SCIENCE CHINA
Information Sciences

• REVIEW •

August 2025, Vol. 68, Iss. 8, 180501:1–180501:17
https://doi.org/10.1007/s11432-024-4491-9

Special Topic: Quantum Information

Advances in continuous variable measurement-device-independent quantum key distribution

Pu WANG[1], Yan TIAN[2*] & Yongmin LI[3,4,5*]

[1]*School of Information, Shanxi University of Finance and Economics, Taiyuan 030006, China*
[2]*School of Information and Communication Engineering, North University of China, Taiyuan 030051, China*
[3]*State Key Laboratory of Quantum Optics Technologies and Devices, Institute of Opto-Electronics, Shanxi University, Taiyuan 030006, China*
[4]*Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan 030006, China*
[5]*Hefei National Laboratory, Hefei 230088, China*

Received 27 December 2024/Revised 25 March 2025/Accepted 10 June 2025/Published online 8 July 2025

Abstract Continuous variable quantum key distribution (CV-QKD), utilizes continuous variables encoding such as the quadrature components of the quantized electromagnetic field and coherent detection decoding, offering good compatibility with the existing telecommunications technology and components. Continuous variable measurement-device-independent QKD (CV-MDI-QKD) can eliminate all the security threats arising from the receiver effectively, the crucial security loophole of CV-QKD implementations. Recently, CV-MDI-QKD has attracted extensive attention and witnessed rapid progress. Here, we review the achievements that have been made in the field of CV-MDI-QKD, including the basic principle, advancements in theoretical protocols, and experimental demonstrations. Finally, we discuss the challenges faced in practical applications and future research directions.

Keywords quantum key distribution, continuous variable, measurement-device-independent, quantum conferencing, quantum communication

Citation Wang P, Tian Y, Li Y M. Advances in continuous variable measurement-device-independent quantum key distribution. Sci China Inf Sci, 2025, 68(8): 180501, https://doi.org/10.1007/s11432-024-4491-9

1 Introduction

Quantum key distribution (QKD) is the most mature technology in quantum information processing, enabling two distant parties, Alice and Bob, to establish a common secret key over an insecure quantum channel with the aid of an authenticated classical channel [1–4]. The security of QKD is fundamentally guaranteed by the principles of quantum mechanics, ensuring that any eavesdropping attempt by Eve introduces detectable perturbations on the quantum states that carry the key information [5–8]. Among various QKD protocols [9–11], continuous variable (CV) QKD has garnered great research interests recently [12–19], given its compatibility with the modern coherent optical communication techniques and its potential to achieve high secret key rates at metropolitan distances using multiphoton quantum states encoding and coherent detection (homodyne or heterodyne).

As a promising solution for secure communication in metropolitan quantum networks, CV-QKD systems have achieved notable achievements, with numerous protocols proposed and experimentally demonstrated over the past two decades [19]. The research primarily focuses on three aspects: analyzing the security of the protocol against various attack strategies potentially employed by an eavesdropper (Eve) and addressing practical security challenges arising from imperfections in real devices [20–40]; enhancing the protocol's performance to achieve higher secure key rates and longer transmission distances [41–61]; promoting the miniaturization, low power consumption, and cost-effectiveness of the protocol's implementation, including protocol simplifications, multi-user network applications, and on-chip integration [62–82]. Despite these achievements, practical implementation challenges still exist, especially the practical security of CV-QKD. Theoretically, the CV-QKD protocols have been proven to be information-theoretically

* Corresponding author (email: tianyan@nuc.edu.cn, yongmin@sxu.edu.cn)

secure under ideal conditions. However, real-world physical devices often deviate from these ideal assumptions, leading to potential security loopholes that can be exploited by adversaries. An effective solution is the device-independent (DI) QKD protocol [83,84], aiming to eliminate all assumptions about the internal working mechanisms of QKD devices. However, it currently remains impractical due to low secret key rates and short transmission distances.

A more feasible solution came with the introduction of measurement-device-independent QKD (MDI-QKD) [85,86], which removes all side-channel attacks on measurement devices, the most vulnerable part of QKD implementations. Moreover, it is particularly suitable for star-type metropolitan QKD networks. The concept of MDI-QKD was lately extended to the CV framework, so-called CV-MDI-QKD [87–89]. In this protocol, Alice and Bob independently prepare CV quantum states and send them to an untrusted third party, Charlie, who performs CV Bell-state measurement (BSM) and broadcasts the outcomes. This protocol allows for the establishment of a secure key between Alice and Bob without relying on trusted detectors, thus closing known and unknown side-channel attacks on the detection side and significantly enhancing practical security.

The inherent advantages of CV-MDI-QKD have attracted intense research attention and witnessed rapid progress in recent years. This review is devoted to providing a comprehensive overview of the state-of-the-art in CV-MDI-QKD. We first delineate the procedures and fundamental principle of the CV-MDI-QKD protocol. Subsequently, we conduct an exhaustive review of the theoretical advancements in the field, encompassing protocol design and optimization, as well as in-depth security analysis. Furthermore, we present the recent proof-of-principle experimental validations. Finally, the review outlines the challenges and future research directions that lie ahead in the field, providing insights into the potential pathways for further advancements and developments.

2 CV-MDI-QKD protocol

2.1 Protocol description

When describing QKD protocols, two schemes are typically employed: "prepare-and-measure" (PM) and "entanglement-based" (EB). The PM scheme is usually easy to implement in practice, while the equivalent EB scheme is convenient for the security analysis of the protocol. To understand how the CV-MDI-QKD protocol works, we start with the PM scheme involving Gaussian-modulated coherent states. It is one of the most widely used CV-MDI-QKD protocols and has been experimentally demonstrated [90]. The schematic setup is shown in Figure 1 and the protocol can be implemented by the following steps.

(1) At the transmitter, Alice and Bob, each independently encode the key information on the amplitude and phase quadratures of a series of coherent states $|\alpha_A\rangle$ and $|\alpha_B\rangle$ by using amplitude and phase modulators. In the phase space, the encoded states are expressed as $|\alpha_A\rangle = |x_A + ip_A\rangle$ and $|\alpha_B\rangle = |x_B + ip_B\rangle$, where x_A and p_A (x_B and p_B) represent two independent field quadratures with zero mean and identical variance V_A (V_B) in shot-noise units (SNUs). Subsequently, both Alice and Bob send their coherent states to an untrusted quantum relay, Charlie, via two unsecured lossy and noisy quantum channels.

(2) At the receiver, a CV BSM is performed. To this end, Charlie applies a beam splitter (BS) with a transmittance of 50% to interfere with the received signal states and establish the correlation. The output states are subsequently detected by using two homodyne detectors: one detects the amplitude quadrature and the other detects the phase quadrature, and the final measurement results are publicly declared by Charlie.

(3) Since Alice and Bob independently prepare their coherent states, whose complex amplitudes follow independent and identically distributed, zero-mean Gaussian distributions, their initial data sets are uncorrelated. To obtain a secret key, Alice and Bob apply a displacement operation to their data based on Charlie's measurement outcomes. Specifically, upon receiving Charlie's measurement results, Alice and Bob adjust their data as follows: $X_A = x_A - g_{x_A}(r)$, $P_A = p_A - g_{p_A}(r)$, $X_B = x_B - g_{x_B}(r)$, $P_B = p_B - g_{p_B}(r)$, where g_* ($* = x_A, p_A, x_B, p_B$) represent the displacement coefficients that relate to Charlie's measurement results [90,91]. By conditionally displacing their data, Alice and Bob can achieve correlated data sets.

(4) Finally, by implementing parameter estimation, information reconciliation, and privacy amplification procedures, the secret keys can be extracted.

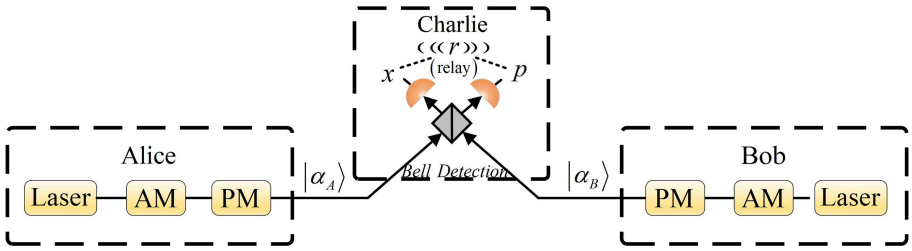

Figure 1 (Color online) PM scheme of the CV-MDI-QKD protocol with Gaussian-modulated coherent states.

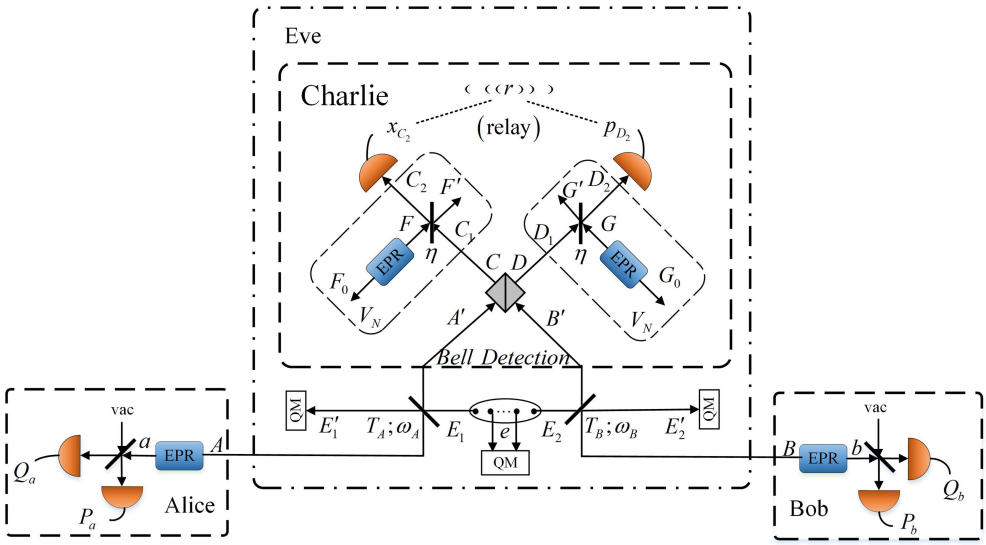

Figure 2 (Color online) Equivalent EB scheme of the CV-MDI-QKD protocol with Gaussian-modulated coherent states.

2.2 Security analysis

The security of CV-MDI-QKD protocol can be established through the implementation of an equivalent EB scheme, as depicted in Figure 2. In this scheme, instead of distributing the coherent states, Alice and Bob each generate an Einstein-Podolsky-Rosen (EPR) pair aA or bB, respectively. Subsequently, they perform heterodyne detection on the retained mode a or b, which projects mode A or B onto coherent states. Modes A and B are transmitted to a trusted third party, Charlie, via separate quantum channels with length L_{AC} and L_{BC}, respectively. The received Modes A' and B' of Charlie interfere at a BS and output two modes C and D. Then the x quadrature of mode C and the p quadrature of mode D are measured using balanced homodyne detectors, respectively. The realistic homodyne detectors are modeled by assuming that the signal is attenuated by a BS with transmission efficiency η and mixed with some thermal noise V_N which simulates the electronic noise v_{el} of the detector, before detected by a perfect homodyne detector. Charlie publicly announces the complex variable $r = (x_{C_2} + ip_{D_2})/\sqrt{2}$ to both Alice and Bob through an authenticated classical channel. Here, the knowledge of r enables them to infer each other's data through the previously discussed data processing techniques. Consequently, a correlation between Alice and Bob is established and results in mutual information $I_{ab|r} > 0$. Finally, the secret keys are extracted via classical data post-processing techniques including parameter estimation, information reconciliation, and privacy amplification.

It is worth noting that a realistic joint two-mode Gaussian attack can be performed by Eve on the two quantum channels of the CV-MDI-QKD. As illustrated in Figure 2, Eve mixes two ancillary modes, denoted as E_1 and E_2, with the two incoming modes, A and B, respectively, through two BSs with a transmittance of T_A and T_B. The covariance matrix can be expressed as [87]

$$\gamma_{E_1E_2} = \begin{bmatrix} \omega_A I & G \\ G & \omega_B I \end{bmatrix}, \; G = \begin{bmatrix} g & 0 \\ 0 & g' \end{bmatrix}, \tag{1}$$

where ω_A and ω_B denote the variances of the thermal noise introduced by E_1 and E_2, respectively.

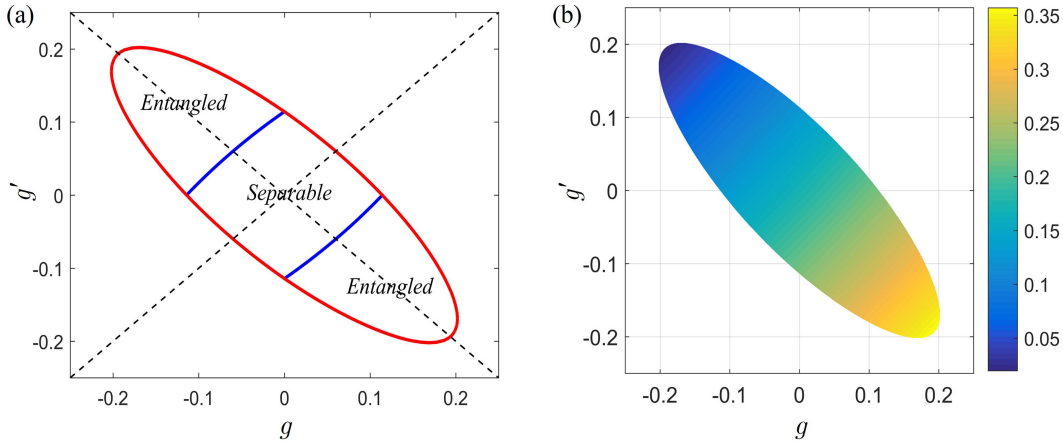

Figure 3 (Color online) (a) Correlation region (g,g') for $\omega_A = 1.21$ and $\omega_B = 1.02$; (b) achievable secret key rate in the correlation region (g, g').

g and g' represent the quantum correlations between the two modes and must adhere to the physical limitations imposed by the Heisenberg uncertainty principle, which imposes physical constraints on the possible values of g and g' as

$$\gamma_{E_1E_2} > 0,\ \lambda_-^2 \geqslant 1, \tag{2}$$

where λ is the least symplectic eigenvalue of $\gamma_{E_1E_2}$.

Such constraints imply that accessible values of g and g' only exist in a limited region, which is surrounded by a red elliptical curve, as shown in Figure 3(a). The region is further divided into two sub-regions. The inner area corresponds to the separable attacks performed by Eve, while the two outer areas denote the entangled attacks. The region is symmetric with respect to the two bisectors $g' = g$ and $g' = -g$ (dashed lines). There are two distinct zones for entangled attacks. In the bottom-right zone, Eve introduces "beneficial" entanglement, referred to as the "positive EPR attack", which aids in the Bell detection process. Conversely, in the top-left zone, Eve injects "harmful" entanglement, and this "negative EPR attack" undermines the Bell detection process. It has been proved that the most effective "negative EPR attack" is located at the top-left point in which [87, 92–94]

$$\begin{aligned} &g' = -g = \phi, \\ &\phi = \min\left\{\sqrt{(\omega_A - 1)(\omega_B + 1)}, \sqrt{(\omega_A + 1)(\omega_B - 1)}\right\}. \end{aligned} \tag{3}$$

Figure 3(b) provides a more intuitive depiction, where the secret key rate in the correlation region (g, g') is presented. At the top-left point of the region, the secret key rate achieves its minimum value.

Since the protocol is symmetric, for convenience, we assume that Alice is the encoder and Bob is the decoder. After the declaration of Charlie's outcome r, the asymptotical secret key rate (i.e., for raw keys of infinite length) against collective attacks is given by [87]

$$K^{\infty} = \beta \cdot I_{ab|r} - \chi_{aE|r}, \tag{4}$$

where β denotes the reconciliation efficiency; $I_{ab|r}$ denotes the Shannon mutual information between Alice and Bob; and $\chi_{aE|r}$ denotes the Holevo bound between Alice and Eve, which puts an upper limit on the information available to Eve on Alice's key. Based on the purification of Eve's system, $\chi_{aE|r}$ can be calculated by the von Neumann entropy of the quantum states $\rho_{ab|r}$ and $\rho_{b|ra}$.

In practice, there are two application scenarios for the protocol: the symmetric configuration ($L_{AC} = L_{BC}$) and the asymmetric configuration ($L_{AC} \neq L_{BC}$). In the symmetric configuration, the maximum achievable distance is about 3.8 km of standard optical fiber from the relay with present technology [87]. The performance of the asymmetric case is superior to the symmetric case. When Alice is the encoder of information, the transmission distance L_{BC} increases significantly as L_{AC} decreases. For the most asymmetric case ($L_{AC} = 0$), a key rate of 2×10^{-4} bit/pulse can be achieved at a distance of 170 km under ideal conditions [95].

By including the finite data statistics effect for the parameter estimation and the post-processing costs, the security of CV-MDI-QKD protocol with Gaussian-modulated coherent states has been extended to

the finite-size scenario under realistic conditions [96, 97]. In the finite-size scenario, the secret key rate can be expressed as follows:

$$K^{\text{finite}} = \frac{n}{N}\left[\beta \cdot I_{ab|r} - \chi_{aE|r} - \Delta(n)\right], \tag{5}$$

where N denotes the total number of signals exchanged between Alice and Bob. A portion of the signals, specifically $(N-n)$, are devoted to the task of parameter estimation, and the remaining n signals are utilized for key extraction. The parameter $\Delta(n)$ is defined by $\Delta(n) \approx 7\sqrt{\left(\log_2(2/\overline{\epsilon})\right)/n}$, reflecting the robustness of the privacy amplification process.

A critical component in the finite-size setting is parameter estimation, which takes into account the maximum discrepancy between expected and observed values arising from statistical fluctuations. As indicated in [91], CV-MDI-QKD facilitates parameter estimation with a significantly reduced requirement for public communication. This advancement permits Alice and Bob to utilize their complete raw data for both parameter estimation and secret key extraction, thereby negating the conventional trade-off between key extraction and the accuracy of the parameter estimation in the finite-size regime. By exploiting this parameter estimation technique and min-entropy estimation approach introduced in [29], a rigorous finite-size analysis with composable security has been conducted [98]. Within this composable security framework, the lower bound for the secret key rate against collective Gaussian attacks is expressed as [98]

$$K_{\text{com-col}}^{s'} = R^L - \frac{1}{\sqrt{N}}\Delta_{\text{AEP}} + \frac{1}{N}\log_2\left(p - \frac{2}{3}ps_{\text{SM}}\right) + \frac{2}{N}\log_2(2s), \tag{6}$$

where s' denotes the overall security parameter, which is composed of several contributing components and can be expressed as $s' = s + s_{\text{SM}} + s_{\text{EC}} + s_{\text{PE}}$.

Specifically, s originates from the leftover hash lemma; S_{SM} represents the smoothing parameter involved in the smooth conditional min-entropy; S_{EC} signifies the error within the error-correction routine, and S_{PE} denotes the probability of error associated with the parameter estimation procedure. Additionally, p is the probability of successful error correction. $\Delta_{\text{AEP}} = 4(d+1)\sqrt{\log_2(9/2p^2s_{\text{SM}}^2)}$ and d represents the number of bits employed to encode each measurement result. Furthermore, R^L is given by

$$R^L = \beta \cdot I_{ab}\left(\Omega_a^{\max}, \Omega_b^{\max}, \Omega_c^{\min}\right) - \chi_{aE}\left(\Omega_a^{\max}, \Omega_b^{\max}, \Omega_c^{\min}\right), \tag{7}$$

where $\Omega_a^{\max}$, $\Omega_b^{\max}$ and $\Omega_c^{\min}$ are the boundary values on the covariance matrix elements accounting for statistical fluctuations, which collectively provide a lower bound on the secret key rate.

Finally, by involving Gaussian de Finetti reduction technique [99], the security proof is extended to the most general class of coherent attacks, resulting in the following lower bound for the secret key rate [98]:

$$K_{\text{com-coh}}^{s''} = \frac{N-k}{N}R^L - \frac{\sqrt{N-k}}{N}\Delta_{\text{AEP}} + \frac{1}{N}\log_2\left(p - \frac{2}{3}ps_{\text{SM}}\right) + \frac{2}{N}\log_2(2s) - \frac{2}{N}\log_2\binom{K+4}{4}, \tag{8}$$

where the security parameter $s'' = s'K^4/50$, $K \sim N$, and k represents the number of signals employed in the energy test.

In Figure 4, we provide a detailed comparison of secret key rates under different security frameworks and key sizes. It is evident that different security frameworks and key sizes significantly influence the performance of the protocol. It is crucial to improve the composable security proof in the finite-size regime to mitigate the impact of finite key size in the future.

3 Theoretical advances of CV-MDI-QKD

After the first Gaussian-modulated coherent states CV-MDI-QKD protocol was proposed, many efforts have been made to improve the protocol. For instance, various protocols have been developed to reduce the complexity of the system, enhance the performance of the protocol, and improve realistic security, as summarized in Table 1 [100–137].

The unidimensional modulation, discrete modulation, and passive-state preparation schemes were introduced to reduce the complexity of the CV-MDI-QKD system. In the unidimensional modulation scheme [100], both Alice and Bob use one modulator to implement the single-quadrature modulation, then the prepared quantum states are sent to Charlie for BSM. In this case, the signal modulations as well as the corresponding parameter estimations can be simplified. The discrete modulation [101, 102],

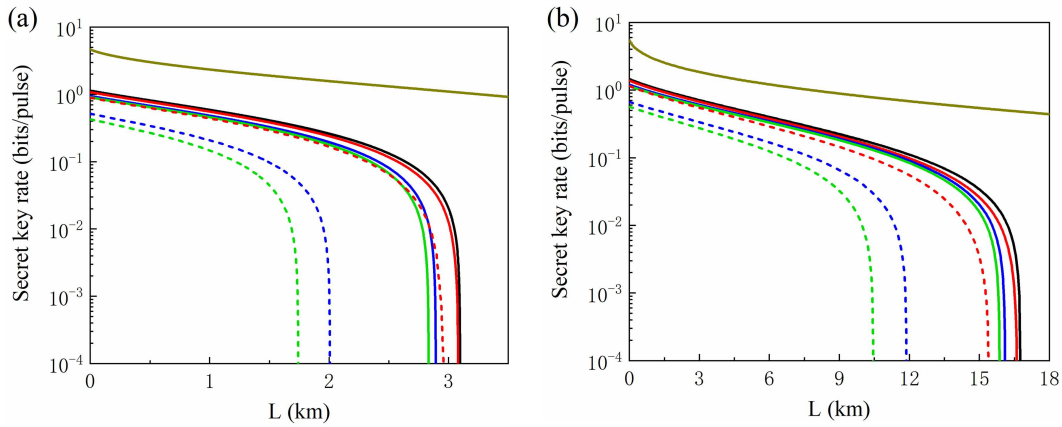

Figure 4 (Color online) Secret key rate versus the transmission distance under different security frameworks. (a) represents the symmetric case with $L_{AC} = L_{BC}$, and (b) represents the most asymmetric case with $L_{AC} \approx 0$ km. The upper (dark yellow) solid curve illustrates the asymptotical secret key rate in the ideal case, characterized by perfect reconciliation efficiency ($\beta = 1$), zero excess noise ($\varepsilon_A = \varepsilon_B = 0$) and ideal detection ($\eta = 1$, $v_{el} = 0$). The black, red, blue, and green curves illustrate the following security levels under realistic scenario with parameters $\beta = 0.97$, $\varepsilon_A = \varepsilon_B = 0.01$, $\eta = 0.97$, and $v_{el} = 0.01$: asymptotic security, finite-size security, composable security against collective Gaussian attacks, and composable security against coherent attacks. The modulation variance has been optimized. The solid and dashed curves correspond to block lengths of $N = 10^{10}$ and $N = 10^8$, respectively.

for example, a four-state scheme, further simplifies the state preparation and allows a good reconciliation efficiency at a low signal-to-noise ratio. Apart from the active state preparation, passive-state preparation is also an attractive alternative for the practical application of CV-MDI-QKD protocol [103, 104], where both Alice and Bob passively prepare quantum states using a true thermal source.

To enhance the performance of the original protocol in terms of the secret key rate and distance, a variety of schemes have been proposed. The squeezed states scheme was introduced into the CV-MDI framework to attain better performance [105, 106]. Later, the modulated squeezed states [107] that combined the advantages of both the squeezed and coherent states was proposed, it can achieve a higher secret key rate and transmission distance than previous protocols. Besides, other schemes including multi-mode modulation [108], one-time shot-noise-unit calibration [109], optical amplifier [107, 110], photon subtraction [111–114], quantum catalysis [115–117], quantum scissor [118], and postselection [119, 120], have also been studied.

A key security assumption in MDI-QKD is that the source is trusted. Even though one can prepare the source with good fidelity in practice, there are inevitably some preparation errors. There are several studies that use different approaches to prove the realistic security of the imperfect state preparation [121–123]. Recently, a countermeasure for negative impact introduced by the actual source in the CV-MDI-QKD system based on the one-time calibration method was proposed [124]. To solve the local oscillator (LO) transmission, the plug-and-play (P&P) technique [125, 126] and Bayesian phase-noise estimation technique [127] were introduced, eliminating the need for transmitting high-intensity LOs. Additionally, researchers also analyzed the performance of CV-MDI-QKD protocols under various complex communication environments, such as fluctuating channel transmittance [128], rainy and foggy weather environment [129], underwater communication [130], satellite-to-submarine model [131], and free-space optical links [132]. These results provide useful guidance for practical applications.

CV-MDI-QKD can be extended to multi-party quantum communication, offering a promising path towards realizing complex and sophisticated quantum networks [87]. In a multi-party setting, multiple users can be connected to a common untrusted node, allowing them to establish and share the secret keys. Quantum secret sharing (QSS) is a typical multi-party quantum communication protocol, where a secret is distributed to network users and the secret becomes accessible only when all legitimate participants agree to collaborate. CV-MDI-QSS can remove all detector side-channel attacks, thereby significantly enhancing the security of QSS in practical applications. CV-MDI-QSS was first investigated in a three-party network by utilizing the post-processed CV Greenberger-Horne-Zeilinger (GHZ) state, which is obtained by using the idea of entanglement swapping [133]. As shown in Figure 5(a), the three participants (Alice, Bob, and Charlie) rely on the measurements taken by an untrusted relay, David, to establish secure communication among themselves. After the measurement outcomes are broadcasted, Alice and Bob keep their data

Table 1 Theoretical advances of CV-MDI-QKD.

Category	References	Approach	Basic idea	Security proof
Protocol simplification	[100]	Unidimensional modulation	Using one modulator instead of two to reduce the complexity and cost of sources.	Finite-size security against collective attacks
	[101,102]	Discrete modulation	Using QPSK to avoid the complexity of the Gaussian modulation.	Asymptotical security against collective attacks
	[103,104]	Passive-state preparation	Preparing quantum states using a thermal source.	Finite-size security against collective attacks
Performance enhancement	[105,106]	Squeezed states	Employing Gaussian-modulated squeezed states to suppress quantum noise originating from the source.	Composable security against coherent attacks
	[107]	Modulated squeezed states	Simultaneously modulating the amplitude and phase of the squeezed states to expand their distribution range in phase space.	Finite-size security against collective attacks
	[108]	Multi-mode states	Transmitting multiple independent quantum states simultaneously through a single quantum channel to increase the utilization efficiency of the channel.	Asymptotical security against collective attacks
	[109]	One-time shot-noise-unit calibration	Replacing multiple measurement calibrations with a one-time calibration to simplify the calibration procedure and reduce statistical fluctuations.	Asymptotical security against collective attacks
	[107,110]	Optical amplifier	Using a phase-sensitive optical amplifier to implement noiseless amplification of a chosen quadrature and squeezing of the conjugate quadrature.	Finite-size security against collective attacks
	[111–114]	Photon subtraction	Implementing the (virtual) photon subtraction operation to increase and distill the entanglement of the source.	Asymptotical security against collective attacks
	[115–117]	Quantum catalysis	Using the zero-photon catalysis to reduce the intensity of the quantum signal without introducing additional noise.	Asymptotical security against Gaussian attacks
	[118]	Quantum scissor	Truncating certain multiphoton states and probabilistically amplifying the remaining states to enhance communication fidelity and entanglement.	Asymptotical security against Gaussian attacks
	[119,120]	Postselection	Selecting only the measurement outcomes that most likely contribute to positive secure keys.	Composable security against collective attacks
Realistic source model	[121]	Noisy coherent states	Simulating noise by mixing an EPR pair with transmitted states at a beam splitter.	Asymptotical security against collective attacks
	[122]	Imperfect state preparation	Simulating noise by combining a phase-insensitive amplifier with transmitted States.	Asymptotical security against collective attacks
	[123]	Source-intensity errors	Establishing a general source intensity errors model and proposing data processing schemes to reduce the adverse effects of intensity errors.	Composable security against collective attacks
	[124]	Source monitoring with one-time-calibration	Considering a practical source monitoring model and eliminating the loophole induced from the relative intensity noise based on the one-time-calibration method.	Finite-size security against collective attacks
Local oscillator transmission	[125,126]	Plug-and-play	Generating the local oscillator at Charlie's side to avoid the synchronization challenges arising from separate lasers of Alice and Bob.	Finite-size security against collective attacks
	[127]	Bayesian phase-noise estimation	Interfering Alice's quantum signal pulses with Bob's local oscillator pulses and performing Bayesian phase estimation.	Asymptotical security against Gaussian attacks
Complex communication environments	[128]	Fluctuating channel transmittance	Constructing a parameter estimation model to accommodate fluctuating channel transmittance.	Asymptotical security against collective attacks
	[129]	Diverse weather conditions	Considering the effects of beam energy's attenuation on rainy days and beam extinction in the foggy condition on channel transmittance.	Asymptotical security against collective attacks
	[130]	Underwater communication	Considering the effects of sun elevation angle, as well as the temperature and salinity of seawater, on channel transmittance.	Asymptotical security against collective attacks
	[131]	Satellite-to-submarine model	Locking Charlie on the sea surface to remove the need for a sea surface channel and estimating the effects of atmospheric (satellite-to-Charlie) and seawater (Charlie-to-submarine) on channel transmittance.	Composable security against collective attacks
	[132]	Free-space optical links	Analyzing the effects of free-space optical links on channel transmission and noise, and establishing composable security.	Composable security against collective attacks
Multi-Party quantum communication	[110, 133–135]	Quantum secret sharing	The secret is distributed among network users, and access to the original secret is permitted only when all legitimate participants agree to collaborate.	Asymptotical security against collective attacks
	[136,137]	Quantum conferencing	Introducing generalized Bell detection based MDI star-network module, and using the one-time pad to connect different modules.	Composable security against coherent attacks

unchanged, while Charlie revises his data to ensure that their combined data satisfies $p_A + p_B + p'_C \to 0$. Two of them share their private data with each other. By implementing the data reconciliation and post-processing procedures, they can collaborate to obtain the third person's secret keys. Subsequently, the three-party CV-MDI-QSS was extended to a four-party scheme, where four participants (Alice, Bob, Charlie and David) prepare and send EPR states to the untrusted relay to construct four-party CV GHZ state [110]. Recently, the three-party CV-MDI-QSS was investigated under the fast-fading channel, implying its adaptability in dynamic channel environments [134]. Moreover, current research suggests that implementing CV-MDI-QSS with coherent states is practical and could potentially support a larger number of users (Figure 5(b)) [135].

Another interesting application of multi-party CV-MDI-QKD is quantum conferencing [136,137], where multiple parties can securely share information in a group setting. Figure 5(c) plots the modular network model for quantum conferencing, where each module M_i represents a star network as shown in Figure 5(d) [136]. Two different modules can be connected by a pair of trusted users. In each star-network module, each of N_i users prepares their own signal states according to the Gaussian distribution and sends them to an untrusted relay node via quantum channels, where a multipartite CV Bell detection

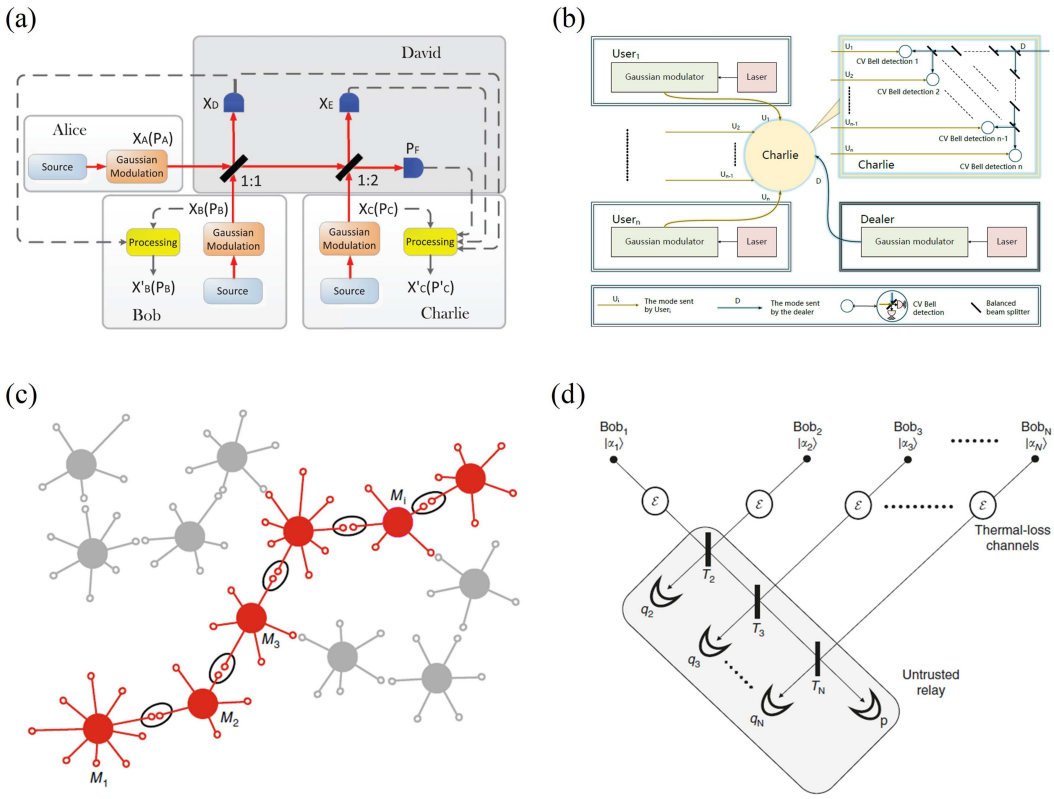

Figure 5 (Color online) (a) Three-party CV-MDI-QSS scheme [133] Copyright 2016 American Physical Society. (b) Schematic diagram of CV-MDI-QSS with n users and a dealer connected to Charlie via quantum channels [135] Copyright 2025 John Wiley and Sons. (c) Modular network for secure quantum conferencing [136] Copyright 2019 Springer Nature. (d) Each module M_i is a star network comprised of a central untrusted relay and N_i trusted users [136] Copyright 2019 Springer Nature.

Table 2 Experimental demonstrations of CV-MDI-QKD.

Ref.	Year	Repetition rate	Reconciliation efficiency	Distance/loss		Total detection efficiency	Excess noise (SNU)	Finite size	SKR
				L_A	L_B				
[87]	2015	100 kHz	0.97	0.087 dB	4 dB	98%	0.01	–	0.1 bits/use
[90]	2022	500 kHz	0.97	0.1 km	10 km	97.20%	0.0045	–	0.19 bits/use
[138]	2023	5 MBaud	0.97	0 dB	2 dB	94%	0.11	–	0.12 bits/use
[139]	2025	20 MBaud	0.97	0 km	10 km	94%	0.0395	4×10^6	2.6 Mbits/s

is performed. After the measurement outcomes are broadcasted, all users in module M_i reconcile their data with a trusted user that is shared with another module M_j. As the distance from the central relay increases or the number of users rises, the secret key rate for each star network decreases. In ideal conditions, within a radius of 40 m, a typical distance for a large building, 50 users can communicate privately with a secret key rate exceeding 0.1 bit per signal use.

4 Experimental advances of CV-MDI-QKD

In this section, we overview the experimental advances of CV-MDI-QKD, which are summarized in Table 2 [87, 90, 138, 139].

In 2015, the first proof-of-principle demonstration of CV-MDI-QKD was reported [87], as shown in Figure 6. A high-stability continuous wave laser at 1064 nm was divided into two parts and delivered to Alice and Bob, respectively. Both Alice and Bob use amplitude and phase modulators to modulate the light field independently with zero-centered Gaussian distributions in phase space. Subsequently, the signal fields were transmitted to the receiver's site, Charlie, through free space. At Charlie's site, the signal fields sent by Alice and Bob interfere at a free-space 50:50 BS, and a pair of conjugate quadratures of the output fields are measured by two high-efficiency balanced homodyne detectors. The quantum

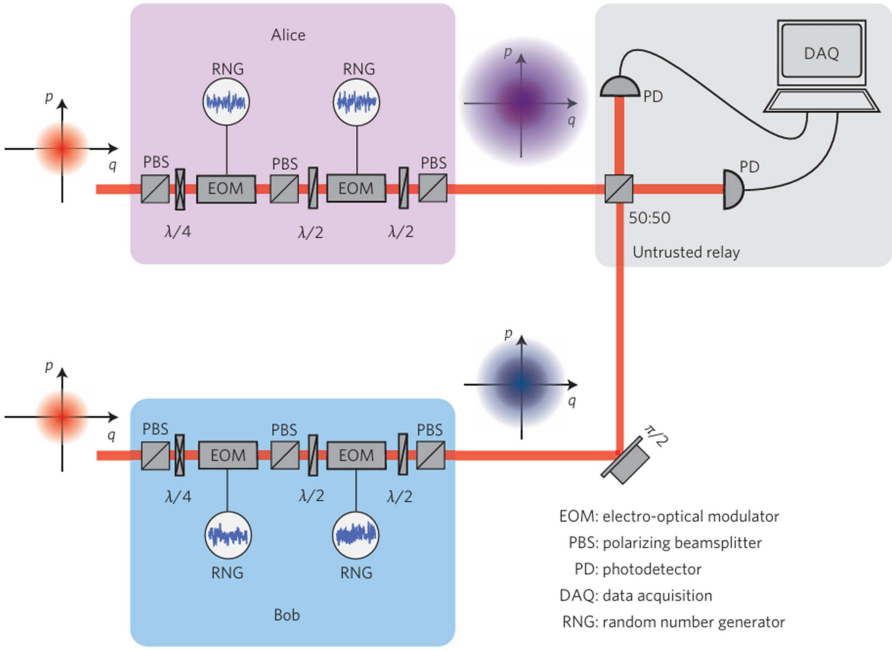

Figure 6 (Color online) Proof-of-principle demonstration of CV-MDI-QKD [87] Copyright 2015 Springer Nature.

signal was encoded on the sidemode, and the carrier of the laser beam was used as the LO. Thus, the continuous-variable BSM was significantly simplified by directly subtracting and adding the measurement results of the balanced BS output modes, which produce the difference between the amplitude quadratures and the sum of the phase quadratures. The losses in the links were simulated by varying the variances of the modulation signals. With a reconciliation efficiency of 97% and a total quantum efficiency of 98%, the secret key rate achieved in this experiment is three orders of magnitude higher than that of the qubit-based protocols over metropolitan area, providing a promising solution for building high-rate metropolitan quantum networks.

The crucial issue that makes the long-distance CV-MDI-QKD challenging is the implementation of high-efficiency CV-BSM of two remote independent quantum states, which requires the establishment of a reliable phase reference between two spatially separated lasers. The dual-homodyne detection is required to achieve simultaneous measurement of a pair of conjugate quadratures. Besides, the imperfect detection efficiency at Charlie's site is equivalent to optical losses that inevitably induce vacuum fluctuation noises, which, along with detector electronic noises, both contribute to the untrusted noises. Hence, the performance of CV-MDI-QKD heavily depends on the detection efficiency of Charlie's detectors, which requires high-efficiency photodiodes and low transmission loss.

In 2022, the experimental demonstration of CV-MDI-QKD over long-distance optical fiber was realized [90], where a technology that consists of optical phase locking, phase estimation, real-time phase feedback, and quadrature remapping was developed to accurately implement CV-BSM of remote independent quantum states, as shown in Figure 7. Two single-frequency continuous-wave lasers with linewidth of kHz at 1550 nm were employed by Alice and Bob. An optical phase-locked loop technique was adopted to compensate for the frequency difference between the two independent lasers, where part of Alice's laser beam is frequency-up-shifted by 80 MHz and sent to Bob's station, which interferes with part of Bob's laser beam to generate a beat signal for frequency-locking. Subsequently, both Alice and Bob adopt two cascaded amplitude modulators to generate 50-ns light pulses with a repetition rate of 500 kHz and modulate the signal pulses independently and randomly with zero-centered Gaussian distributions in phase space. In order to accurately estimate the slow phase drifts of the signal and phase-reference (LO) fields in real-time, Alice and Bob periodically insert some phase-calibration pulses into the signal pulses. Finally, the signal and phase-reference (LO) fields are time and polarization multiplexed, and sent to Charlie through SMF-28 fiber spools.

At receiver's site, a 90-deg optical hybrid was used to perform heterodyne detection and obtain the amplitude and phase quadrature of the phase-reference pulses to estimate the fast phase shift for each signal pulse. The fast phase shift consists of residual phase noise after frequency-locking of two independent

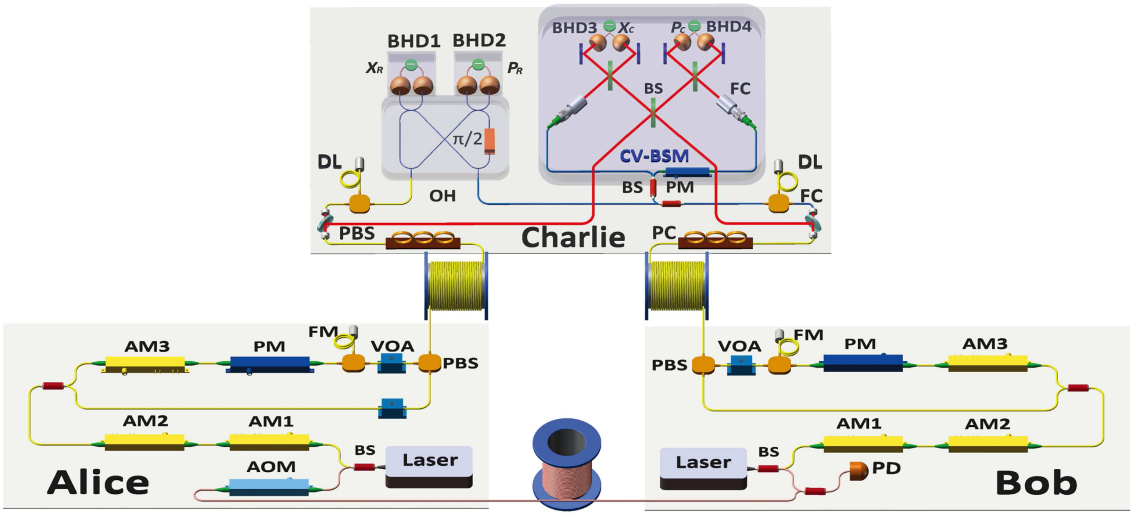

Figure 7 (Color online) Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over long distance optical fiber [90] Copyright 2022 Optica Publishing Group.

lasers, the phase noise arising from the finite laser linewidth, and independent transmission fiber links. A phase modulator was adopted to apply a compensated phase shift to one of the LO fields in CV-BSM based on the values estimated by the phase-calibration pulses of Alice and Bob in real time, to ensure that the field quadratures measured by dual-homodyne detection were faithfully orthogonal. Besides, to achieve high-efficiency CV-BSM, the signal and LO fields are coupled from optical fibers to free space where high quality free-space optical components with very low losses are used. Two time-domain BHDs with a quantum efficiency of 99% are developed to measure two conjugated quadratures. Considering the insertion loss of the optical components and interference visibility, the total detection efficiency is 97.2%. Finally, both Alice and Bob implement a quadrature remapping, where they rotate their data at hand with the estimated phase-drift information to ensure that the data measured by Charlie to be matched with the data of Alice and Bob. With a reconciliation efficiency of 97%, the distance between Bob (Alice) and Charlie of 0.1 km (5/10 km), the achieved secret key rate is 0.43 (0.19) bits/pulse. When the transmission distance is less than 15 km, the secret key rate of the CV protocol is significantly better than that of its DV counterpart even considering the cryogenic single-photon detectors. The proposed approaches in this work comprise a promising solution for the construction of a high-key rate and low-cost metropolitan CV-MDI-QKD network.

In 2023, a simple and practical CV-MDI-QKD system was reported, which was achieved by using a new relay structure leveraging the concept of a polarization-based 90-degree optical hybrid and digital signal processing (DSP) pipeline for CV-BSM [138], as shown in Figure 8. A 1550 nm continuous-wave laser at Alice with a linewidth of 100 Hz was shared with the relay to implement an asymmetric configuration of the CV-MDI protocol, where the relay and Alice were placed together. Moreover, a portion of Alice's laser was sent to Bob through an independent fiber channel in order to avoid the frequency locking.

In each transmitter, an in-phase and quadrature (IQ) modulator was used to generate the ensemble of coherent states. The DSP techniques consisting of digital pulse shaping and sideband modulation were implemented, simplifying the CV-MDI-QKD system. At the relay, the incoming signal beams from Alice and Bob were overlapped at a fiber-based polarization beamsplitter. Then, the signal was coupled into the free-space polarization-based 90-degree hybrid. Because the LO was prepared in circular polarization by using a quarter wave-plate and the signal was linearly polarized, the amplitude quadrature and phase quadrature can be detected simultaneously. After the relay publicly announced the output of CV-BSM, the quantum signals were recovered using DSP. The relay output was digitally demodulated to the baseband by downconversion and low-pass filtering. Temporal synchronization was achieved by calculating the cross-correlation between the samples transmitted by Alice and Bob and the relay output. Then, the synchronized samples were matched filtered and downsampled to symbols. In order to compensate for the phase drift, both Alice and Bob rotated their data at hand to maximize the cross-correlation. Finally, Alice and Bob performed displacement operations on their own data according to the relay output to correlate their data. Considering the information reconciliation efficiency of 97%, the total detection

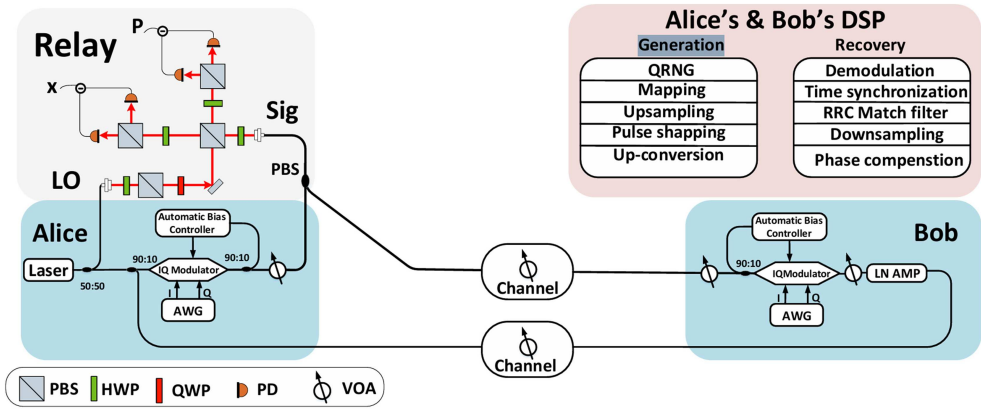

Figure 8 (Color online) CV-MDI-QKD system without frequency and phase locking [138] Copyright 2023 Optica Publishing Group.

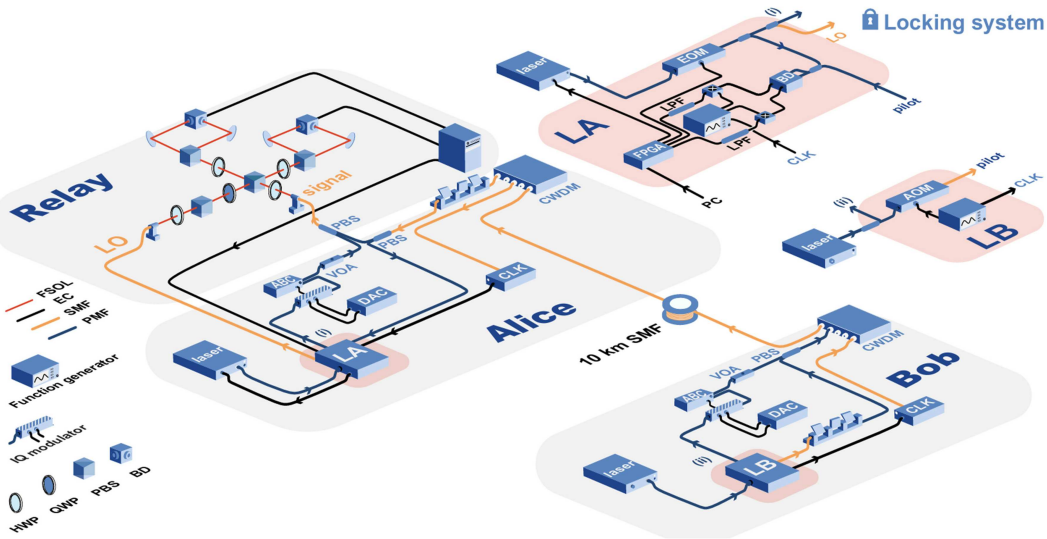

Figure 9 (Color online) Experimental CV-MDI-QKD with finite-size security against collective attacks [139] Copyright 2025 IOP Publishing Ltd.

efficiency of 94%, and Bob's channel loss of 2 dB, a secret key fraction of 0.12 bit per relay use can be achieved.

In 2025, Hajomer et al. [139] further performed the experimental demonstration of CV-MDI-QKD with finite-size security against collective attacks. In this work, a locally generated LO based on a real-time phase locking system was adopted in comparison to their previous work, as shown in Figure 9. An asymmetric configuration of the MDI protocol was implemented, where the relay is co-located with Alice's station. Bob's station and the relay were connected through a single-mode fiber.

To experimentally realize CV-BSM over a long distance, a heterodyne optical locking system was employed to phase-lock the two independent lasers that are used to generate the quantum states at Alice's and Bob's stations. At Bob's station, a part of the laser beam was frequency shifted by 40 MHz using an acousto-optical modulator and then sent to Alice's station, where it interfered with part of Alice's laser beam on a 50:50 BS. The beat signal generated by the interference was detected by a balanced detector. The phase detection was performed by analog I-Q demodulation at 40 MHz. An FPGA was used to generate an error signal, and drive the piezoelectric wavelength modulator inside Alice's laser to compensate for the slow phase fluctuations. An electro-optic phase modulator was adopted to compensate for the fast phase fluctuations. Finally, Alice's stabilized laser was used as the optical source of quantum signal and shared with the relay as LO through a short single-mode fiber channel.

Alice's and Bob's stations were clock synchronized using a synchronizing clock signal. To this end, a 10 MHz master clock generated at Bob's station was converted to an optical signal at a wavelength of 1310 nm using an electrical-to-optical converter circuit. Subsequently, the optical clock was multiplexed

with the quantum signal using a coarse wavelength division multiplexer (CWDM) and transmitted to Alice's station through the same fiber channel. At Alice's station, the optical clock was then converted back to an electrical signal and distributed to the digital-to-analog converter, the locking system and the relay's analog-to-digital converter. Considering the information reconciliation efficiency of 97%, the total detection efficiency of 94%, a block size of 4×10^6, and a failure probability of 10^{-10}, a positive expected secrete key rate of 2.6 Mbit/s was achieved over 10 km fiber link.

The common phase-reference is a crucial challenge for CV-MDI-QKD because of the CV-BSM of two remote independent quantum states. By placing the laser at Charlie's site and using plug-and-play configuration [126], the issues of synchronization between different lasers as well as the generation of LO can be solved. Moreover, the polarization drifts can be compensated automatically since only one laser is needed. Yin et al. [140] proposed a phase self-aligned CV-MDI-QKD scheme. By delicately manipulating the polarization state of the quantum signals, they can transmit along the same fiber link before CV-BSM in the relay. Thus their relative phase fluctuation can be negligible and the phase-reference is self-aligned. This approach can establish a reliable phase reference.

The above schemes effectively solve the phase-reference problem, however, there are still some issues that need to be addressed. The first is the untrusted source problem, which exists in all plug-and-play type QKD systems. For example, the Trojan-horse attack will greatly decrease the key rate along with the increase of the mean photon number of the Trojan-horse mode. The other one is noise photons caused by the strong Rayleigh scattering, which will affect the coherent detection at Charlie.

5 Challenges and future directions

Despite significant progress, practical CV-MDI-QKD still faces technical challenges. In this section, we discuss the main research challenges and future directions of CV-MDI-QKD.

5.1 Performance

At present, the best performance of the CV-MDI-QKD only achieves at an asymmetric configuration and the distribution distance is still limited. Furthermore, it requires high detection efficiency. Although a variety of schemes, including Gaussian and non-Gaussian operations as discussed in Section 3, have been proposed to improve the performance, they are still required to be experimentally verified. In addition, effective data post-selecting is a potential solution to deal with the challenges of limited transmission distance. Post-selection is commonly done for the classical telecommunication protocols and discrete variable QKD protocols to discard noisy data and improve the performance of the protocols. Future research also involves designing new protocols that can operate using heterodyne detection with ordinary detection efficiency and exhibit superior performance in both asymmetric and symmetric configurations.

5.2 Security

A key security assumption in CV-MDI-QKD is that the source should be trusted. The perfect state preparation or fully characterized sources are difficult to realize in practice. Although efforts have been made to prove the security of CV-MDI-QKD when there are imperfections or errors in the source's devices, the practical security issue has not been perfectly solved. Hence, analyzing the practical security and seeking more robust and advanced countermeasures to protect against both known and unknown vulnerabilities are crucial for future research. In addition, as presented in Table 1, the security of many protocols is only proven in the asymptotic regime. There is a growing need to extend the security analysis to finite-size or composable security framework. DM CV-QKD has recently attracted widespread attention due to its simple modulation. However, the present security analyses for DM CV-MDI-QKD depend on the assumption of linear channels. Therefore, it is imperative to establish its security without any assumption about the channels by employing numerical methods.

5.3 Implementation

In current experimental demonstrations, a complex, active optical phase locking system is required to perform CV-BSM of two remote independent quantum states, which is not conducive to the practical application and network expansion of CV-MDI-QKD. Therefore, it is crucial to simplify the experimental implementation. Notice that TF-QKD without active optical phase locking has been reported [141–143].

Moreover, the current system repetition rate of CV-MDI-QKD is relatively low (20 MBaud) and a higher symbol rate over GBaud is expected in the future [77, 79, 144].

5.4 Chip integration

With the rapid development of photonics-integrated technology, the on-chip integrated CV-MDI-QKD system is desired to meet the demands of miniaturization, low power consumption, and low-cost [76, 145] which are crucial for future large-scale applications. The feasibility of using integrated photonics for discrete-variable MDI-QKD has been demonstrated, such as integrated encoding components [146], integrated transmitters [147], and integrated relay server [148]. CV-QKD can utilize the coherent optical communications components and is more suitable for photonic integration. All optical components except the laser source have been integrated onto a silicon photonic chip for CV-QKD [149]. Recently, chip-based laser sources have also been reported [150], and a fully integrated CV-QKD is expected to be realized in the near future. However, the on-chip integrated system also faces some challenges. Potential security loopholes arise due to the specific imperfections of integrated photonic devices [76, 151], and more rigorous practical security analyses or enhanced defense strategies are required in future research. The coupling loss of integrated photonic chips results in relatively low overall detection efficiency of the receiver [79, 152, 153], which hinders CV-MDI-QKD from generating positive secure keys. Therefore, the on-chip integration of the transmitters is feasible whereas the on-chip integration of the measurement devices is still a challenge. To enhance the overall detection efficiency, an advanced low-loss coupling technique is desired.

5.5 Network

CV-MDI-QKD is naturally suitable for a star-type network with an untrusted relay. Such a network architecture is particularly advantageous in metropolitan areas where multiple users need to communicate securely over a shared infrastructure. When combined with QSS and QC, as discussed in Section 3, the security of both QSS and QC is strengthened by effectively eliminating all detector side-channel vulnerabilities. Also, by combining multiplexing techniques, CV-MDI-QKD can be extended to networks serving a large number of users [154–156]. However, due to performance limitations, CV-MDI-QKD networks require that at least one of the QKD users is close to the relay. By properly combining with other quantum protocols and technologies, CV-MDI-QKD will find more novel applications and opportunities in quantum networks [80–82, 157–164].

6 Conclusion

In summary, this review provides a comprehensive overview of the past advancements in the field of CV-MDI-QKD. At present, both the asymptotic and composable security of the protocol have been rigorously proven. The experimental demonstrations over long-distance optical fiber paves the way for the practical deployment of CV-MDI-QKD in real-world scenarios, particularly in metropolitan areas. Although significant progress has been made, challenges still remain for future practical applications. Both the theory and technique breakthroughs are crucial to overcome the obstacles and fully realize the promise of CV-MDI-QKD in practical applications.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant Nos. 62175138, 62205188, 62305198), Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0300703), Fundamental Research Program of Shanxi Province (Grant Nos. 202303021212168, 202403021212343), and Scientific and Technological Innovation Programs of Higher Education Institutions in Shanxi (STIP) (Grant No. 2024L183).

References

1 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, 1984. 175–179
2 Bennett C H, Brassard G, Mermin N D. Quantum cryptography without Bell's theorem. Phys Rev Lett, 1992, 68: 557–559
3 Gisin N, Ribordy G, Tittel W, et al. Quantum cryptography. Rev Mod Phys, 2002, 74: 145–195
4 Braunstein S L, van Loock P. Quantum information with continuous variables. Rev Mod Phys, 2005, 77: 513–577
5 Lo H K, Chau H F. Unconditional security of quantum key distribution over arbitrarily long distances. Science, 1999, 283: 2050–2056
6 Lo H K, Chau H F, Ardehali M. Efficient quantum key distribution scheme and a proof of its unconditional security. J Cryptology, 2005, 18: 133–165
7 Inamori H, Lütkenhaus N, Mayers D. Unconditional security of practical quantum key distribution. Eur Phys J D, 2007, 41: 599–627
8 Lo H K, Curty M, Tamaki K. Secure quantum key distribution. Nat Photon, 2014, 8: 595–604

9 Pirandola S, Andersen U L, Banchi L, et al. Advances in quantum cryptography. Adv Opt Photon, 2020, 12: 1012
10 Xu F, Ma X, Zhang Q, et al. Secure quantum key distribution with realistic devices. Rev Mod Phys, 2020, 92: 025002
11 Portmann C, Renner R. Security in quantum cryptography. Rev Mod Phys, 2022, 94: 025008
12 Weedbrook C, Pirandola S, García-Patrón R, et al. Gaussian quantum information. Rev Mod Phys, 2012, 84: 621–669
13 Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: principle, security and implementations. Entropy, 2015, 17: 6072–6092
14 Li Y M, Wang X Y, Bai Z L, et al. Continuous variable quantum key distribution. Chin Phys B, 2017, 26: 040303
15 Laudenbach F, Pacher C, Fung C-F, et al. Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations. Adv Quantum Tech, 2018, 1: 1800011
16 Guo H, Li Z, Yu S, et al. Toward practical quantum key distribution using telecom components. Fundamental Res, 2021, 1: 96–98
17 Goncharov R, Vorontsova I, Kirichenko D, et al. The rationale for the optimal continuous-variable quantum key distribution protocol. Optics, 2022, 3: 338–351
18 Liu W B, Li C L, Liu Z P, et al. Theoretical development of discrete-modulated continuous-variable quantum key distribution. Front Quantum Sci Technol, 2022, 1: 985276
19 Zhang Y, Bian Y, Li Z, et al. Continuous-variable quantum key distribution system: past, present, and future. Appl Phys Rev, 2024, 11: 011318
20 Grosshans F, Cerf N J, Wenger J, et al. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quantum Inf Comput, 2003, 3: 535–552
21 Grosshans F, van Assche G, Wenger J, et al. Quantum key distribution using Gaussian-modulated coherent states. Nature, 2003, 421: 238–241
22 Navascués M, Grosshans F, Acín A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. Phys Rev Lett, 2006, 97: 190502
23 García-Patrón R, Cerf N J. Continuous-variable quantum key distribution protocols over noisy channels. Phys Rev Lett, 2009, 102: 130501
24 Leverrier A, Grangier P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. Phys Rev Lett, 2009, 102: 180504
25 Leverrier A, Grosshans F, Grangier P. Finite-size analysis of a continuous-variable quantum key distribution. Phys Rev A, 2010, 81: 062343
26 Furrer F, Franz T, Berta M, et al. Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks. Phys Rev Lett, 2012, 109: 100502
27 Ma X C, Sun S H, Jiang M S, et al. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. Phys Rev A, 2013, 87: 052309
28 Gehring T, Händchen V, Duhme J, et al. Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks. Nat Commun, 2015, 6: 8795
29 Leverrier A. Composable security proof for continuous-variable quantum key distribution with coherent states. Phys Rev Lett, 2015, 114: 070501
30 Walk N, Hosseini S, Geng J, et al. Experimental demonstration of Gaussian protocols for one-sided device-independent quantum key distribution. Optica, 2016, 3: 634–642
31 Wang P, Wang X, Li J, et al. Finite-size analysis of unidimensional continuous-variable quantum key distribution under realistic conditions. Opt Express, 2017, 25: 27995–28009
32 Ghorai S, Grangier P, Diamanti E, et al. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. Phys Rev X, 2019, 9: 021059
33 Lin J, Upadhyaya T, Lütkenhaus N. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. Phys Rev X, 2019, 9: 041064
34 Zheng Y, Huang P, Huang A, et al. Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack. Opt Express, 2019, 27: 27369–27384
35 Hosseinidehaj N, Walk N, Ralph T C. Composable finite-size effects in free-space continuous-variable quantum-key-distribution systems. Phys Rev A, 2021, 103: 012605
36 Li C, Qian L, Lo H K. Simple security proofs for continuous variable quantum key distribution with intensity fluctuating sources. npj Quantum Inf, 2021, 7: 150
37 Liao Q, Wang Z, Liu H, et al. Detecting practical quantum attacks for continuous-variable quantum key distribution using density-based spatial clustering of applications with noise. Phys Rev A, 2022, 106: 022607
38 Liu J, Cao Y, Wang P, et al. Impact of homodyne receiver bandwidth and signal modulation patterns on the continuous-variable quantum key distribution. Opt Express, 2022, 30: 27912–27925
39 Luo H, Zhang L, Qin H, et al. Beyond universal attack detection for continuous-variable quantum key distribution via deep learning. Phys Rev A, 2022, 105: 042411
40 Xu Y, Wang T, Liao X, et al. Robust continuous-variable quantum key distribution in the finite-size regime. Photon Res, 2024, 12: 2549–2558
41 Silberhorn C, Ralph T C, Lütkenhaus N, et al. Continuous variable quantum cryptography: beating the 3 dB loss limit. Phys Rev Lett, 2002, 89: 167901
42 Weedbrook C, Lance A M, Bowen W P, et al. Quantum cryptography without switching. Phys Rev Lett, 2004, 93: 170504
43 Su X, Jing J, Pan Q, et al. Dense-coding quantum key distribution based on continuous-variable entanglement. Phys Rev A, 2006, 74: 062305
44 Lodewyck J, Bloch M, García-Patrón R, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. Phys Rev A, 2007, 76: 042305
45 Madsen L S, Usenko V C, Lassen M, et al. Continuous variable quantum key distribution with modulated entangled states. Nat Commun, 2012, 3: 1083
46 Jouguet P, Kunz-Jacques S, Leverrier A, et al. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat Photon, 2013, 7: 378–381
47 Bai Z L, Wang X Y, Yang S S, et al. High-efficiency Gaussian key reconciliation in continuous variable quantum key distribution. Sci China-Phys Mech Astron, 2015, 59: 614201
48 Huang D, Lin D, Wang C, et al. Continuous-variable quantum key distribution with 1 Mbps secure key rate. Opt Express, 2015, 23: 17511–17519
49 Liu W, Huang P, Peng J, et al. Integrating machine learning to achieve an automatic parameter prediction for practical continuous-variable quantum key distribution. Phys Rev A, 2018, 97: 022316
50 Wang N, Du S, Liu W, et al. Long-distance continuous-variable quantum key distribution with entangled states. Phys Rev Appl, 2018, 10: 064028
51 Wang T, Huang P, Zhou Y, et al. High key rate continuous-variable quantum key distribution with a real local oscillator. Opt Express, 2018, 26: 2794–2806
52 Zhang Y, Li Z, Chen Z, et al. Continuous-variable QKD over 50 km commercial fiber. Quantum Sci Technol, 2019, 4: 035006

53 Kish S P, Villaseñor E, Malaney R, et al. Feasibility assessment for practical continuous variable quantum key distribution over the satellite-to-Earth channel. Quantum Eng, 2020, 2: e50
54 Yang S S, Lu Z G, Li Y M. High-speed post-processing in continuous-variable quantum key distribution based on FPGA implementation. J Lightwave Technol, 2020, 38: 3935–3941
55 Zhang Y, Chen Z, Pirandola S, et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. Phys Rev Lett, 2020, 125: 010502
56 Dequal D, Vidarte L T, Rodriguez V R, et al. Feasibility of satellite-to-ground continuous-variable quantum key distribution. npj Quantum Inf, 2021, 7: 3
57 Jeong S, Jung H, Ha J. Rate-compatible multi-edge type low-density parity-check code ensembles for continuous-variable quantum key distribution systems. npj Quantum Inf, 2022, 8: 6
58 Pi Y, Wang H, Pan Y, et al. Sub-Mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber. Opt Lett, 2023, 48: 1766–1769
59 Yang S, Yan Z, Yang H, et al. Information reconciliation of continuous-variables quantum key distribution: principles, implementations and applications. EPJ Quantum Technol, 2023, 10: 40
60 Wang T, Huang P, Li L, et al. High key rate continuous-variable quantum key distribution using telecom optical components. New J Phys, 2024, 26: 023002
61 Hajomer A A E, Derkach I, Jain N, et al. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator. Sci Adv, 2024, 10: eadi9474
62 Su X, Wang W, Wang Y, et al. Continuous variable quantum key distribution based on optical entangled states without signal modulation. Europhys Lett, 2009, 87: 20005
63 Fossier S, Diamanti E, Debuisschert T, et al. Field test of a continuous-variable quantum key distribution prototype. New J Phys, 2009, 11: 045023
64 Wang X Y, Bai Z L, Wang S F, et al. Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise. Chin Phys Lett, 2013, 30: 010305
65 Weedbrook C. Continuous-variable quantum key distribution with entanglement in the middle. Phys Rev A, 2013, 87: 022308
66 Qi B, Lougovski P, Pooser R, et al. Generating the local oscillator "Locally" in continuous-variable quantum key distribution based on coherent detection. Phys Rev X, 2015, 5: 041009
67 Soh D B S, Brif C, Coles P J, et al. Self-referenced continuous-variable quantum key distribution protocol. Phys Rev X, 2015, 5: 041010
68 Usenko V C, Grosshans F. Unidimensional continuous-variable quantum key distribution. Phys Rev A, 2015, 92: 062337
69 Huang D, Huang P, Li H, et al. Field demonstration of a continuous-variable quantum key distribution network. Opt Lett, 2016, 41: 3511–3514
70 Wang X, Liu W, Wang P, et al. Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution. Phys Rev A, 2017, 95: 062330
71 Karinou F, Brunner H H, Fung C H F, et al. Toward the integration of CV quantum key distribution in deployed optical networks. IEEE Photon Technol Lett, 2018, 30: 650–653
72 Qi B, Gunther H, Evans P G, et al. Experimental passive-state preparation for continuous-variable quantum communications. Phys Rev Appl, 2020, 13: 054065
73 Milovancev D, Vokic N, Laudenbach F, et al. High rate CV-QKD secured mobile WDM fronthaul for dense 5G radio networks. J Lightwave Technol, 2021, 39: 3445–3457
74 Chen Z, Wang X, Yu S, et al. Continuous-mode quantum key distribution with digital signal processing. npj Quantum Inf, 2023, 9: 28
75 Du S, Wang P, Liu J, et al. Continuous variable quantum key distribution with a shared partially characterized entangled source. Photon Res, 2023, 11: 463–475
76 Luo W, Cao L, Shi Y, et al. Recent progress in quantum photonic chips for quantum communication and internet. Light Sci Appl, 2023, 12: 175
77 Tian Y, Zhang Y, Liu S, et al. High-performance long-distance discrete-modulation continuous-variable quantum key distribution. Opt Lett, 2023, 48: 2953–2956
78 Wang P, Zhang Y, Lu Z, et al. Discrete-modulation continuous-variable quantum key distribution with a high key rate. New J Phys, 2023, 25: 023019
79 Hajomer A A E, Bruynsteen C, Derkach I, et al. Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver. Optica, 2024, 11: 1197–1204
80 Wang X, Chen Z, Li Z, et al. Experimental upstream transmission of continuous variable quantum key distribution access network. Opt Lett, 2023, 48: 3327–3330
81 Hajomer A A E, Derkach I, Filip R, et al. Continuous-variable quantum passive optical network. Light Sci Appl, 2024, 13: 291
82 Ji F, Huang P, Wang T, et al. Gbps key rate passive-state-preparation continuous-variable quantum key distribution within an access-network area. Photon Res, 2024, 12: 1485–1493
83 Acín A, Brunner N, Gisin N, et al. Device-independent security of quantum cryptography against collective attacks. Phys Rev Lett, 2007, 98: 230501
84 Zapatero V, van Leent T, Arnon-Friedman R, et al. Advances in device-independent quantum key distribution. npj Quantum Inf, 2023, 9: 10
85 Braunstein S L, Pirandola S. Side-channel-free quantum key distribution. Phys Rev Lett, 2012, 108: 130502
86 Lo H K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503
87 Pirandola S, Ottaviani C, Spedalieri G, et al. High-rate measurement-device-independent quantum cryptography. Nat Photon, 2015, 9: 397–402
88 Li Z, Zhang Y C, Xu F, et al. Continuous-variable measurement-device-independent quantum key distribution. Phys Rev A, 2014, 89: 052301
89 Ma X C, Sun S H, Jiang M S, et al. Gaussian-modulated coherent-state measurement-device-independent quantum key distribution. Phys Rev A, 2014, 89: 042335
90 Tian Y, Wang P, Liu J, et al. Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber. Optica, 2022, 9: 492–500
91 Lupo C, Ottaviani C, Papanastasiou P, et al. Parameter estimation with almost no public communication for continuous-variable quantum key distribution. Phys Rev Lett, 2018, 120: 220505
92 Pirandola S. Entanglement reactivation in separable environments. New J Phys, 2013, 15: 113046
93 Ottaviani C, Spedalieri G, Braunstein S L, et al. Continuous-variable quantum cryptography with an untrusted relay: detailed security analysis of the symmetric configuration. Phys Rev A, 2015, 91: 022320
94 Ottaviani C, Spedalieri G, Braunstein S L, et al. CV-MDI-QKD with coherent state: beyond one-mode Gaussian attacks. IOPSciNotes, 2020, 1: 025202
95 Gaetana S, Carlo O, Samuel L B, et al. Quantum cryptography with an ideal local relay. In: Proceedings of SPIE, 2015
96 Papanastasiou P, Ottaviani C, Pirandola S. Finite-size analysis of measurement-device-independent quantum cryptography

with continuous variables. Phys Rev A, 2017, 96: 042332
97 Zhang X, Zhang Y, Zhao Y, et al. Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution. Phys Rev A, 2017, 96: 042334
98 Lupo C, Ottaviani C, Papanastasiou P, et al. Continuous-variable measurement-device-independent quantum key distribution: composable security against coherent attacks. Phys Rev A, 2018, 97: 052327
99 Leverrier A. Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction. Phys Rev Lett, 2017, 118: 200501
100 Bai D, Huang P, Zhu Y, et al. Unidimensional continuous-variable measurement-device-independent quantum key distribution. Quantum Inf Process, 2019, 19: 53
101 Ma H X, Huang P, Bai D Y, et al. Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation. Phys Rev A, 2019, 99: 022322
102 Wu C X D, Huang C D, Huang C P, et al. Discrete modulation continuous-variable measurement-device-independent quantum key distribution scheme based on realistic detector compensation. Acta Phys Sin, 2022, 71: 240304
103 Bai D, Huang P, Ma H, et al. Passive-state preparation in continuous-variable measurement-device-independent quantum key distribution. J Phys B-At Mol Opt Phys, 2019, 52: 135502
104 Wu X, Wang Y, Li S, et al. Security analysis of passive measurement-device-independent continuous-variable quantum key distribution with almost no public communication. Quantum Inf Process, 2019, 18: 372
105 Zhang Y C, Li Z, Yu S, et al. Continuous-variable measurement-device-independent quantum key distribution using squeezed states. Phys Rev A, 2014, 90: 052325
106 Chen Z, Zhang Y, Wang G, et al. Composable security analysis of continuous-variable measurement-device-independent quantum key distribution with squeezed states for coherent attacks. Phys Rev A, 2018, 98: 012314
107 Wang P, Wang X, Li Y. Continuous-variable measurement-device-independent quantum key distribution using modulated squeezed states and optical amplifiers. Phys Rev A, 2019, 99: 042309
108 Ding C, Wang Y, Zhang W, et al. Multi-mode Gaussian modulated continuous-variable measurement-device-independent quantum key distribution. Int J Theor Phys, 2021, 60: 1361–1373
109 Huang L, Zhang Y, Yu S. Continuous-variable measurement-device-independent quantum key distribution with one-time shot-noise unit calibration. Chin Phys Lett, 2021, 38: 040301
110 Guo Y, Zhao W, Li F, et al. Improving continuous-variable measurement-device-independent multipartite quantum communication with optical amplifiers. Commun Theor Phys, 2017, 68: 191
111 Ma H X, Huang P, Bai D Y, et al. Continuous-variable measurement-device-independent quantum key distribution with photon subtraction. Phys Rev A, 2018, 97: 042329
112 Zhao Y, Zhang Y, Xu B, et al. Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction. Phys Rev A, 2018, 97: 042328
113 Djordjevic I B. On the photon subtraction-based measurement-device-independent CV-QKD protocols. IEEE Access, 2019, 7: 147399
114 Yu C, Li Y, Ding J, et al. Photon subtraction-based continuous-variable measurement-device-independent quantum key distribution with discrete modulation over a fiber-to-water channel. Commun Theor Phys, 2022, 74: 035104
115 Ye W, Zhong H, Wu X, et al. Continuous-variable measurement-device-independent quantum key distribution via quantum catalysis. Quantum Inf Process, 2020, 19: 346
116 Ye W, Guo Y, Zhang H, et al. Enhancing discrete-modulated continuous-variable measurement-device-independent quantum key distribution via quantum catalysis. J Phys B-At Mol Opt Phys, 2021, 54: 045501
117 Bilal Khan M, Waseem M, Irfan M, et al. Zero-photon catalysis based eight-state discrete modulated measurement-device-independent continuous-variable quantum key distribution. J Opt Soc Am B, 2023, 40: 763–772
118 Jafari K, Golshani M, Bahrampour A. Discrete-modulation measurement-device-independent continuous-variable quantum key distribution with a quantum scissor: exact non-Gaussian calculation. Opt Express, 2022, 30: 11400–11423
119 Wilkinson K N, Papanastasiou P, Ottaviani C, et al. Long-distance continuous-variable measurement-device-independent quantum key distribution with postselection. Phys Rev Res, 2020, 2: 033424
120 Papanastasiou P, Mountogiannakis A G, Pirandola S. Composable security of CV-MDI-QKD with secret key rate and data processing. Sci Rep, 2023, 13: 11636
121 Huang C, Wang X. CV MDI-QKD with noisy coherent states. Opt Quant Electron, 2016, 48: 430
122 Ma H X, Huang P, Wang T, et al. Security of continuous-variable measurement-device-independent quantum key distribution with imperfect state preparation. Phys Lett A, 2019, 383: 126005
123 Wang P, Wang X, Li Y. Continuous-variable measurement-device-independent quantum key distribution with source-intensity errors. Phys Rev A, 2020, 102: 022609
124 Huang L, Wang X, Chen Z, et al. Countermeasure for negative impact of a practical source in continuous-variable measurement-device-independent quantum key distribution. Phys Rev Appl, 2023, 19: 014023
125 Zhou J, Feng Y, Shi J, et al. Plug-and-play continuous variable measurement-device-independent quantum key distribution. Annalen der Physik, 2023, 535: 2200614
126 Liao Q, Wang Y, Huang D, et al. Dual-phase-modulated plug-and-play measurement-device-independent continuous-variable quantum key distribution. Opt Express, 2018, 26: 19907–19920
127 Zhao W, Shi R, Shi J, et al. Phase-noise estimation using Bayesian inference for discretely modulated measurement-device-independent continuous-variable quantum key distribution. Phys Rev A, 2020, 102: 022621
128 Zheng Y, Shi H, Pan W, et al. Security analysis of continuous-variable measurement-device-independent quantum key distribution systems in complex communication environments. Entropy, 2022, 24: 127
129 Zhang S J, Xiao C, Zhou C, et al. Performance analysis of continuous-variable measurementdevice-independent quantum key distribution under diverse weather conditions*. Chin Phys B, 2020, 29: 020301
130 Wang Y, Zou S, Mao Y, et al. Improving underwater continuous-variable measurement-device-independent quantum key distribution via zero-photon catalysis. Entropy, 2020, 22: 571
131 Peng Q, Guo Y, Liao Q, et al. Satellite-to-submarine quantum communication based on measurement-device-independent continuous-variable quantum key distribution. Quantum Inf Process, 2022, 21: 61
132 Ghalaii M, Pirandola S. Continuous-variable measurement-device-independent quantum key distribution in free-space channels. Phys Rev A, 2023, 108: 042621
133 Wu Y, Zhou J, Gong X, et al. Continuous-variable measurement-device-independent multipartite quantum communication. Phys Rev A, 2016, 93: 022325
134 Zhao R, Zhou J, Shi R, et al. Continuous-variable measurement-device-independent multipartite quantum communication via a fast-fading channel. Phys Rev A, 2025, 111: 012613
135 Liao Q, Huang L, Fei Z, et al. Measurement-device-independent continuous-variable quantum secret sharing. Adv Quantum Tech, 2025. doi:10.1002/qute.202400505
136 Ottaviani C, Lupo C, Laurenza R, et al. Modular network for high-rate quantum conferencing. Commun Phys, 2019, 2: 118
137 Fletcher A I, Pirandola S. Continuous variable measurement device independent quantum conferencing with postselection. Sci Rep, 2022, 12: 17329

138 Hajomer A A E, Nguyen H Q, Andersen U L, et al. High-rate continuous-variable measurement-device-independent quantum key distribution. In: Proceedings of Optical Fiber Communications Conference and Exhibition (OFC), San Diego, 2023. 1–3
139 Hajomer A A E, Andersen U L, Gehring T. High-rate continuous-variable measurement device-independent quantum key distribution with finite-size security. Quantum Sci Technol, 2025, 10: 025032
140 Yin H L, Zhu W, Fu Y. Phase self-aligned continuous-variable measurement-device-independent quantum key distribution. Sci Rep, 2019, 9: 49
141 Zhou L, Lin J, Jing Y, et al. Twin-field quantum key distribution without optical frequency dissemination. Nat Commun, 2023, 14: 928
142 Li W, Zhang L, Lu Y, et al. Twin-field quantum key distribution without phase locking. Phys Rev Lett, 2023, 130: 250802
143 Chen J P, Zhou F, Zhang C, et al. Twin-field quantum key distribution with local frequency reference. Phys Rev Lett, 2024, 132: 260802
144 Wang H, Li Y, Pi Y, et al. Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. Commun Phys, 2022, 5: 162
145 Wang J, Sciarrino F, Laing A, et al. Integrated photonic quantum technologies. Nat Photonics, 2020, 14: 273–284
146 Wei K, Li W, Tan H, et al. High-speed measurement-device-independent quantum key distribution with integrated silicon photonics. Phys Rev X, 2020, 10: 031030
147 Semenenko H, Sibson P, Hart A, et al. Chip-based measurement-device-independent quantum key distribution. Optica, 2020, 7: 238–242
148 Zheng X, Zhang P, Ge R, et al. Heterogeneously integrated, superconducting silicon-photonic platform for measurement-device-independent quantum key distribution. Adv Photon, 2021, 3: 055002
149 Zhang G, Haw J Y, Cai H, et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. Nat Photon, 2019, 13: 839–842
150 Li L, Wang T, Li X, et al. Continuous-variable quantum key distribution with on-chip light sources. Photon Res, 2023, 11: 504–516
151 Li L, Huang P, Wang T, et al. Practical security of a chip-based continuous-variable quantum-key-distribution system. Phys Rev A, 2021, 103: 032611
152 Piétri Y, Trigo Vidarte L, Schiavon M, et al. Experimental demonstration of continuous-variable quantum key distribution with a silicon photonics integrated receiver. Optica Quantum, 2024, 2: 428–437
153 Bian Y, Pan Y, Xu X, et al. Continuous-variable quantum key distribution over 28.6 km fiber with an integrated silicon photonic receiver chip. Appl Phys Lett, 2024, 124: 174001
154 Park C H, Woo M K, Park B K, et al. 2×N twin-field quantum key distribution network configuration based on polarization, wavelength, and time division multiplexing. npj Quantum Inf, 2022, 8: 48
155 Xu Y, Wang T, Zhao H, et al. Round-trip multi-band quantum access network. Photon Res, 2023, 11: 1449–1464
156 Liu S, Tian Y, Zhang Y, et al. Integrated quantum communication network and vibration sensing in optical fibers. Optica, 2024, 11: 1762–1772
157 Fröhlich B, Dynes J F, Lucamarini M, et al. A quantum access network. Nature, 2013, 501: 69–72
158 Wang Y, Tian C X, Su Q, et al. Measurement-device-independent quantum secret sharing and quantum conference based on Gaussian cluster state. Sci China Inf Sci, 2019, 62: 072501
159 Su X L, Wang M H, Yan Z H, et al. Quantum network based on non-classical light. Sci China Inf Sci, 2020, 63: 180503
160 Ren S Y, Wang Y, Su X L. Hybrid quantum key distribution network. Sci China Inf Sci, 2022, 65: 200502
161 Liu S, Lu Z, Wang P, et al. Experimental demonstration of multiparty quantum secret sharing and conference key agreement. npj Quantum Inf, 2023, 9: 92
162 Fang K, Zhao J T, Li X F, et al. Quantum NETwork: from theory to practice. Sci China Inf Sci, 2023, 66: 180509
163 Jain N, Chin H M, Hajomer A A E, et al. Future proofing network encryption technology with continuous-variable quantum key distribution. Opt Express, 2024, 32: 43607–43620
164 Du Y, Li B H, Hua X, et al. Chip-integrated quantum signature network over 200 km. Light Sci Appl, 2025, 14: 108