution for securing high-rate local area networks (LANs) where multiple devices communicate through a central, potentially untrusted relay. The compatibility with standard telecom components and the potential for high key generation rates over short distances

make it especially suitable for densely connected LAN environments, such as data centres or enterprise networks, where secure and efficient key exchange is critical.

Acknowledgements. AH and TG acknowledge support from the Innovation Foundation Grand Solutions project CyberQ (grant agreement 3200-00035B), the Danish National Research Foundation, Center for Macroscopic Quantum States (bigQ, DNRF142), and the Carlsberg Foundation (grant agreement number CF21-0466). This project has also received funding from the European Union's Horizon Europe research and innovation programme under the project "Quantum Security Networks Partnership" (QSNP, grant agreement No. 101114043).

-
- [1] C. H. Bennett, *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, , 175 (1984).
 - [2] C. H. Bennett and G. Brassard, *Theor. Comput. Sci.* **560**, 7 (2014).
 - [3] 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. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, *Adv. Opt. Photon.* **12**, 1012 (2020).
 - [4] R. Colbeck and R. Renner, *Nature Physics* **8**, 450–453 (2011).
 - [5] R. Gallego, L. Masanes, G. D. L. Torre, C. Dhara, L. Aolita, and A. Acín, *Nature Communications* **4**, 2654 (2013).
 - [6] M. W. Mitchell, C. Abellan, and W. Amaya, *Phys. Rev. A* **91**, 012314 (2015).
 - [7] T. Lunghi, J. B. Brask, C. C. W. Lim, Q. Lavigne, J. Bowles, A. Martin, H. Zbinden, and N. Brunner, *Phys. Rev. Lett.* **114**, 150501 (2015).
 - [8] F. G. S. L. Brandão, R. Ramanathan, A. Grudka, K. Horodecki, M. Horodecki, P. Horodecki, T. Szarek, and H. Wojewódka, *Nature Communications* **7**, 11345 (2016).
 - [9] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, *npj Quantum Information* **2**, 16021 (2016).
 - [10] A. Acín and L. Masanes, *Nature* **540**, 213–219 (2016).
 - [11] M. Herrero-Collantes and J. C. Garcia-Escartin, *Rev. Mod. Phys.* **89**, 015004 (2017).
 - [12] M. Hillery, V. Bužek, and A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999).
 - [13] R. Cleve, D. Gottesman, and H.-K. Lo, *Phys. Rev. Lett.* **83**, 648 (1999).
 - [14] J. Ribeiro, G. Murta, and S. Wehner, *Phys. Rev. A* **97**, 022307 (2018).
 - [15] A. Keet, B. Fortescue, D. Markham, and B. C. Sanders, *Phys. Rev. A* **82**, 062315 (2010).
 - [16] C. Ottaviani, C. Lupo, R. Laurenza, and S. Pirandola, *Communications Physics* **2**, 118 (2019).
 - [17] F. Grasselli, H. Kampermann, and D. Bruß, *New Journal of Physics* **21**, 123002 (2019).
 - [18] S. Pirandola, *IET Quantum Communication* **1**, 22 (2020).
 - [19] D. Gottesman and I. Chuang, *quant-ph/0105032* (2001).
 - [20] P. J. Clarke, R. J. Collins, V. D. and Erika Andersson, J. Jeffers, and G. S. Buller, *Nature Communications* **3**, 1174 (2012).
 - [21] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, *Phys. Rev. Lett.* **113**, 040502 (2014).
 - [22] V. Dunjko, P. Wallden, and E. Andersson, *Phys. Rev. Lett.* **112**, 040502 (2014).
 - [23] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, *Phys. Rev. A* **91**, 042304 (2015).
 - [24] C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, *Phys. Rev. Lett.* **117**, 100503 (2016).
 - [25] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, *Opt. Lett.* **41**, 4883 (2016).
 - [26] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, *Nature Communications* **8**, 1098 (2017).
 - [27] D. Mayers, *Phys. Rev. Lett.* **78**, 3414 (1997).
 - [28] H.-K. Lo and H. Chau, *Physica D: Nonlinear Phenomena* **120**, 177 (1998), proceedings of the Fourth Workshop on Physics and Consumption.
 - [29] H. Buhrman, M. Christandl, P. Hayden, H.-K. Lo, and S. Wehner, *Phys. Rev. A* **78**, 022316 (2008).
 - [30] A. Chailloux and I. Kerenidis, in *2011 IEEE 52nd Annual Symposium on Foundations of Computer Science* (2011) pp. 354–362.
 - [31] A. Kent, *Phys. Rev. Lett.* **109**, 130501 (2012).
 - [32] A. Broadbent, J. Fitzsimons, and E. Kashefi, in *2009 50th Annual IEEE Symposium on Foundations of Computer Science* (2009) pp. 517–526.
 - [33] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, *Science* **335**, 303 (2012).
 - [34] S. Barz, J. F. Fitzsimons, E. Kashefi, and P. Walther, *Nature Physics* **9**, 727–731 (2013).
 - [35] J. F. Fitzsimons and E. Kashefi, *Phys. Rev. A* **96**, 012303 (2017).
 - [36] E. Kashefi and A. Pappa, *Cryptography* **1**, 2 (2017).
 - [37] H. J. Kimble, *Nature* **453**, 1023 (2008).
 - [38] K. Azuma, A. Mizutani, and H.-K. Lo, *Nature Communications* **7**, 13523 (2016).
 - [39] S. Pirandola and S. L. Braunstein, *Nature* **532**, 169 (2016).
 - [40] S. Wehner, D. Elkouss, and R. Hanson, *Science* **362**, 6412 (2018).
 - [41] K. Azuma, *De Physicus*, pages: 52–54 (2019).
 - [42] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).

- [43] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
- [44] D. Brūß, Phys. Rev. Lett. **81**, 3018 (1998).
- [45] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
- [46] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).
- [47] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
- [48] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
- [49] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
- [50] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature **421**, 238 (2003).
- [51] R. Filip, Phys. Rev. A **77**, 022310 (2008).
- [52] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).
- [53] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).
- [54] C. Weedbrook, S. Pirandola, and T. C. Ralph, Phys. Rev. A **86**, 022318 (2012).
- [55] C. Weedbrook, C. Ottaviani, and S. Pirandola, Phys. Rev. A **89**, 012309 (2014).
- [56] C. Ottaviani, M. Woolley, M. Erementchouk, J. Federici, P. Mazumder, S. Pirandola, and C. Weedbrook, IEEE Journal on Selected Areas in Communications **38**, 483 (2020).
- [57] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
- [58] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
- [59] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Nature Physics **4**, 726–730 (2008).
- [60] I. B. Djordjevic, IEEE Photonics Journal **12**, 1 (2020).
- [61] I. B. Djordjevic, IEEE Access **10**, 23284 (2022).
- [62] I. W. Primaatmaja, C. C. Liang, G. Zhang, J. Y. Haw, C. Wang, and C. C.-W. Lim, Quantum **6**, 613 (2022).
- [63] M. E. Mycroft, T. McDermott, A. Buraczewski, and M. Stobińska, Phys. Rev. A **107**, 012607 (2023).
- [64] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
- [65] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).
- [66] S. Pirandola, Commun. Phys. **2**, 51 (2019), see also preprint arXiv:1601.00966 (2016).
- [67] S. Pirandola, Quantum Science and Technology **4**, 045006 (2019).
- [68] S. L. Braunstein and S. Pirandola, Phys. Rev. Lett. **108**, 130502 (2012).
- [69] H.-K. Lo, M. Curty, and B. Qi, Phys. Rev. Lett. **108**, 130503 (2012).
- [70] Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, J. Wang, K. Cui, H.-L. Yin, N.-L. Liu, L. Li, X. Ma, J. S. Pelc, M. M. Fejer, C.-Z. Peng, Q. Zhang, and J.-W. Pan, Phys. Rev. Lett. **111**, 130502 (2013).
- [71] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nature Communications **5**, 3732 (2014).
- [72] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Nature **557**, 397 (2018).
- [73] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Nature Photonics **13**, 334–338 (2019).
- [74] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, and S. L. Braunstein, arXiv:1312.4104v1 (2013).
- [75] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, Nature Photonics **9**, 397 (2015).
- [76] X.-C. Ma, S.-H. Sun, M.-S. Jiang, M. Gui, and L.-M. Liang, Phys. Rev. A **89**, 042335 (2014).
- [77] Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, Phys. Rev. A **89**, 052301 (2014).
- [78] Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, Phys. Rev. A **97**, 042328 (2018).
- [79] H.-X. Ma, P. Huang, D.-Y. Bai, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Phys. Rev. A **97**, 042329 (2018).
- [80] Y. Zhang, Z. Li, C. Weedbrook, K. Marshall, S. Pirandola, S. Yu, and H. Guo, Entropy **17**, 4547 (2015).
- [81] P. Wang, X. Wang, and Y. Li, Phys. Rev. A **99**, 042309 (2019).
- [82] M. Ghalaii and S. Pirandola, Phys. Rev. A **108**, 042621 (2023).
- [83] Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, and H. Guo, Phys. Rev. A **90**, 052325 (2014).
- [84] D. Bai, P. Huang, H. Ma, T. Wang, and G. Zeng, Journal of Physics B: Atomic, Molecular and Optical Physics **52**, 135502 (2019).
- [85] D. Bai, P. Huang, Y. Zhu, H. Ma, T. Xiao, T. Wang, and G. Zeng, Quantum Information Processing **19** (2019).
- [86] H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, W.-S. Bao, and G.-H. Zeng, Phys. Rev. A **99**, 022322 (2019).
- [87] Q. Liao, Y. Wang, D. Huang, and Y. Guo, Opt. Express **26**, 19907 (2018).
- [88] P. Papanastasiou, C. Ottaviani, and S. Pirandola, Phys. Rev. A **96**, 042332 (2017).
- [89] A. G. Mountogiannakis, P. Papanastasiou, and S. Pirandola, Phys. Rev. A **106**, 042606 (2022).
- [90] K. N. Wilkinson, P. Papanastasiou, C. Ottaviani, T. Gehring, and S. Pirandola, Phys. Rev. Research **2**, 033424 (2020).
- [91] A. I. Fletcher and S. Pirandola, Sci Rep **12**, 17329 (2022).
- [92] M. Ghalaii, P. Papanastasiou, and S. Pirandola, npj Quantum Inf **8**, 105 (2022).
- [93] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
- [94] A. Fletcher, PhD Thesis, University of York (2023).
- [95] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Physical Review Letters **89**, 167901 (2002).
- [96] C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, Phys. Rev. A **97**, 052327 (2018).
- [97] P. Papanastasiou, A. Mountogiannakis, and S. Pirandola, Sci. Rep. **13**, 11636 (2023).
- [98] S. Pirandola and P. Papanastasiou, Phys. Rev. Res. **6**, 023321 (2024).
- [99] Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, Z. Lu, X. Wang, and Y. Li, Optica **9**, 492 (2022).
- [100] A. A. Hajomer, H. Q. Nguyen, and T. Gehring, arXiv preprint arXiv:2210.07576 (2022).
- [101] A. A. Hajomer, U. L. Andersen, and T. Gehring, arXiv preprint arXiv:2303.01611 (2025).
- [102] A. A. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, S. Bastiaens, U. L. Andersen, X. Yin, and T. Gehring, Optica **11**, 1197 (2024).