Continuous-variable quantum key distribution system: A review and perspective

Yichen Zhang,[1] Yiming Bian,[1] Zhengyu Li,[2, a)] Song Yu,[1, b)] and Hong Guo[3, c)]
[1)]*State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China.*
[2)]*Central Research Institute, 2012 Labs, Huawei Technologies Co., Ltd, Shenzhen 518129, Guangdong, China.*
[3)]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China.*

(Dated: 15 January 2024)

ABSTRACT

Quantum key distribution provides secure keys with information-theoretic security ensured by the principle of quantum mechanics. The continuous-variable version of quantum key distribution using coherent states offers the advantages of its compatibility with telecom industry, e.g., using commercial laser and homodyne detector, is now going through a booming period. In this review article, we describe the principle of continuous-variable quantum key distribution system, focus on protocols based on coherent states, whose systems are gradually moving from proof-of-principle lab demonstrations to in-field implementations and technological prototypes. We start by reviewing the theoretical protocols and the current security status of these protocols. Then, we discuss the system structure, the key module, and the mainstream system implementations. The advanced progress for future applications are discussed, including the digital techniques, system on chip and point-to-multipoint system. Finally, we discuss the practical security of the system and conclude with promising perspectives in this research field.

CONTENTS

[a)]Electronic mail: lizhengyu2@huawei.com
[b)]Electronic mail: yusong@bupt.edu.cn
[c)]Electronic mail: hongguo@pku.edu.cn

I. INTRODUCTION

Since 1984, quantum key distribution (QKD)[1] has ushered in an era of secure communications using quantum methods by providing information-theoretic secure key distribution[2–8]. The combination of this method with one-time-pad encryption provides the ultimate protection for the transmission of confidential messages. In general, for simplified implementations, QKD protocols are formulated in a prepare-and-measure fashion, where classical information is encoded in non-orthogonal quantum states: these are randomly prepared by Alice (the sender) and then transmitted to Bob (the receiver) through an insecure quantum channel. At the output of the channel, the states are measured by Bob to retrieve the encoded classical information. The quantum no-cloning theorem dictates that an unknown quantum state cannot be reliably cloned[9], ensuring long-term security based on physical principles[10] against unlimited computational power.

So far, various QKD protocols with discrete variables have been proposed to support the long-distance and practical-secure system implementations[1,2,11–28], including the decoy states experiments[29–42], the measurement-device-independent (MDI) experiments[43–59], the twin-field experiments[60–69], the system on chip[59,70–75], and so on[76–86]. Specifically, the twin-field QKD with a 3-station scheme has significantly promoted the development of the long-distance QKD, where the total distance can break the PLOB bound[87]. These achievements have resulted in the long-haul point-to-point connection up to 1000 km[69], high-speed metropolitan system[88–92], and field deployed QKD network[93–97], even with satellite-to-ground links[98–103]. Furthermore, it is worth noting a distinct category of protocols where information is encoded on the quadrature of light that is continuous-variable. The use of such continuous-variable quantum information carriers, instead of qubits, constitutes a potent and alternative approach for QKD[104–112] and more broadly, for quantum information processing[108,110,113–120].

Continuous-variable QKD (CV-QKD) using coherent states[106,107] is now currently experiencing a booming period due to its compatibility with telecom industry, e.g., using commercial continuous-wave laser and coherent receiver. This potential has led to significant advancements in CV-QKD, including protocol design, security analysis, and system implementation (See Fig. 1). The security of CV-QKD protocol using Gaussian-modulated coherent states was initially proved under asymptotic conditions[121,122], and later extended to the finite-size regime with universal composability against collective attack[123], and general attacks by exploiting Gaussian de Finetti theorem[124]. In addition to continuous modulation, the discrete modulation of coherent states has also been well investigated[125–129]. Along with the improving security proof, the implementation of CV-QKD system has progressed from the initial proof-of-principle demonstration to the second stage with swift advancements in high performance and system robustness. Currently, it has entered the third stage where a modern architecture is evolving with the benefit of being fully compatible with coherent communication.

During the initial phases of the CV-QKD system, the primary challenge was to overcome the 3 dB limit, which was solved by the reverse reconciliation[130]. Subsequently, the CV-QKD system progressed towards allowing long-distance transmission to facilitate two-user interconnection across a wide range without a trusted relay. Developments of the reconciliation resulted in enhanced error correction capability even with an extremely low signal-to-noise ratio (SNR)[131], which played a significant role in the long-distance system covering a distance from 25 km[132] up to 80 km[133]. At this stage, both the quantum signal and local oscillator (LO) are generated by the same laser of transmitter and co-propagated in the quantum channel, known as the in-line LO system, which contributes to the suppression of phase noise when the quantum and LO interfere for coherent detection. However, a significant challenge towards achieving long-distance and stable transmission is to reduce crosstalk between the strong LO and the weak quantum signal. The most effective current approach is using pulsed signals with high extinction ratio, then combining polarization multiplexing and time-division multiplexing[133–139]. This methodology has resulted in the longest lab experiment over 202 km[139], the longest field test of 50 km[137], the long-term test of a 3-node CV-QKD network in Qingdao, China[140], and the first chip-based system[138].

In 2015, an alternative scheme was proposed, which relaxed the requirement of the extremely high isolation by generating LO inside the receiver and using a pilot assisted phase recovery to suppress the phase noise introduced by the different laser source[141,142]. As the pilot signal has significantly lower power compared to the LO, the high-extinction pulse generation for time division multiplexing is no longer required. Instead, frequency-division multiplexing is widely used, which simplifies the signal generation, and sometimes can be combined with polarization multiplexing for better isolation. For higher secret key rate and better phase recovery, the repetition rate of the system is gradually enhanced, where digital techniques in classical optical communication systems, such as pulse shaping and matched filter, are introduced to overcome the limited bandwidth of devices. Further, more and more digital algorithms for a CV-QKD system are developed, including the de-multiplexing, impairment compensation, synchronization etc., which then drive the innovation in system architecture. To date, the local LO scheme contributes to the high-speed system with the repetition rate of 5 GBaud, resulting in 190 Mbps secret key rate at 5 km[143], as well as a flexible network deployment, which has been demonstrated by the software-defined CV-QKD network in Madrid, Spain[144].

The use of digital techniques from classical communications has significantly advanced the development of CV-QKD systems, allowing for the completion of most operations in

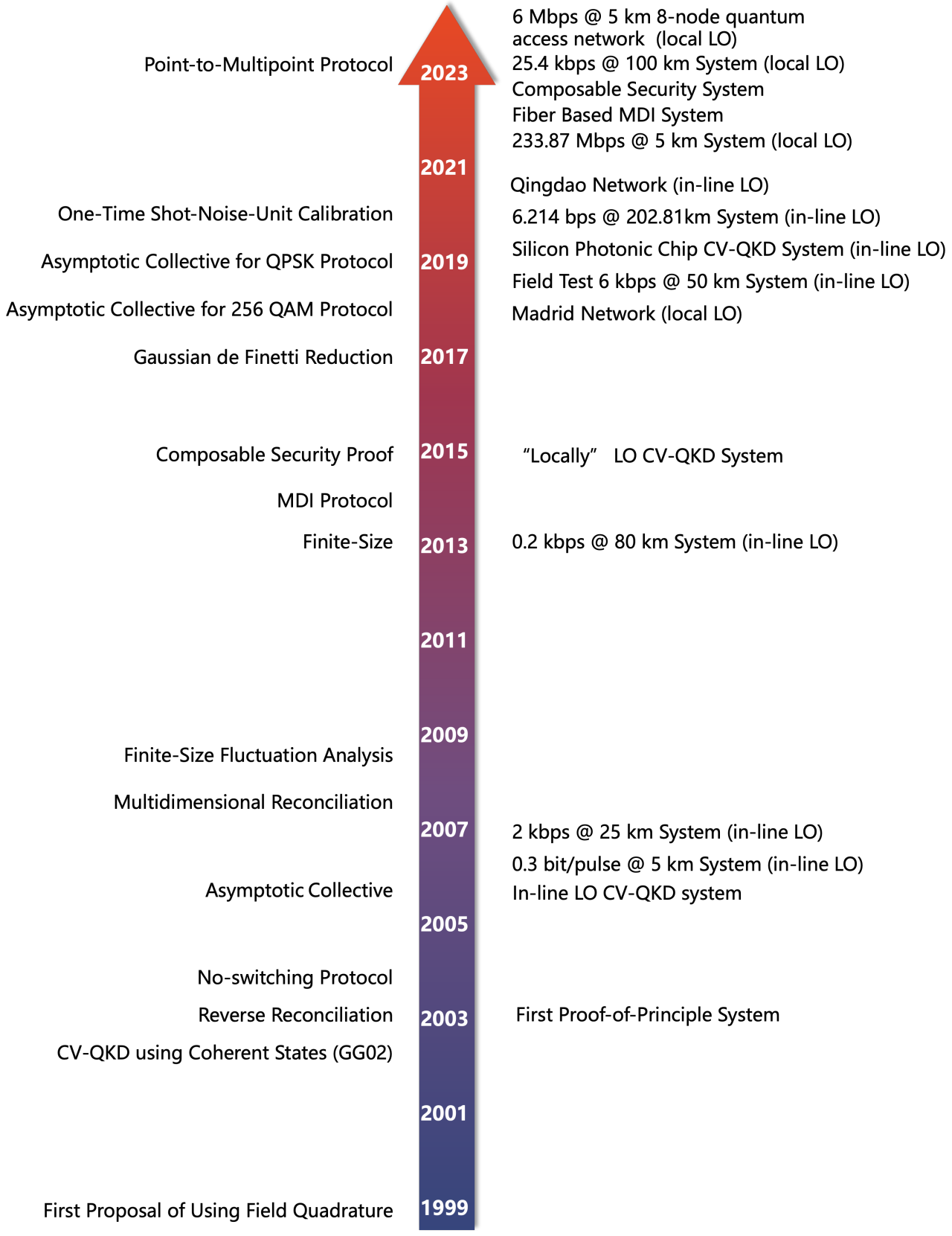

FIG. 1. Selected key developments in CV-QKD. On both sides of the arrow are theoretical research progress (left) and experimental research progress (right). Here, the theroetical research progress includes the protocol proposal, security proof and optimization of protocol steps. The experimental progress includes the development of in-line LO and local LO systems.

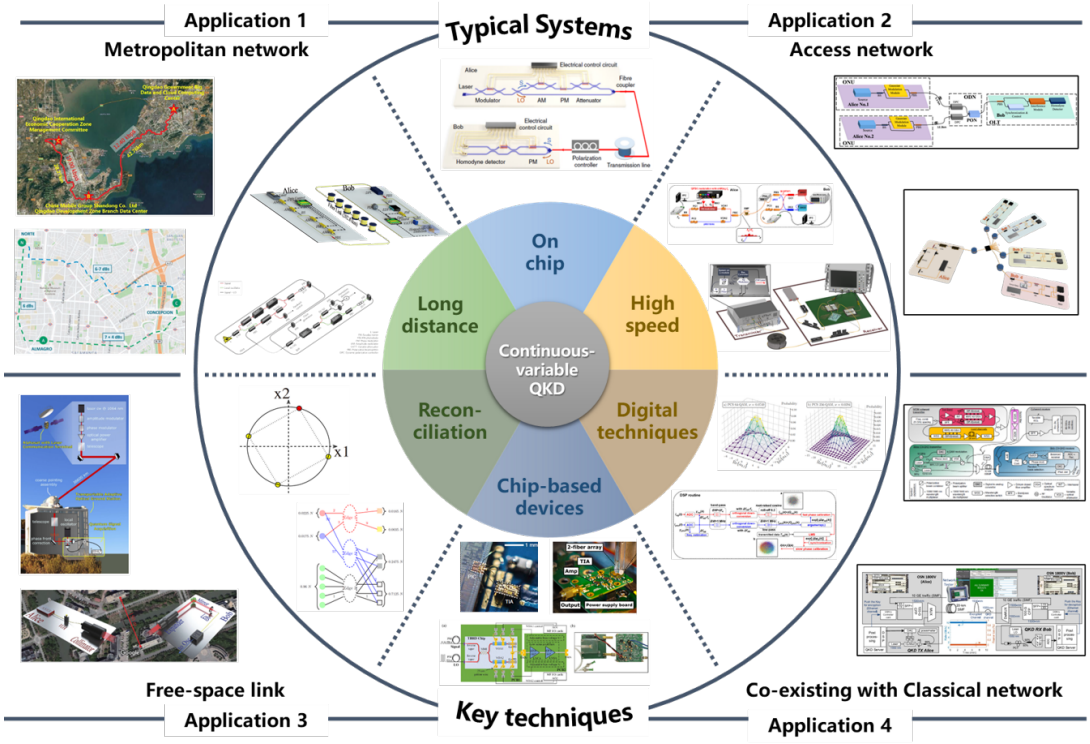

FIG. 2. The overview of the CV-QKD system, including the typical systems, key techniques and the appliactions. Here we mainly show the long-distance, chip-based and high-speed system, as well as the key techniques including the reconciliation, chip-based devices and digital techniques.

digital domain, and resulting in a system compatible with classical optical communication in the aspect of both architectures and algorithms[145]. Meanwhile, the advanced progresses of the homodyne detector integrated on chip have shown the potential of a compact system with high-performance, where the baud rate of the system using chip-based homodyne detector can reach 10 GBaud[146]. Additionally, the implementation of a high-rate downstream point-to-multipoint CV-QKD network can facilitate large-scale deployments, enabling multi-user access with low-cost devices and simplified network structures[147].

An overview of the typical CV-QKD systems, key techniques and application scenarios is presented in Fig. 2. These typical system achievements, supported by the advanced reconciliation, digital signal processing (DSP) and chip-based devices, have proved that the CV-QKD system is suitable for the metropolitan network and access network, as well as the free space communication and co-existing with the classical optical networks. With these advanced techniques, a large-scale cost-effective QKD network supported by advanced CV-QKD systems is on the way.

In all this panorama, the present review aims at providing an overview of the most important results and the most recent advances in the field of CV-QKD system. After a brief introduction of the general notions, we review the main CV-QKD protocols and security analysis in Sec. II. The system structure and key modules are reviewed in Sec. III, and the typical currently-achievable implementations are detailed in Sec. IV, including the in-line LO systems, local LO systems, systems co-existing with classical networks, and so on. We then discuss the advanced progress for future applications, such as digital continuous-variable system and point-to-multipoint network, in Sec. V. Finally, we will discuss the practical security of the system in Sec. VI and conclude with promising perspectives in this research field in Sec. VII.

II. CV-QKD PROTOCOL AND SECURITY PROOF

The CV-QKD system relies on a protocol to establish the system's operating procedures, where the security of the protocol is determined by security proof. In this section, we introduce the basic notions, the CV-QKD protocols and security analysis.

A. Basic notions of continuous-variable systems

A continuous-variable system is a typical infinite dimensional quantum system. Suppose that a CV system consists of a sequence of n modes in the Hilbert space $\mathscr{H} = \otimes_{i=1}^{n}\mathscr{H}_i$, there are n pairs of annihilation and creation operators $\left\{\hat{a}_i, \hat{a}_i^{\dagger}\right\}$ with $i = 1, 2, ..., n$, which satisfies

$$\begin{aligned}\left[\hat{a}_i,\hat{a}_k^\dagger\right]&=\delta_{ik},\\ [\hat{a}_i,\hat{a}_k]&=0,\\ \left[\hat{a}_i^\dagger,\hat{a}_k^\dagger\right]&=0.\end{aligned}\tag{1}$$

For each mode, we can correspondingly define the operators $\hat{x}$ and $\hat{p}$ as

$$\hat{x}=\hat{a}^\dagger+\hat{a},\hat{p}=i(\hat{a}^\dagger-\hat{a}),\tag{2}$$

which are so-called quadratures of electromagnetic field, and the quadratures can be described by a n-mode vector $\hat{r}=(\hat{x}_1,\hat{p}_1,\hat{x}_2,\hat{p}_2,...,\hat{x}_n,\hat{p}_n)^T$. Using the standard bosonic canonical commutation relations as well as Eq. (1) and (2) we can easily get

$$\begin{aligned}[\hat{x}_i,\hat{x}_k]&=0,\\ [\hat{p}_i,\hat{p}_k]&=0,\\ [\hat{x}_i,\hat{p}_k]&=2i\delta_{ik},\end{aligned}\tag{3}$$

which gives the well-known Heisenberg uncertainty relation

$$\Delta\hat{x}\Delta\hat{p}\geq|\langle[x,p]\rangle|=1.\tag{4}$$

Here, $\Delta\hat{A}=(\langle\hat{A}^2\rangle-\langle\hat{A}\rangle^2)^{1/2}$. Now it is straightforward to derive the following relation

$$[\hat{r}_i,\hat{r}_k]=2i\Omega_{ik},\tag{5}$$

where $\Omega=\bigoplus_{i=1}^{n}\begin{bmatrix}0&1\\-1&0\end{bmatrix}$, and Ω_{ik} is the generic element of Ω.

Gaussian states are the states that their characteristic function is a Gaussian function in phase space. Its displacement operator can be defined as $d=\langle\hat{r}\rangle=Tr[\rho\hat{r}]$, while the positive-semidefinite symmetric covariance matrix is defined as

$$\gamma_{ij}=\frac{1}{2}Tr[\rho\{(\hat{r}_i-d_i),(\hat{r}_j-d_j)\}],\tag{6}$$

where $\{\}$ denotes the anticommutator, and ρ is a general density operator. Since a state is Gaussian if its Wigner function is Gaussian, it is completely characterized by the first two statistical moments, the mean value d, and the covariance matrix γ.

Since all physical existed Gaussian states should obey the Heisenberg uncertainty relation, therefore the covariance matrix is generally[148].

$$\gamma+i\Omega\geq 0.\tag{7}$$

The most common single-mode Gaussian states include vacuum state, coherent states and squeezed states. The vacuum state is centered at the origin of the phase space and the covariance matrix is an identity matrix. The coherent states are the displaced vacuum state with non-zero displacement vectors $\mathbf{d}=(d_x,d_p)$. Thus, the covariance matrices of the coherent states are also identity matrices. The squeezed states can be obtained by squeezing coherent states at one of the two quadratures. Suppose the states are squeezed on x quadrature, the conjugate p quadrature is anti-squeezed.

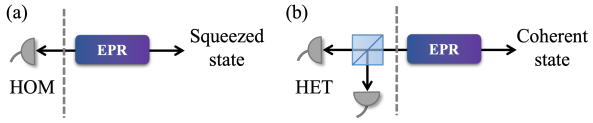

FIG. 3. The preparation of a squeezed (a) or coherent state (b) using homodyne or heterodyne detection on one mode of the EPR state. HOM: homodyne detection, HET: heterodyne detection.

For two-mode Gaussian states, the commonly used states in CV system are two mode squeezed vacuum states, which can also be noted as the Einstein-Podolsky-Rosen (EPR) states in CV system[149], of which the covariance matrix reads

$$\gamma_{EPR}=\begin{bmatrix}cosh\ 2r\ I_2 & sinh\ 2r\ \sigma_z\\ sinh\ 2r\ \sigma_z & cosh\ 2r\ I_2\end{bmatrix}=\begin{bmatrix}V\ I_2 & \sqrt{V^2-1}\ \sigma_z\\ \sqrt{V^2-1}\ \sigma_z & V\ I_2\end{bmatrix},\tag{8}$$

where

$$I_2=\begin{bmatrix}1&0\\0&1\end{bmatrix},\ \sigma_z=\begin{bmatrix}1&0\\0&-1\end{bmatrix},\tag{9}$$

r is the squeezed ratio, and V is called the variance of the EPR state. In particular, performing homodyne detection on one of the modes of an EPR state results in the other mode being projected on a squeezed state, while performing heterodyne detection on one of the modes of an EPR state results in the other mode being projected on a coherent state[150], as shown in Fig. 3.

B. A historical outline of CV-QKD protocols and the current security status

The first CV-QKD protocol was proposed in 1999, using squeezed states to achieve secret key distribution[104]. However, due to the challenges in preparing squeezed states, a protocol of using coherent states and homodyne detection to distribute secret key was proposed in 2002[106], namely the GG02 protocol. Because the coherent states can be easily generated by a laser, this protocol has received an increasing attention in recent years. Subsequently the protocol based on Gaussian modulated coherent states got further developments. The no-switching protocol was reported in 2004[107], in which heterodyne detection instead of homodyne detection was used. In 2009, heterodyne detection was also utilized in the Gaussian modulated squeezed-state protocol and an improvement of performance was found[161].

Although Gaussian modulated CV-QKD protocols have undergone extensive study and development, there remain technical challenges to implementing ideal Gaussian modulation

TABLE I. Current security status of the main one-way CV-QKD protocols.

Protocol	State	Modulation	Measurement	Best Current-Available Security Proof
F. Grosshans et al.[106]	Coherent	Gaussian	Homodyne	Asymptotic Collective[151] Finite-Size Collective[152–154]
C. Weedbrook et al.[107]	Coherent	Gaussian	Heterodyne	Finite-Size[123,124,152–154] $K^{\varepsilon}_{\text{coll}}(N) \approx K^{\text{asympt}}_{\text{coll}}$ for practical N $K^{\varepsilon}(N) = 0$ for practical N[155]
N. J. Cerf et al.[105]	Squeezed	Gaussian	Homodyne	Finite-Size[156,157] $K^{\varepsilon}(N) > 0$ for practical N $\lim_{N\to\infty} K^{\varepsilon}(N) < K^{\text{asympt}}_{\text{coll}}$
A. Leverrier et al.[158]	Coherent	QPSK	Homodyne	Asymptotic Collective with linear assumption [158]
Z. Li et al.[125]	Coherent	QPSK, Arbitrary	Homo/Heterodyne	Asymptotic Collective[125]
S. Ghorai et al.[126]	Coherent	QPSK, Arbitrary[128]	Homo/Heterodyne	Asymptotic Collective[126,128]
J. Lin et al.[127]	Coherent	QPSK	Homo/Heterodyne	Asymptotic Collective[127]
V. Usenko et al.[159]	Coherent	Gaussian 1D	Homodyne	Finite-size Collective[160]
R. García-Patrón et al.[161]	Squeezed	Gaussian	Heterodyne	Asymptotic Collective[161]
R. Filip[162,163]	Thermal	Gaussian	Homo/Heterodyne	Asymptotic Collective[164]
J. Fiurášek et al.[165] N. Walk et al.[166]	Coherent	Gaussian	Homo/Heterodyne + Gaussian Post-selection	Asymptotic Collective [165–167]
Z. Li et al.[168]	Coherent	Gaussian + Non- Gaussian Post-selection	Homo/Heterodyne	Asymptotic Collective[168]
L. S. Madsen et al.[169]	Squeezed	Gaussian + Additional Gaussian	Homodyne	Asymptotic Collective[169]

in experiments. Therefore, discrete modulated CV-QKD protocol[158] was proposed. The initial discrete modulated CV protocol is the four-state modulation protocol, where a modulation method similar to QPSK in classical communications was used. Soon afterwards, A. Leverrier[186] highlighted that CV protocols can be used for secret key distribution with multi-dimensional discrete modulation. In addition to discrete modulation, other modulation methods are also considered, including unidimensional modulation[159]. It simplifies the modulation process at the Alice side can be compared with the GG02 protocol when the excess noise is small. Most of the theoretical analysis of the CV-QKD protocols are based on fiber channels, and recently, the study is extended to the free space scenario for considerations of satellite quantum communications.[187]

Generally, the classification of standard one-way CV-QKD protocols, in which the quantum state passes through a single channel, can follow the type of the used quantum states (coherent or squeezed), the methods of modulation (Gaussian modulation, unidimensional modulation or discrete modulation) or the type of measurement (homodyne or heterodyne). In addition to the one-way protocols, various other protocols correspond to different application scenarios are proposed, such as two-way protocols, source-device-independent protocols, measurement-device-independent protocols, and so forth[188].

In 2008, the original two-way protocol was proposed[170], in which an optical switch was used to randomly switch between two working statuses "ON" or "OFF". The tolerable noise on ON mode is higher than that of one-way protocol. However, the use of optical switches cannot meet the demand for high-speed quantum key distribution. Subsequently in 2012, an improved two-way protocol was reported[172], in which Alice uses a Gaussian modulated coherent state and a beam splitter to replace the ON-OFF switch and translation operation in the original two-way protocol. Very recently, the protocol is proved to be secure in the finite-size regime [171]. In addition, the unidimensional two-way CV-QKD protocol is proposed to simplify the system realization and is proved to be secure against collective attack [189].

It should be noted, however, that the one-way and two-way protocols can be considered theoretically secure only with the trustworthy equipments. The issue of practical security remains a major concern due to the possible mismatch between practical devices and theoretical assumptions. An optimal solution would be a device-independent protocol, in which system security is not influenced by the trustworthiness of the devices. However, since achieving comprehensive device independence is challenging, semi-device-independence protocols have been developed and well studied, including the MDI

TABLE II. Current security status of the main two-way and MDI CV-QKD protocols.

Protocol	Alice's side		Bob's side		Measurement	Best Currently-Available Security Proofs
	State	Modulation	State	Modulation		
S. Pirandola et al.[170]	Coherent	Gaussian	Coherent	Gaussian	Homo/Heterodyne	Finite-size [171]
M. Sun et al.[172]	Coherent	Gaussian	Coherent	Gaussian	Homo/Heterodyne	Asymptotic [172]
Y. Zhao et al.[173]	Coherent	Gaussian + Non-Gaussian Post-selection	Coherent	Gaussian + Non-Gaussian Post-selection	Homodyne	Asymptotic collective [173]
C. Li et al.[174]	Coherent	Gaussian	Coherent	Gaussian	Homo/Heterodyne + Gaussian Post-selection	Asymptotic collective
Y. Bian et al.[175]	Coherent	Gaussian 1D	Coherent	Gaussian	Homodyne	Asymptotic collective[175]
Z. Li et al.[176] S. Pirandola et al.[177]	Coherent	Gaussian	Coherent	Gaussian	Bell-state Measurement	Finite-size [178,179] $K^{\epsilon}(N) > 0$ for practical N $\lim_{N\to\infty} K^{\epsilon}(N) < K_{\text{coll}}^{\text{asympt}}$
Y. Zhang et al.[180]	Squeezed	Gaussian	Squeezed	Gaussian	Bell-state Measurement	Finite-size[181] $K^{\epsilon}(N) > 0$ for practical N $\lim_{N\to\infty} K^{\epsilon}(N) < K_{\text{coll}}^{\text{asympt}}$
L. Huang et al.[182]	Coherent	Gaussian 1D	Coherent	Gaussian 1D	Bell-state Measurement	Asymptotic collective[182,183]
H. Ma et al.[184]	Coherent	QPSK	Coherent	QPSK	Bell-state Measurement	Asymptotic collective[184]
Y. Zhao et al.[185]	Coherent	Gaussian + Non-Gaussian Post-selection	Coherent	Gaussian + Non-Gaussian Post-selection	Bell-state Measurement	Asymptotic collective[185]

protocols[176,177] and the source-device-independent (SDI) protocols[190]. These protocols eliminate certain assumptions regarding the reliability of the devices and, thus, close the corresponding security loopholes.

The CV-MDI QKD was independently proposed by Z. Li et al.[176] and S. Pirandola et al.[177], in which Alice and Bob are both senders, preparing coherent states and sending them through two independent channels to the untrusted party, Charlie, to perform Bell-state measurement. Note that there are no assumptions about the trustworthiness on Charlie, which implies that Eve can have complete control over Charlie, and it can withstand all attacks that are based on detector's loopholes. However, the CV-MDI QKD protocol has a limited transmission distance which restricts the long-haul deployment. In 2019, the discrete modulation is used for CV-MDI QKD[184], whose secret key rate correspondingly decreases but can still guarantee its security against collective attack. The unidimensional CV-MDI QKD protocol was also proposed[182,183], in which more cases are considered in[182], while the finite-size effect is involved in[183]. The security of the CV-MDI protocol under the source intensity errors is also investigated[191]. Here, the current security proofs status of the two-way protocols and the MDI protocols are revealed in Table II.

Another semi-device-independent protocol, known as the SDI protocol, has also undergone development in addition to the MDI protocol. The CV-SDI QKD protocol was initially proposed in 2013 and has been demonstrated to be resistant to collective attacks[190]. Furthermore, Y. Zhang et al. supplemented the security proof in 2020[192]. Similar to the CV-MDI QKD, the CV-SDI QKD protocol does not make any assumptions about the source's credibility. In this protocol, an entanglement source is positioned between Alice and Bob as both Alice and Bob are receivers. In addition, there are also some

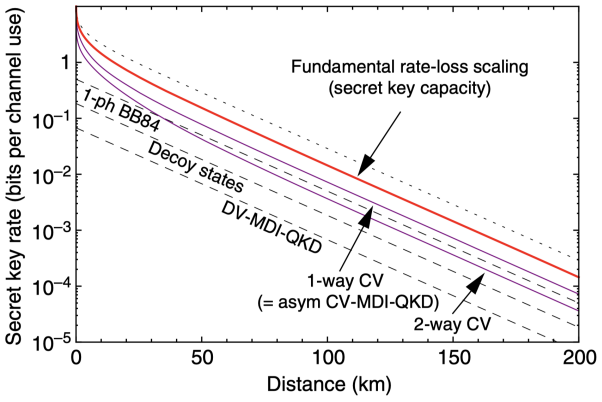

FIG. 4. The PLOB bound and the distance between the PLOB bound and various QKD protocols in ideal case. From S. Pirandola et al.[87]. S. Pirandola et al., Nat. Commun., 8, 15043, 2017; licensed under a Creative Commons Attribution (CC BY) license.

special CV-QKD protocols such as using a thermal state as the source, so called the passive protocol[193].

As shown in Fig. 4, ideal CV-QKD protocols are closer to the theoretical limit, known as the PLOB bound[87], which shows the potential of achieving high secret key rate and long transmission distance using CV-QKD. But we have to remark that, there is still a gap between the optimal parameters of the existing CV-QKD protocols for practical and ideal situations, where the reconciliation efficiency is normally less than 100 % and the optimal modulation variance is limited to less than 5. Therefore the performance in a practical CV-QKD system still has room to be improved, and more CV-QKD protocols are expected to be proposed for further approaching the theoretical limit.

C. Security analysis

Before starting the security analysis, it is essential to introduce two equivalent schemes, namely the prepare-and-measurement (PM) scheme and the entanglement-based (EB) scheme, as shown in Fig. 5. These schemes differ mainly in the method of preparing quantum states. In the PM scheme, Alice generates the states with a light resource, usually a laser, whereas in the EB scheme, Alice generates EPR states. As homodyne (heterodyne) detection performed on one mode of the EPR state has the effect of projecting the other mode onto a squeezed (coherent) state, the transmitter's outputs of both methods are identical for the third party. Therefore, both schemes are equivalent to Bob and Eve, which is an important property.

It is important to note that although both schemes are equivalent, they are used in different application scenarios. For instance, the PM scheme is used for experimental implementation, whereas the EB scheme is used for theoretical analysis due to its ease of calculation. Our analysis is based on the EB scheme in the following part.

Reconciliation is the key technique to make Alice and Bob share a same bit string, which can be categorized into two types, the direct reconciliation and the reverse reconciliation[194]. In direct reconciliation, the detection data is corrected to the modulation data, however, the tolerable channel loss is limited under 3 dB. Reverse reconciliation is proposed to solve this issue, by correcting the modulation data to the detection data.

In the aspect of an eavesdropper, the attack strategy can be categorized into 3 types, individual attack, collective attack and coherent attack. In individual attack, Eve manipulates and measures the transmitted states independently and identically. In collective attack, Eve manipulates the transmitted states independently and identically, but measures them jointly. While for coherent attack, Eve manipulates and measures the transmitted states jointly. Usually, coherent attack is the strongest one, while in asymptotic case the collective attack is normally the most powerful coherent attack.

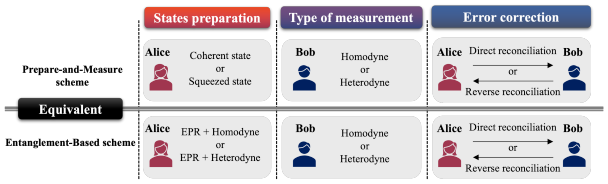

FIG. 5. The PM protocol and the equivalent EB protocol in CV-QKD. The most important steps in a CV-QKD protocol are the state preparation, the measurement and the error correction. The main difference between these two types of the protocols are the state preparation, where the coherent state preparation is equal to the heterodyne detection on one of the modes of the EPR state, and the squeezed state preparation is equal to the homodyne detection on one of the modes of the EPR state.

1. *Gaussian-modulated protocol*

The protocols based on Gaussian modulation are the most fundamental among all CV-QKD protocols, which are usually categorized into four types based on types of quantum states (coherent or squeezed) and detection methods (homodyne or heterodyne). So far, the protocols based on Gaussian modulated coherent states which can be generated by the off-the-shelf laser have received much attentions. Therefore, we detail the security analysis of the Gaussian-modulated coherent state protocol, and briefly introduce the squeezed-state protocol.

The security indicator is the secret key rate. If the secret key rate is greater than zero while considering attacks, then Alice and Bob can distill a secret key under the attack. Otherwise, the protocol will not be effective. The asymptotic secret key rate with reverse reconciliation can be given by[195]

$$R = \beta I_{AB} - S_{BE}, \tag{10}$$

where I_{AB} is the classical mutual information between Alice and Bob, that can be easily estimated, normally written as

$$\begin{aligned} I_{AB}^{hom} &= \frac{1}{2}\log_2\frac{V_B}{V_{B|A}} = \frac{1}{2}\log_2\frac{V+\chi_{line}}{1+\chi_{line}}, \\ I_{AB}^{het} &= \log_2\frac{V_B+1}{V_{B|A}+1} = \log_2\frac{T\,(V+\chi_{line})+1}{T\,(1+\chi_{line})+1}, \end{aligned} \tag{11}$$

for perfect homodyne and heterodyne detection. Here V is the variance of EPR state owned by Alice, V_B is the variance of the state Bob receives, $V_{A|B}$ is the conditional variance given Bob's measurement result. $\chi_{line} = 1/T - 1 + \varepsilon$ is the total channel-added noise expressed in shot noise units (SNUs), relevant to the channel parameters, including the transmittance (T) and excess noise (ε)[196]. Since mainstream CV-QKD implementations use reverse reconciliation, where the modulation data is corrected to the detection data, the quantum mutual information between Bob and Eve, S_{BE}, is the concern.

It is pointed out that the maximum information available to Eve is bounded by Holevo quantity[197]:

$$S_{BE} = \chi_{BE} = S(E) - S(E|m_B), \tag{12}$$

TABLE III. Main calculation equations of secret key rate of Gaussian-modulated CV-QKD protocols.

States	Measurement	I_{AB}	Eigenvalues of the Covariance Matrix before Measurement	Type of Reconciliation	Eigenvalues of the Covariance Matrix after Measurement	χ_{BE}
Squeezed	Homodyne	$\frac{1}{2}\log_2\frac{V+\chi}{\chi+1/V}$	$\lambda_{1,2}=\sqrt{\frac{1}{2}\left[\Delta\pm\sqrt{\Delta^2-4D^2}\right]}$	Direct	$\lambda_3=\sqrt{\frac{T^2(V+\chi)}{(\chi+1/V)}}$	$\sum_{i=1}^{2}G(\lambda_i)-G(\lambda_3)$
				Reverse	$\lambda_4=\sqrt{\frac{V(V\chi+1)}{(\chi+V)}}$	$\sum_{i=1}^{2}G(\lambda_i)-G(\lambda_4)$
Coherent	Homodyne	$\frac{1}{2}\log_2\frac{V+\chi}{\chi+1}$		Direct	$\lambda_{5,6}=\sqrt{\frac{1}{2}\left[A\pm\sqrt{A^2-4B}\right]}$	$\sum_{i=1}^{2}G(\lambda_i)-\sum_{i=5}^{6}G(\lambda_i)$
				Reverse	$\lambda_7=\lambda_4=\sqrt{\frac{V(V\chi+1)}{(\chi+V)}}$	$\sum_{i=1}^{2}G(\lambda_i)-G(\lambda_7)$
Squeezed	Heterodyne	$\frac{1}{2}\log_2\frac{T(V+\chi)+1}{T(\chi+1/V)+1}$		Direct	$\lambda_8=\lambda_3=\sqrt{\frac{T^2(V+\chi)}{(\chi+1/V)}}$	$\sum_{i=1}^{2}G(\lambda_i)-G(\lambda_8)$
				Reverse	$\lambda_{9,10}=\sqrt{\frac{1}{2}\left[A'\pm\sqrt{A'^2-4B'}\right]}$	$\sum_{i=1}^{2}G(\lambda_i)-\sum_{i=9}^{10}G(\lambda_i)$
Coherent	Heterodyne	$\log_2\frac{T(V+\chi)+1}{T(\chi+1)+1}$		Direct	$\lambda_{11}=T(\chi+1)$	$\sum_{i=1}^{2}G(\lambda_i)-G(\lambda_{11})$
				Reverse	$\lambda_{12}=\frac{T(V\chi+1)+1}{T(V+\chi)+1}$	$\sum_{i=1}^{2}G(\lambda_i)-G(\lambda_{12})$
Notice	$\begin{pmatrix} a\,I_2 & c\,\sigma_z \\ c\,\sigma_z & b\,I_2 \end{pmatrix}=\begin{pmatrix} V\,I_2 & \sqrt{T(V^2-1)}\,\sigma_z \\ \sqrt{T(V^2-1)}\,\sigma_z & T(V+\chi)\,I_2 \end{pmatrix}$, $\Delta=a^2+b^2-2c^2, D=ab-c^2, A=\frac{1}{a+1}(a+bD+\Delta), A'=\frac{1}{b+1}(b+aD+\Delta), B=\frac{D}{a+1}(b+D)$, $B'=\frac{D}{b+1}(a+D), G(x)=\frac{x+1}{2}\log_2\frac{x+1}{2}-\frac{x-1}{2}\log_2\frac{x-1}{2}$, V is the variance of the EPR state which is also written as V_A when representing the variance of mode V.					

where $S(E)$ is the von Neumann entropy of the eavesdropper's state ρ_E, and $S(E|m_B)$ is von Neumann entropy conditional on Bob's measurement result and is determined by the detection method. Based on the fact that the eavesdropper Eve is able to purify the binary quantum system ρ_{AB}, Eq. (12) becomes

$$\chi_{BE}=S(\rho_{AB})-S\left(\rho_{AB|m_B}\right). \tag{13}$$

As for χ_{BE}, usually we use the Gaussian extremity theorem to find its upper bound[198], corresponding to the lower bound of the secret key rate. This means there always exists a Gaussian state ρ_{AB}^G with the same covariance matrix as ρ_{AB} who makes

$$\chi_{BE}\leq\chi_{BE}^G=S\left(\rho_{AB}^G\right)-S\left(\rho_{AB|m_B}^G\right). \tag{14}$$

Specifically, calculations of $S\left(\rho_{AB}^G\right)$ and $S\left(\rho_{AB|m_B}^G\right)$ can be simplified using the symplectic eigenvalues of the covariance matrix γ_{AB} and $\gamma_{AB|m_B}$ respectively, corresponding to the states ρ_{AB} and $\rho_{AB|m_B}$. Covariance matrix γ_{AB} can be estimated from the modulation and detection data

$$\gamma_{AB}=\begin{pmatrix}\gamma_A & \sigma_{AB}\\ \sigma_{AB} & \gamma_B\end{pmatrix}=\begin{pmatrix}V_A\,I_2 & C_{AB}\,\sigma_z\\ C_{AB}\,\sigma_z & V_B\,I_2\end{pmatrix}=\begin{pmatrix}a\,I_2 & c\,\sigma_z\\ c\,\sigma_z & b\,I_2\end{pmatrix}. \tag{15}$$

then $\gamma_{AB|m_B}$ is given by

$$\gamma_{AB|m_B}=\gamma_A-\sigma_{AB}^T H\sigma_{AB}. \tag{16}$$

Here, H is the symplectic matrix on behalf of the measurement operation on mode B, and can be written respectively:

$$\begin{aligned}H^{hom}&=(X\gamma_B X)^{MP},\\ H^{het}&=(\gamma_B+I_2)^{-1},\end{aligned} \tag{17}$$

where $X=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ (for homodyne detection on p quadrature, we use $P=\begin{pmatrix}0&0\\0&1\end{pmatrix}$), and MP represents for the Moore-Penrose pseudo-inverse of a matrix. Notice that γ_A, γ_B and σ_{AB} are the subsmatrices of the covariance matrix γ_{AB} as detailed in Eq. (15).

Generally, the symplectic eigenvalues of a covariance matrix γ can be achieved by calculating the eigenvalues of $i\Omega\gamma$. For the two-mode system, one can easily achieve the analytical solution, as detailed in Table. III, where $S\left(\rho_{AB}^G\right)$ can be calculated with $\lambda_{1,2}$, and $S\left(\rho_{AB|m_B}^G\right)$ can be calculated with λ_7 for homodyne detection and λ_{12} for heterodyne detection.

$$\begin{aligned}\chi_{BE}^{hom}&=\sum_{i=1}^{2}G(\lambda_i)-G(\lambda_7),\\ \chi_{BE}^{het}&=\sum_{i=1}^{2}G(\lambda_i)-G(\lambda_{12}),\end{aligned} \tag{18}$$

where

$$G(x)=\frac{x+1}{2}\log_2\frac{x+1}{2}-\frac{x-1}{2}\log_2\frac{x-1}{2}. \tag{19}$$

Similarly, the case with direct reconciliation or the security analysis of squeezed states protocols can be analyzed, for simplicity, the analytical solutions are concluded in Table. III.

2. *Discrete-modulated protocol*

The earliest investigation on discrete-modulated CV-QKD is in 2009, when the transmission distance of a CV-QKD sys-

tem is limited to less than 30 km due to the lack of the efficient error correction strategy of Gaussian variable at low SNR, and the proposed discrete-modulated protocol reduces the requirement of error correction, which can be a promising way to enhance the system transmission distance[158].

The early security proof requires the linear channel assumption, where the input-output relations of the quadrature operators in Heisenberg representation are given by

$$X_{out} = g_X X_{in} + B_X, P_{out} = g_P P_{in} + B_P. \tag{20}$$

Here the added noises B_X, B_P are uncorrelated with the input quadratures X_{in}, P_{in}. Only based on this assumption, the covariance matrix describing the system after the quantum state transmission can be written as

$$\gamma = \begin{pmatrix} (V_M+1)\, I_2 & \sqrt{T}Z\, \sigma_z \\ \sqrt{T}Z\, \sigma_z & (TV_M+1+T\varepsilon)\, I_2 \end{pmatrix}, \tag{21}$$

where V_M, T, and ε correspond, respectively, to modulation variance ($V_M = V-1$, V is the variance of mode A), the channel transmittance, and the excess noise estimated experimentally in the prepare and measure scenario. Here, Z is a function of V_M. Once the covariance matrix is achieved, the Gaussian extremity theorem can be used to calculate the upper bound of the eavesdropper's knowledge, which is similar to the security analysis method in Gaussian-modulated protocol. Then, the lower bound of secret key rate can be derived.

The linear channel assumption is adopted since the quadrature measurement of one mode of an EPR state cannot directly map the other mode to a group of discrete-modulated coherent states. This results in the lack of covariance item Z in the covariance matrix, leading to the need for an additional assumption. If considering general case without linear channel assumption, the unknown of Z will lead to the worst-case estimation of the secret key rate, which is zero. Since the security proof of the discrete-modulated CV-QKD is not perfect, the discrete-modulated CV-QKD system is less concerned for a period of time.

This situation did not change until 2018, as the security proof of discrete-modulated protocols gradually improved and no longer required linear channel assumptions[125]. The eavesdropping behavior can be bounded through methods such as the uncertainty principle[125], the semidefine programming[126,127], and the entropy uncertainty[129], then the secret key rate of the protocol can be obtained by searching for the lower bound.

Introducing an auxiliary mode into the EB scheme is a feasible strategy to continuously use the security analysis method based on covariance matrix[125]. Before sending the mode into the unsecured quantum channel, the mode is divided by a beamsplitter, and one of the output mode is preserved by the sender. This preserved mode can be used to construct correlations between Alice and Bob. Therefore, the covariance matrix describing the system contains 3 modes, which weakens the negative influence of the undefined covariance on secret key rate. This works for arbitrary discrete modulation formats, specifically, 256 QAM with Gaussian probability shaping performs close to the Gaussian modulated protocol, and the 64 QAM system can still support the transmission of more than 100 km.

Specifically, after the transmission of the quantum state, the covariance matrix of the quantum state shared by Alice and Bob can be written as

$$\gamma_{\mathbf{A}\mathbf{C}B} = \begin{pmatrix} \gamma_{\mathbf{A}} & \phi_{\mathbf{A}\mathbf{C}} & \kappa_{\mathbf{A}B} \\ \phi_{\mathbf{A}\mathbf{C}}^T & \gamma_{\mathbf{C}} & \phi_{\mathbf{C}B} \\ \kappa_{\mathbf{A}B}^T & \phi_{\mathbf{C}B}^T & \gamma_B \end{pmatrix}, \tag{22}$$

where $\gamma_{\mathbf{A}}$, $\gamma_{\mathbf{C}}$, and $\phi_{\mathbf{A}\mathbf{C}}$ can be theoretically calculated, $\phi_{\mathbf{C}B}$, γ_B can be estimated through the measured data, and only the covariance term $\kappa_{\mathbf{A}B}$ is unknown. Since the covariance matrix γ_N for a N-mode state is constrained by the uncertainty principle (Eq. (7)). The constraint set S_κ which limits the possible value of $\kappa_{\mathbf{A}B}$ can be obtained as

$$S_\kappa = \{\phi_{\mathbf{A}B} \mid \gamma_{\mathbf{A}\mathbf{C}B}[\kappa_{\mathbf{A}B} = \phi_{\mathbf{A}B}] + i\Omega_N \geq 0\} \tag{23}$$

and the maximum value of S_{BE}^G can be obtained by searching in the set.

Overall, the secret key rate at the asymptotic limit can be calculated as follow:

$$K = \beta I(M_{\mathbf{A}} : H_B) - \sup_{\kappa_{\mathbf{A}B} \in S_\kappa} S_{BE}^G(\kappa_{\mathbf{A}B}), \tag{24}$$

where $I(M_{\mathbf{A}} : H_B)$is the classical mutual information, and β is the reconciliation efficiency.

In 2019, S. Ghorai et al. proposed another security framework based on formulating the above problem as a semidefinite program (SDP) and focused on analyzing the security of a QPSK protocol[126]. In this framework, SDP is used to search a state bounded by specially designed statistics between modulation and detection data. It can be extended to a high-order modulation format and can be derived with an analytical solution of secret key rate in a symmetric modulation case[128].

Soon later in 2019, J. Lin et al. proposed another strategy to analyze the security of a discrete-modulated CV-QKD protocol with SDP[127]. The security of two QPSK protocols, with homodyne and heterodyne detection respectively are analyzed. It adopts a mapping and postselection based on the detection data to construct the positive operator valued measurement of the receiver. In principle, this security framework can also be extended to high-order modulation format, but practically, it is limited by the demand of high computational resource.

In the method proposed by J. Lin et al.[127], the secret key rate under collective attacks in the asymptotic limit can be can rewritten as

$$K = \min_{\rho_{AB} \in \mathbf{S}} D(\mathscr{G}(\rho_{AB}) \| \mathscr{Z}[\mathscr{G}(\rho_{AB})]) - p_{\text{pass}}\, \delta_{\text{EC}} \tag{25}$$

where $D(\sigma\|\tau) := \text{tr}(\sigma log\sigma) - \text{tr}(\sigma log\tau)$ is the quantum relative entropy, $\mathscr{G}$ is a completely positive map related to the postselection in terms of actions on the bipartite state ρ_{AB} and $\mathscr{Z}$ is a completely positive trace preserving map related to the key map, δ_{EC} stands for the actual amount of information leakage per signal and p_{pass} is the sifting probability.

TABLE IV. The security framework of discrete-modulated CV-QKD.

Security analysis methods	Years	Representative results
Uncertainty principle[125]	2018	Arbitrary formats, 256 QAM, QPSK et al.
Linear semidefinite program[126]	2019	Arbitrary formats, 256 QAM, QPSK et al.
Nonlinear semidefinite program[127]	2019	12-state double ring, QPSK et al.
Entangled photon pairs[129]	2021	2-state

In the transformed formula, only the first term is unknown, so the rate calculation problem has become a convex optimization problem for solving the minimum value of the first term in the formula. The set **S** is the feasible set of the optimization problem, which contains all bipartite density operators ρ_{AB} that are compatible with experimental observations.

From the measurement of Bob, the expectation values of the first and second moments of the quadrature operators $\langle\hat{x}\rangle$, $\langle\hat{x}^2\rangle$, $\langle\hat{p}\rangle$, $\langle\hat{p}^2\rangle$ can be obtained. In addition, the operators $\hat{n}=\hat{a}^\dagger\hat{a}$ and $\hat{d}=\hat{a}^2+(\hat{a}^\dagger)^2$ to constrain ρ_{AB}.

The relevant optimization problem is

$$\text{minimize}\, D\left(\mathscr{G}\left(\rho_{AB}\right)\|\mathscr{Z}\left[\mathscr{G}\left(\rho_{AB}\right)\right]\right), \tag{26}$$

subject to

$$\begin{cases} \mathrm{Tr}\left[\rho_{AB}\left(|k\rangle\langle k|_A\otimes\hat{x}\right)\right]=p_k\langle\hat{q}\rangle_k, \\ \mathrm{Tr}\left[\rho_{AB}\left(|k\rangle\langle k|_A\otimes\hat{p}\right)\right]=p_k\langle\hat{p}\rangle_k, \\ \mathrm{Tr}\left[\rho_{AB}\left(|k\rangle\langle k|_A\otimes\hat{n}\right)\right]=p_k\langle\hat{n}\rangle_k, \\ \mathrm{Tr}\left[\rho_{AB}\left(|k\rangle\langle k|_A\otimes\hat{d}\right)\right]=p_k\langle\hat{d}\rangle_k, \\ \mathrm{Tr}\left[\rho_{AB}\right]=1, \\ \mathrm{Tr}_B\left[\rho_{AB}\right]=\sum_{i,j=0}^{3}\sqrt{p_ip_j}\langle\varphi_j\mid\varphi_i\rangle|i\rangle\langle j|_A, \\ \rho_{AB}\geq 0, \end{cases} \tag{27}$$

where $k\in\{0,1,...M\}$, p_k is the probability of sending the corresponding state, M is the modulation order, and $\langle\hat{q}\rangle_k$, $\langle\hat{p}\rangle_k$, $\langle\hat{n}\rangle_k$, $\langle\hat{d}\rangle_k$ denote the corresponding expectation values of operators $\hat{x}$, $\hat{q}$, $\hat{n}$, $\hat{d}$ for the conditional state ρ_B^x. This security analysis framework is further developed to higher modulation level with various formats[199–206].

In addition to the security analysis methods we mentioned above, there also exists some other strategies that can reach security under finite-size effect, such as the binary modulated protocol[207], the QPSK protocol using the entropy accumulation[208] and the discrete alphabet CV-QKD[209]. The recent progress of the security analysis of discrete-modulated protocol is shown in Table. IV and the performance is shown in Fig. 6. In conclusion, the mainstream strategy to provide a general security analysis of the discrete-modulated protocol is to introduce more correlation between Alice and Bob, which contributes to a tighter bound on the possible eavesdropping behavior.

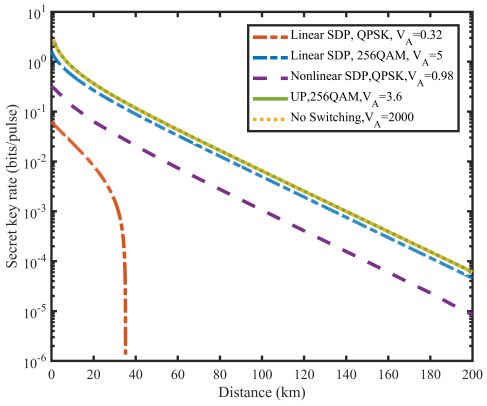

FIG. 6. The performance of different heterodyne detected discrete-modulated CV-QKD security analysis, including the linear SDP (red and blue line), the nolinear SDP (purple line) and the security analysis using uncertainty principle (UP) (green line). The modulation variance are the optimal for different security analysis. The performance of the no-switching protocol is also presented (yellow line).

3. *Practical protocol with trusted noise*

The practical measurement of a CV-QKD system usually suffers from the imperfect detection efficiency and electronic noise, leading to the increase of channel loss and excess noise. While in device-dependent system, the trusted device with specific noise model can relax the degradation caused by device imperfections[132,210,211]. Normally, the coherent receiver of a CV-QKD system can be trusted, where the loss and noise inside the detector can be modeled by an EPR state with one mode (denoted as F_0) coupled into the signal path by a beamsplitter. The trusted detector module significantly enhances the transmission distance and the secret key rate of the system, which is demonstrated in the early experiment[132]. Further, the feasibility of enhancing the system performance using optical amplifiers is proved[212–216]. As shown in Fig. 7, here we denote the output mode after the coupling as F, and the other mode of the EPR state as G. The transmittance of the beamsplitter, η, reflects the detection efficiency. The variance of the EPR state is written as,

$$V_D=1+v_{ele}/(1-\eta), \tag{28}$$

where v_{ele} reflects the variance of the electronic noise of a homodyne detector. For heterodyne detection, v_{ele} should be replaced by $2v_{ele}$. The security analysis is based on the covariance matrix γ_{AFGB}

$$\gamma_{AFGB}=\begin{pmatrix}\gamma_{AFG} & \sigma_{AFGB}^T\\ \sigma_{AFGB} & \gamma_B\end{pmatrix}. \tag{29}$$

For convenience, we will discuss both homodyne and heterodyne scenarios simultaneously in this section. A practical detector is characterized by an efficiency η and a noise v_{ele} due to detector electronics. As we did for the channel, we can define a detection-added noise referred to Bob's input and

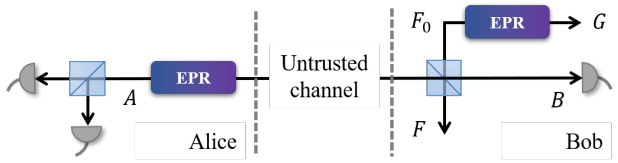

FIG. 7. The EB scheme of the security analysis with trusted detector module. The structure of Alice is the same as preparing coherent state with EPR states. The beamsplitter at the receiver site has the transmittance of η, and the variance of the EPR state is $V_D = 1 + v_{ele}/(1-\eta)$. Here, v_{ele} is the electronic noise of the homodyne detector.

expressed in shot-noise units that we devote in general as χ_h, and is given by the expressions

$$\chi_{hom} = [(1-\eta) + v_{ele}]/\eta, \tag{30}$$

and

$$\chi_{het} = [1 + (1-\eta) + 2v_{ele}]/\eta, \tag{31}$$

for homodyne and heterodyne detection, respectively. The total noise refered to the channel input can then be expressed as $\chi_{tot} = \chi_{line} + \chi_h/T$.

The mutual information between Alice and Bob is given in the case of practical protocol with trusted noise by the same expressions as Eq. (11) by replacing χ_{line} to χ_{tot}. The upper bound of Eve's knowledge, χ_{BE} becomes

$$\chi_{BE} = \sum_{i=1}^{2} G(\lambda_i') - \sum_{i=3}^{5} G(\lambda_i'), \tag{32}$$

where $\lambda_{1,2}'$ represent the symplectic eigenvalues of covariance matrix γ_{AB}. $\lambda_{3,4,5}'$ represent the symplectic eigenvalues of covariance matrix $\gamma_{AFGB|m_A}$ which is given by

$$\gamma_{AFGB|m_A} = \gamma_{AFG} - \sigma_{AFGB}^T H \sigma_{AFGB}. \tag{33}$$

Here, γ_{AFG} and σ_{AFGB} are the sub-matrix of γ_{AFGB}. The symplectic eigenvalues can be given by expressions of the form,

$$\lambda_{1,2}'^2 = \frac{1}{2}[\Delta \pm \sqrt{\Delta^2 - 4D}], \tag{34}$$

$$\lambda_{3,4}'^2 = \frac{1}{2}[E \pm \sqrt{E^2 - 4F}], \tag{35}$$

and $\lambda_5' = 1$. For the homodyne case,

$$E_{hom} = \frac{\Delta\chi_{hom} + V\sqrt{D} + T(V + \chi_{line})}{T(V + \chi_{tot})}, \tag{36}$$

$$F_{hom} = \sqrt{D}\frac{V + \sqrt{D}\chi_{hom}}{T(V + \chi_{tot})}, \tag{37}$$

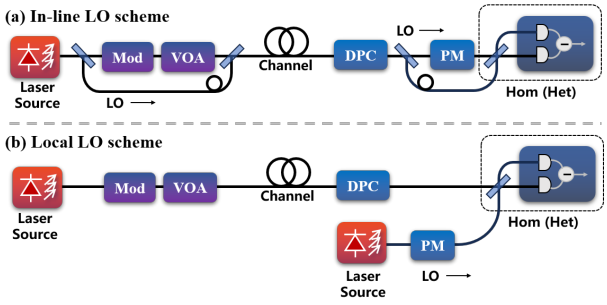

FIG. 8. Two mainstream structures of CV-QKD system implementation: (a) In-line LO scheme and (b) Local LO scheme. The phase modulator at the receiver's side, is used to choose the quadrature of measurement for homodyne detection, which is not needed for heterodyne detection. Mod: Gaussian or discrete modulation, VOA: variable optical attenuator, DPC: dynamic polarization controller, PM: phase modulator, Hom: homodyne detector, Het: heterodyne detector.

and for the heterodyne case,

$$E_{het} = \frac{\Delta\chi_{het}^2 + D + 1 + 2\chi_{het}(V\sqrt{D} + T(V + \chi_{line})) + 2T(V^2 - 1)}{(T(V + \chi_{tot}))^2}, \tag{38}$$

$$F_{het} = (\frac{V + \sqrt{D}\chi_{het}}{T(V + \chi_{tot})})^2, \tag{39}$$

where Δ, D are given in Table. III.

III. CV-QKD SYSTEM AND KEY MODULE

In this section, we will provide an overview of the architecture and the details of the main modules in a CV-QKD system. A summary of the current status of the key modules in a CV-QKD system using coherent states can be found in Table V. Generally, CV-QKD system can be categorized into two types, the in-line LO and the local LO. As shown in Fig. 8, of all the differences between these two types of systems, the greatest one is whether the LO is generated inside the receiver. For the in-line LO system, as shown in Fig. 8 (a), the light generated by the laser source is divided, where part of the light is modulated and attenuated to quantum level, while the other part of the light is used as the strong LO. The quantum signal and LO are then multiplexed and transmitted to the receiver simultaneously. For the local LO system, displayed in Fig. 8 (b), in principal the transmitter only need to modulate and send the quantum signal, and the receiver uses the locally generated LO to perform coherent detection, which simplifies the system structure and prevents the access of LO by Eve. These two different system schemes result in different main noise source, therefore various system architectures are adopted for suppressing the excess noise and raise the secret key rate.

Generally, the structure of a CV-QKD system can be concluded in Fig. 9. The transmitter and receiver are the optical

TABLE V. Current implementation status of the key module technology of CV-QKD system using coherent states. TDM: Time-Division Multiplexing, Pol.M: Polarization Multiplexing, FDM: Frequency-Division Multiplexing, MIMO: Multiple-Input Multiple-Output, LDPC: Low Density Parity Check.

Key Module			Function	Notes
Transmitter	Source	Pulsed	Pulsed light generation	High extinction ratio of $\geq$ 60 dB with narrow linewidth
		Continuous-wave	Continuous-wave light generation	Narrow linewidth $\leq$ 20 kHz
	Modulation	Gaussian modulation	Preparation of coherent states obeying Gaussian distribution	1 GHz repetition frequency with IQ modulator
		Discrete modulation	Preparation of coherent states obeying discrete distribution	1 GBaud 256 QAM Gaussian probability shaping with IQ modulator
		Attenuation	Reducing the power of signals to quantum level for security	Variable optical attenuator or amplitued modulator
		Multiplexing	Co-propagation of quantum signal and LO / pilot-tone	TDM, Pol.M, TDM+Pol.M, FDM, FDM+Pol.M, Dual Pol.
	Transmitter Monitoring	Source monitoring	Source modeling	Detecting a fraction of the modulated signal
		Injected light monitoring	Closing potential security loopholes	Detecting the injected light
Receiver	Receiver Monitoring	LO monitoring	Closing potential security loopholes	Detecting a fraction of the LO
		Injected light monitoring		Detecting the injected light
	De-modulation	Sychronization	Keeping the receiver's clock consistent with the sender's clock	Co-propagation or a separately transmission of the clock signal
		De-multiplexing	Separating the quantum signal and LO (or pilot signal if necessary) before detection	Optical delay line and / or polarization beamsplitter before detection
		Optical compensation	Suppressing the noise from polarization or phase mismatch	Dynamic polarization controller and / or phase shifter
	Detection	Detection balance	Compensation of the imbalance from different optical paths	Variable optical attenuator before photodiodes
		Hom / Het detection	Measurement of the quadrature information	Shot noise limited homodyne detection, heterodyne detection
QRNG	-	Continuous	Getting continuous-distributed random numbers to support Gaussian modulation	Transmitting from the discrete-distributed random number, or QRNG with continuous ouput
		Discrete	Getting 0&1 random numbers for discrete modulation, sifting and postprocessing	High-speed QRNG, normally based on continous-variable system
SNU Calibration	-	Two time	Achieving the SNU for data normoalization	Calibrating the total noise and electronic noise
		One time		Calibrating the total noise
DSP	Pulse shaping	-	Generating signal pulses and raise the spectrum efficiency	RRC filter
	Framing	-	Quantum signal, LO / pilot tone and frame signal	Frequency division multiplexing
	Synchronization	Clock	Keeping the receiver's clock consistent with the sender's clock	Co-propagation or a separately transmission of the clock signal
		Frame	Definition of the starting and ending positions	Data frame in LO or pilot tone
	Equalization	Static	Compensation of device imperfections	S21 compensation, matched filter, skew compensation
		Dynamic	Compensation of transmission impairments	Phase and polarization mismatch with MIMO algorithms
Post-processing	Sifting	-	Preseving the modulation data with the same detection basis as the detector	Detection basis announcement
	Parameter estimation	-	Estimation of the secret key rate	Estimating the covariance matrix or system parameters
	Information reconciliation	Reconciliation	Mapping the continous data to discrete form	Slice reconciliation and multidimensional reconciliation
		Error Correction	Making the two parties share a same bit string	LDPC and Polar code
	Privacy amplification	-	Distilling the final secret key bits	Toepliz matrix

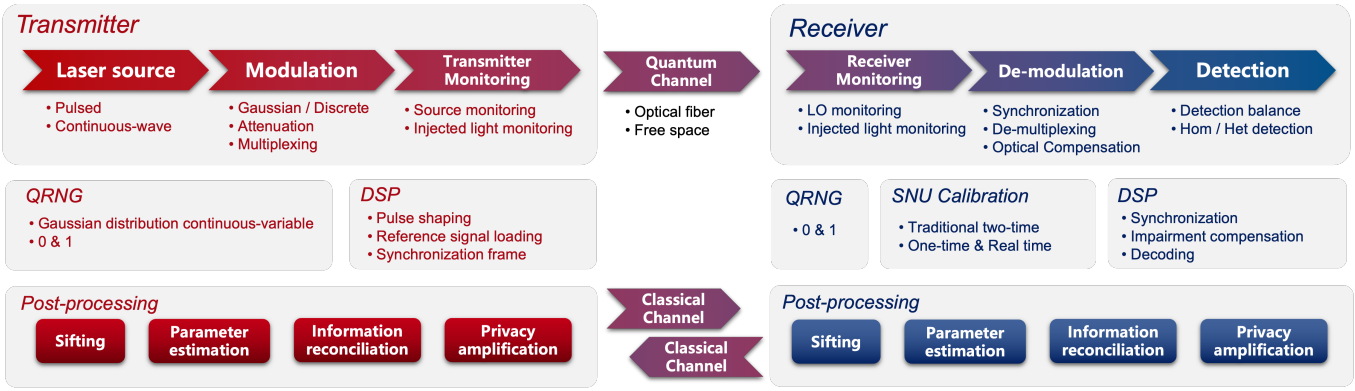

FIG. 9. The key modules in a CV-QKD system. The transmitter and receiver form the optical part. Optical fiber and free space are the two kinds of quantum channel, where the optical fiber is the mainstream way to transmit the quantum signals. System control is normally used to realize the synchronization between the transmitter and the receiver. QRNG are deployed at both sides to provide the random numbers for modulation, detection and postprocessing. Shot noise unit (SNU) calibration is the security module which provides the normalized unit of the detection data. Post-processing uses classical channel to exchange the information on modulation and detection data, and getting the final secret key bits.

modules of the system, which are responsible for the information encoding and decoding.

The transmitter consists of the laser source, the modulation module and the monitoring module. The laser source can be pulsed or continuous-wave light. The mostly commonly employed modulation formats are Gaussian and discrete modulation. Additionally, the modulator must modulate and multiplex a classical auxiliary signal with the quantum signal, which is the LO in an in-line LO system and the pilot tone in a local LO system. The quantum signal is multiplexed with LO or pilot tone using time-division, frequency-division and polarization multiplexing techniques. For security reasons, monitoring is typically employed at the output stage.

At the receiver end, the co-transmitted quantum and classical signals are demodulated and detected by shot-noise-limited balanced homodyne detectors. A seperate monitoring module is deployed to ensure the practical security. Several automatic feedback methods are used to calibrate sampling time, polarization, and phase of the quantum states in order to overcome perturbations in the channel due to changing environmental conditions. These calibrations can be realized using either hardware or digital techniques.

To map the output of the detector to the quadrature information, DSP is employed with the aim of achieving maximal correlation between the transmitter and receiver. With the assist of DSP, SNU calibration enables the establishment of a connection between theoretical security analysis and the practical system, a crucial aspect of system security. Lastly, postprocessing is processed to extract the secret key bits from the correlation established by the aforementioned procedures. It comprises sifting, parameter estimation, information reconciliation, and privacy amplification. The randomness of the overall system is supported by the quantum random number generator (QRNG), which provides the information of modulation and controls the postprocessing.

A. Quantum random number generator

Randomness determines the security of a CV-QKD system. In fact, all of the random numbers used in a CV-QKD system should satisfy the true randomness, which is essential to the unconditional security[3–6]. An outstanding alternative is a QRNG, which exploits the intrinsic random nature of quantum mechanics, acts as a promising method in generating truly random numbers[217–219].

The random numbers are used for controlling the modulators so that the sender can prepare random coherent states following a certain modulation format, determining the detection basis during homodyne detection, and constructing mappings or universal hash functions in postprocessing. Specifically, Gaussian distributed random numbers, Rayleigh distributed or uniformly distributed random numbers in continuous-variable form are required in Gaussian modulation of coherent states. Discrete-variable random numbers are required in discrete-modulation, basis selection and postprocessing.

Based on different security levels, the QRNG can be divided into the practical type[220,235–239], the semi-device independent type[240–249] and the device independent type[250–253]. The QRNG can also be divided into the discrete-variable and continuous-variable types corresponding to different types of entropy source. Normally, the continuous-variable QRNG can support high generation rate with simple structure, where the randomness can come from the ASE noise[232–234,254–257], the phase noise[225–230,258–267] and the vacuum noise[222–224,268–270]. The QRNG based on vacuum noise can achieve high-speed and simple structure, using only a laser source and a homodyne detector[222,223,270]. The state of the art QRNG based on the vacuum noise can achieve a generation rate of 100 Gbps using photonic integrated circuits[271], where the speed, size and scalability can well satisfy the need of a CV-QKD system[224]. Here we summarize the most commonly used QRNG implementations as shown in Table VI.

However, the most of the QRNG generates random num-

TABLE VI. Current QRNG implementations. The bandwidth with * represents the repetition rate of the laser pulse.

Scheme	Year	Bandwidth	Generation Rate
Vacuum fluctuation	2011	120 MHz	2 Gbps (real-time)[220]
	2019	1 GHz	6.83 Gbps (real-time)[221]
	2021	3.5 GHz	18.8 Gbps (real-time)[222]
	2021	400 MHz	2.9 Gbps (real-time)[223]
	2023	10 GHz	100 Gbps[224]
Laser phase noise	2010	1 GHz	500 Mbps[225]
	2016	1 GHz	5.4 Gbps (real-time)[226]
	2014	2.5 GHz *	20 Gbps[227]
	2015	12 GHz	68 Gbps[228]
	2019	1 GHz *	8 Gbps (real-time)[229]
	2021	2.5 GHz *	10 Gbps[230]
	2023	20 GHz	218 Gbps[231]
ASE	2010	7.5 GHz	12.5 Gbps[232]
	2011	15 GHz	20 Gbps[233]
	2020	5 GHz	118.375 Gbps[234]

bers that are uniform distributed. Therefore, a transformation from the uniform distributed random numbers to the Gaussian distributed random numbers would be a mandatory step. There are several ways of transforming the uniform distributed random numbers into the Gaussian distributed random numbers. For example, the CDF Inversion Method[272], Box-Muller Transform[273], Central Limit Theorem[274], Piecewise Linear Approximation using Triangular Distributions[275], Rejection methods[276] and so on. Typically, the Box-Muller Transform is one of the most widely used methods. It is based on the independent samples, U_1 and U_2, chosen from the uniform distribution on the unit interval $(0,1)$. Let

$$\begin{aligned} Z_0 &= \sqrt{-2lnU_1}\, cos(2\pi U_2), \\ Z_1 &= \sqrt{-2lnU_1}\, sin(2\pi U_2). \end{aligned} \tag{40}$$

Then Z_0 and Z_1 are independent random variables with a standard normal distribution. A discrete-modulated CV-QKD system can naturally avoid this issue, where the only step using continuous-variable random numbers, the Gaussian modulation, is replaced.

B. Transmitter

The function of the transmitter of a CV-QKD system is to prepare the modulated quantum signals and the classical auxiliary signals such as the LO and pilot tones. It usually consists of the laser source, the modulation module and the monitoring module.

1. Source

Laser source usually requires the narrow linewidth and low relative intensity noise to achieve high-performance and stability. Among the wide range of lasers, fiber lasers are the most commonly used, which is advanced in monochromaticity, directionality, and stability. The distributed feedback lasers and external cavity lasers are also adopted in some systems[277–280].

The laser source can be pulsed or continuous-wave form. The pulsed laser source usually consists of a laser diode with amplitude modulators, while the continuous-wave laser source only requires a narrow-linewidth laser diode. In the early stage of CV-QKD system, pulsed light is naturally used since the separation in time domain provides a clear understanding of different quantum states. Moreover, it is suitable for time division multiplexing to suppress the crosstalk between quantum and classical auxiliary signals. Since the necessary classical auxiliary signal is around 10^4 to 10^8 photons per pulse, to eliminate the leakage from the classical pulse to quantum signal pulse, the required extinction ratio is normally about 80 dB or more. Usually a conventional amplitude modulators has an extinction ratio less than 40 dB, therefore, two or more cascaded amplitude modulators are required for pulse generation[281].

As the system repetition frequency increases for higher performance, it is harder to achieve pulses with high extinction ratio and high repetition frequency simultaneously, resulting in the demand of directly using continous-wave laser source. Meanwhile, the local LO system reduces the crosstalk between quantum and classical signals, which relaxes the requirement of the extremely high isolation. Therefore, the continous-wave laser source without the complex cascaded amplitude modulators is widely used in the recent local LO systems[143,282–286]. However, for an accurate interference with signals from two different lasers, the laser diodes in an local LO system require narrower linewidth. In addition, a laser locking module can be optionally used to reduce the phase noise.

2. Modulation

The light output from the laser source is then modulated to encode the quantum information, generate the classical signals such as frame signals, and the LO or reference signal, which are combined at the output of the transmitter through various multiplexing techniques. In this part, we will detail the modulation process in three steps, encoding information, controlling the average power of quantum signal and adding classical auxiliary signals.

For encoding information, two mainstream methods are adopted as shown in Fig. 10 (a) and (b). One is the combination of a phase modulator and an amplitude modulator, and the other is the use of an in-phase quadrature (IQ) modulator. The structure of the modulators used here is detailed in Fig. 10 (c), (d) and (e). The modulation format of a CV-QKD system includes Gaussian modulation and discrete modulation, as shown in Fig. 11 (a) and (b). Both of them require displacements of coherent states on two quadratures of the phase space. An exception is the unidimensional modulation shown in Fig.11 (c), which only requires the modulation

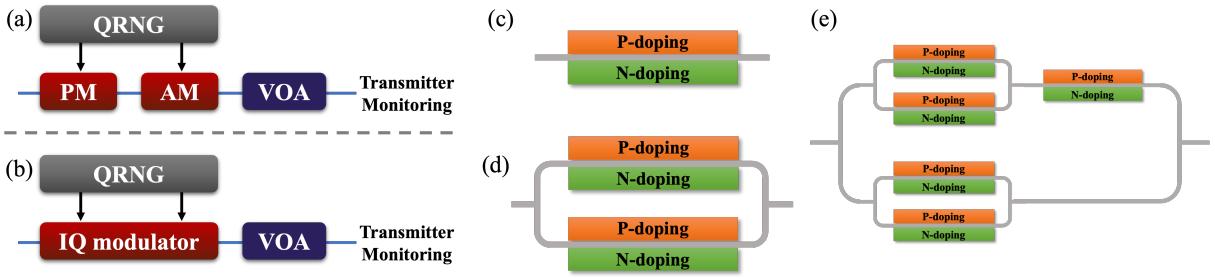

FIG. 10. (a) The structure of modulation module for quantum signals. QRNG is used for providing modulation data, AM and PM is used to load the modulation information, and variable optical attenuator is used to adjust the intensity of quantum signal to quantum level. (b) The modulation module using IQ modulator. (c) A simple structure of the phase modulator, which consists of a PIN junction. (d) The structure of the amplitude modulator, which consists of two phase modulators. (e) The structure of the IQ modulator, with two amplitude modulators and one phase modulator.

of one quadrature and can be realized with a single amplitude modulator. In addition, the Phase Shift Keying (PSK) discrete-modulation only requires a phase modulator for encoding, as shown in Fig. 11 (d).

In fact, using the phase and amplitude modulators or using an IQ modulator, are the different perspectives of a two-dimensional distribution, as shown in Fig. 11 (a) and (b). Take the Gaussian modulation as an example, for an IQ modulator, if we denote I and Q as the data loaded to the in-phase and quadrature path of the IQ modulator, which corresponds to the x and p quadrature on phase space, they should obey normal distribution as

$$I \sim N(0,\sigma^2), Q \sim N(0,\sigma^2), \tag{41}$$

where σ^2 is the variance, N represents the normal distribution. For phase and amplitude modulators, the information is loaded with a polar coordinate system, therefore requires the Rayleigh distributed amplitude,

$$f(x,\sigma) = \frac{x}{\sigma^2} e^{-x^2/2\sigma^2}, \tag{42}$$

and the uniform distributed phase information.

We remark that, sometimes the x or p quadrature is also called basis, but it is different to the basis in single-photon protocol since the security of CV-QKD is not determined by quadrature selection. Actually, the security of a coherent state CV-QKD system is ensured by the indistinguishability of coherent states on phase space. There also exists a noval CV-QKD protocol based on the basis encoding, where the secret information is encoded on the random choices of two measurement basis, and the security against individual attack has been proved[287]. The scheme exhibits the potential to tolerate high excess noise.

For practical implementations, we remark that these two methods require different acquisition[288]. Besides that, the working parameters of the modulators should be accurately adjusted, since the imperfect modulation may increase the excess noise and open security loopholes[289].

After the encoding, one should adjust the average power of the prepared quantum states to a proper level. Although in principle, CV-QKD protocols can use the quantum states with high average power, the practical implementations always require the extremely low average power in a few photon number level, since the practical devices with limited resolution cannot measure the quantum characteristics of the high-power states. Using the variable optical attenuator with manual adjustment or automatic control is a general method to adjust the level of attenuation, as shown in Fig. 10. Further, Y. Zhang et al. used an amplitude modulator to realize the real time attenuation control. It allows one to flexibly raise the launching power of the frame signals for better SNR, and reduce the power of the quantum signals[139].

In addition, the passive-state-preparation CV-QKD without modulation modules has also been proposed, where the trans-

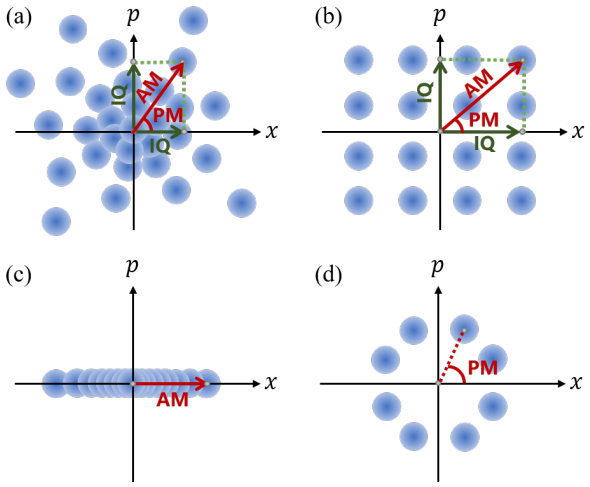

FIG. 11. (a) The Gaussian modulation format with phase and amplitude modulation or IQ modulation. The coherent states on phase space obeys a two-dimensional Gaussian distribution, where the x and p quadrature obeys independent identical Gaussian distribution. (b) The discrete-modulation format with phase and amplitude modulation or IQ modulation. Here a 16 QAM is specified. (c) The unidimensional modulation on x quadrature with only amplitude modulation. (d) The PSK modulation with only phase modulation, while the amplitude of each coherent state is equal. AM: amplitude modulator, PM: phase modulator, IQ: in-phase quadrature modulator.

mitter consists of a thermal source, beamsplitters, optical attenuators, and homodyne detectors[193,290,291].

In the earliest experimental demonstrations, the quantum signals and the LOs are transmitted separately[130]. Later, in order to avoid any polarization and phase drifts that may occur between the signal and LO over long-distance fiber transmissions, time-division multiplexing scheme was proposed to co-transmit the quantum signals and the LOs in the same fiber[132]. In another literature, B. Qi et al. also co-transmitted the quantum signals with the LOs, but adopted a scheme combining polarization and frequency-division multiplexing[292]. In later experimental demonstration, the co-transmission schemes basically adopt the combination scheme of time multiplexing and polarization multiplexing[133,136,137,139,293]. In this way, the leakage from the LOs to the quantum signals can be maximally suppressed, while maintaining a relatively simple implementation structure.

For local LO systems, though LO is generated by the receiver, a classical reference signal is still necessary for phase recovery. Early local LO systems using pulsed laser source is suitable with time division multiplexing, where the quantum signal and the classical pilot tone are alternately transmitted[141,142]. It can be combined with the polarization multiplexing to suppress the leakage of the pilot tone[294]. Towards high-speed and continuous-wave system, frequency division multiplexing of quantum signal and pilot tone is widely used[282,283,286]. Since the power of pilot tone is far lower than that of the LO, the requirement of isolation is relaxed. It can also be combined with polarization multiplexing for higher isolation[143,284].

Besides the LO or reference signal, some classical frame signals are inserted in the quantum signal sequence to provide the essential information for synchronization, phase compensation, et al.. These frame signals are usually generated by the same modulation module of quantum signals, and time-division multiplexed.

3. *Transmitter Monitoring*

A source monitor is deployed after the modulation module to evaluate Alice's real output state by detecting a fraction of the signal before entering into the quantum channel. It can be categorized into the active source monitor and the passive source monitor. As shown in Fig. 12 (a), the active source monitor adopts the optical switch for getting a part of the signal for monitor, while the passive source monitor uses a beamsplitter to divide the quantum signal for monitor, shown in Fig. 12 (b).

The monitor module can be a homodyne or heterodyne detector, which provides the statistic of the modulated coherent states, including the modulation variance, which is related to the power of the modulated signals. Besides, for Gaussian modulation, since the modulation variance corresponds to the average photon number, which is related to the optical power, an optical power meter can replace the homodyne or heterodyne detector for source monitor.

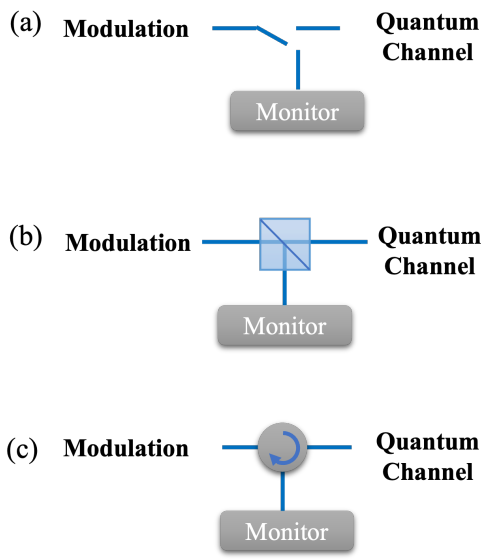

FIG. 12. (a) The active transmitter monitor. (b) The passive transmitter monitor. (c) The transmitter monitor aiming at monitoring the injected light.

Specifically, for Gaussian modulation, we can get

$$\langle \hat{n} \rangle = \frac{1}{4}(\langle x^2 \rangle + \langle p^2 \rangle) - \frac{1}{2} = \frac{1}{2}(V-1) = \frac{V_M}{2}, \tag{43}$$

where $V = V_M + 1$ is the variance of the mode, and V_M is defined as the modulation variance. The average photon number of the output mode, $\hat{n}$, can be achieved by detecting the power of the output signal, denoted as P_{out}. Each photonic has the energy of $E = h\nu$, where h is the Plank constant and ν is the frequency. Assuming N pulses are detected, where N is a sufficient large number, and the repetition frequency of the system is f_{rep}. The average photon number can be achieved by

$$\langle \hat{n} \rangle = \frac{P_{out}}{h\nu f_{rep}}. \tag{44}$$

Therefore, the modulation variance is $V_M = 2P_{out}/(h\nu f_{rep})$. If we denote the modulation variance of the electrical data as V_M^e and assume the modulator works linearly, the scale coefficient can be achieved as $c = \sqrt{V_M/V_M^e}$. Therefore, the output of the sender can be denoted by $(D_{x_{B_0}}, D_{p_{B_0}}) = c\,(D'_{x_{B_0}}, D'_{p_{B_0}})$. Here $(D'_{x_{B_0}}, D'_{p_{B_0}})$ is the electrical modulation data and $(D_{x_{B_0}}, D_{p_{B_0}})$ is the calibrated modulation data on phase space.

In this way, one can define the data of state preparation on phase space corresponding to the electrical modulation data entered into the modulation module, and the estimated average power of the output quantum states, which is a crucial step for security analysis of a practical system.

The source monitor also contributes to a tight estimation of channel parameters. In a practical system, the laser fluctuation[295], imperfect modulation[289] and other factors introduce source noise into state preparation stage[296]. It has been shown

that the secret key rate may be undermined by the source noise[163,297,298]. Traditionally, source noise is ascribed into the channel noise to calculate the secret key rate, while in practice it is controlled neither by Eve, nor by legitimate users. So, this untrusted source noise model just overestimates Eve's power and leads to an untight security bound. By real-time monitoring the modulated quantum signals, the source noise can be calibrated and removed from the channel noise, which helps to enhance the system performance.

In addition, for practical security considerations, the monitoring module of the source can help to resist the potential attacks on the system by injecting a strong light, such as the Trojan-horse attack[299], which can open a side channel for Eve. The monitoring structure is shown in Fig. 12 (c), where a circulator isolates the injected light from the components inside the transmitter, and directs it to the monitoring module, which can be a homodyne detector, or an optical power meter. The specific attack methods and countermeasures are detailed in the section of practical security.

C. Receiver

The receiver of a CV-QKD system should accurately measure the quadrature of the received state on phase space, which normally contains the monitoring, de-modulation and detection sub-modules, detailed as below.

1. *Receiver Monitoring*

The receiver monitoring module is mainly used to monitor the classical light from the channel, including the wavelength, frequency, power and amplitude of the LO in an in-line LO system, as well as the pilot tone in a local LO system[300].

Receiver monitoring is essential for an in-line LO system, since the LO is transmitted in the quantum channel, which may be manipulated by Eve, and directly participates in the homodyne or heterodyne detection. For an in-line LO system with polarization multiplexed quantum signal and LO, after the de-multiplexing of the received signal, the LO can be divided by an unbalanced beamsplitter. The stronger output is sent to the detector and the weaker one is detected by a photodiode for monitoring.

Besides that, the monitor also need to ensure that the receiver is not affected by the potential injection of a strong light. Several efficient attacking strategies for the CV-QKD system are aiming at the receiver by injecting a strong light to disturb the detection or SNU calibration process. The attacks and countermeasures are detailed in the section of practical security.

2. *De-modulation*

The de-modulation module responses for the compensation and de-multiplexing in optical path to well separate the quantum and classical signals, mainly including the polarization[301,302] and phase compensation[303–306], as well as the de-multiplexing of polarization and time. It also includes the synchronization in hardware layer[307–311].

Since the quantum signal is transmitted in single-mode fiber while the receiver is a polarization-maintaining system, the compensation of polarization is crucial for reducing the loss of quantum signals. More importantly, it can suppress the excess noise caused by the crosstalk of quantum and classical auxiliary signals in a polarization-multiplexing system. For proof-of-principle experiments, the polarization compensation is realized by a manual polarization controller, while dynamic polarization controller with feedback systems is adopted in long-term or field tests[137].

Phase noise is inevitably introduced in a CV-QKD system, caused by the phase mismatch between quantum signal and LO. Though they are co-transmitted in an in-line system, the differences in transmission paths before and after multiplexing, as well as the disturbance of fiber link, result in different phases. The local LO system is worse, since quantum signal and LO are generated separately. Generally, the phase mismatch consists of the slow-fading and fast-fading ones. The slow-fading phase noise is normally caused by the optical path difference, while the fast-fading phase noise is caused by the channel disturbance and the frequency drift between the two lasers in local LO systems. The slow-fading ones can be compensated with the inserted frame signals, such as the four-state modulated signals. While more reference signals are required for fast-fading phase compensation, such as pilot tones. The phase compensation in optical path is normally realized with a phase modulator. Specifically, for the system with GG02 protocol, phase compensation can be integrated with the phase modulator for detection basis switching.

In a pulsed CV-QKD system, a de-multiplexing operation is usually performed before the homodyne or heterodyne detection to seperate the quantum signals and LO (or pilot tone). After the polarization compensation at the beginning of the receiver, a polarization beamsplitter is used to separate the quantum and classical signals in orthogonal polarization directions. Then, for the time-division multiplexed signals, such as the quantum signal and LO, an optical delay line is adopted to align the quantum signal pulse and LO pulse for homodyne detection. In this structure, a phase modulator in the LO path realizes the basis switching and phase compensation as we mentioned before. Finally, the detection results can be used as the raw data.

The continous-wave system is different, where most of the de-multiplexing and compensation can be realized in digital domain, using the data after the detection. The architecture of the receiver is similar to the integrated coherent receiver in classical coherent optical communications, and lots of algorithms participate in the compensation and de-multiplexing process. We will detail this process in the part after detection.

Clock synchronization responses for the alignment of the sampling points at the transmitter and the receiver site. If the sampling points of the receiver are mismatched to those of the transmitter, the correlation between the modulation data and the detection data will be reduced. As for clock synchronization, there are many hardware layer solution, such as trans-

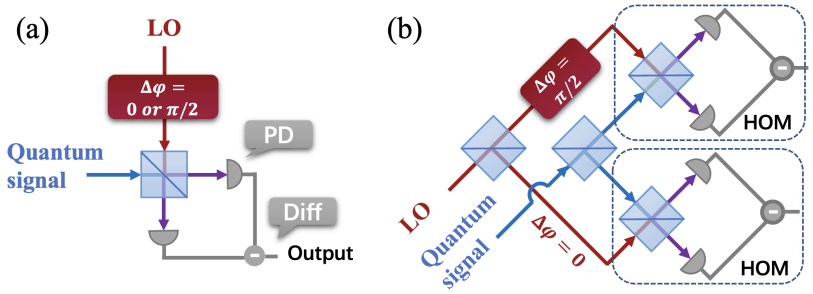

FIG. 13. The two mainstream detection strategies in CV-QKD systems. (a) The homodyne detector, where the quantum signal and local oscillator are interfered by a 50:50 coupler, then the two output signals are detected by two photodiodes, finally the output of the two photodiodes, the differential current, is output. A phase shifter is necessary to switch the detection basis between x and p for ensuring the system security. (b) The heterodyne detector, where the quantum and local oscillator are divided respectively and detected by two homodyne detectors. A phase shift of $\pi/2$ between the two local oscillators is introduced to realize the detection of x and p quadratures of the quantum signals. LO: local oscillator, PD: photodiode, Diff: differentiator and HOM: homodyne detector.

mitting in a cable[312], in a paired fiber[313], multiplexing with quantum signal in one fiber by wave-length division multiplex (WDM)[314], and distilling the synchronization signal from local oscillator. Each of the above options has its advantages and disadvantages. The electric cable is not only expensive and also instable for distant transmission. Transmitting clock signal and quantum signal in the same fiber by WDM can compensate the difference of signal arrival time but may introduce excess noise generated by WDM crosstalk. Distilling the synchronization signal from local oscillator need divide the local oscillator beam. The division of local oscillator power will decrease the maximal transmission distance or require higher gain of homodyne detection to compensate. Transmitting clock signal in another independent fiber will generate the fluctuation between quantum and clock signal.

The recent system normally adopts the clock synchronization in digital domain[315], using algorithms to realize the above requirements, which will be detailed in DSP part.

3. Detection

Homodyne detection is the basis of measuring the quantum signals in a CV-QKD system[316–327]. As shown in Fig. 13 (a), the quantum and LO signals are interfered by a 50:50 coupler, then the two output signals are detected by two photodiodes. The two branches of the photocurrent generated by the photodiodes are differentiated and output. The differential current contains the information on the quadrature of the quantum signal. A simple derivation of homodyne detection is shown as below.

We define the modes of quantum signal and LO as $\hat{a}_S$ and $\hat{a}_L$. Therefore, the output modes of after the coupler are

$$\begin{aligned}\hat{a}_1 &= \frac{1}{\sqrt{2}}(\hat{a}_S+\hat{a}_L),\\ \hat{a}_2 &= \frac{1}{\sqrt{2}}(\hat{a}_S-\hat{a}_L).\end{aligned} \tag{45}$$

Then, the photon number of the two output modes can be achieved

$$\begin{aligned}\hat{n}_1 &= \hat{a}_1^\dagger\hat{a}_1 = \frac{1}{2}(\hat{a}_S^\dagger+\hat{a}_L^\dagger)(\hat{a}_S+\hat{a}_L),\\ \hat{n}_2 &= \hat{a}_2^\dagger\hat{a}_2 = \frac{1}{2}(\hat{a}_S^\dagger-\hat{a}_L^\dagger)(\hat{a}_S-\hat{a}_L).\end{aligned} \tag{46}$$

The differential current can be written as

$$\delta I = I_1 - I_2 \propto (\hat{n}_1-\hat{n}_2) = (\hat{a}_S^\dagger\hat{a}_L+\hat{a}_L^\dagger\hat{a}_S). \tag{47}$$

The strong LO can be seen as a classical light, written as

$$\hat{a}_L = |a_L|e^{i\theta}. \tag{48}$$

Therefore, one can get

$$\delta I \propto |a_L|(\hat{a}_S^\dagger e^{i\theta}+\hat{a}_S e^{-i\theta}). \tag{49}$$

We get the measurement result of x quadrature when $\theta=0$, where

$$\delta I(\theta=0) \propto |a_L|(\hat{a}_S^\dagger+\hat{a}_S) \propto \hat{x}, \tag{50}$$

and p quadrature when $\theta=\pi/2$,

$$\delta I(\theta=\pi/2) \propto i|a_L|(\hat{a}_S^\dagger-\hat{a}_S) \propto \hat{p}. \tag{51}$$

A homodyne detector can only measure one quadrature at a time but the security analysis requires detection of both quadratures. Therefore a phase modulator is deployed on the path of the LO, for switching the phase difference between the LO and quantum signal between 0 and $\pi/2$ randomly. This can realize the function of switching the detection basis, satisfying the requirement of getting the statistic data of both quadratures. Further, by combining two homodyne detector together, a heterodyne detector which enables the detection of both quadratures of the quantum signal is realized, as shown in Fig. 13 (b). It can simultaneously detect the x and p quadrature of a quantum signal since a phase shift of $\pi/2$ is introduced to one path of the LO. To avoid the low frequency noise, the heterodyne detection can also be realized by moving the quantum signal to the intermediate band in frequency

TABLE VII. A comparison between BHDs. Here, BW means the 3 dB bandwidth, QCNR means quantum to classical noise ratio, the and CMRR means the common mode rejection ratio.

	Year	BW	QCNR	CMRR
Bulk	2011	104 MHz	13 dB	46 dB[321]
	2011	100 MHz	13 dB	52.4 dB[322]
	2013	300 MHz	14 dB	54 dB[324]
	2015	5 MHz	37 dB	75.2 dB[328]
	2018	40 MHz	14.5 dB	//[329]
	2018	1.2 GHz	18.5 dB	57.9 dB[326]
On chip	2019	1-10 MHz	5 dB	//[138]
	2021	750 MHz	26.82 dB	40 dB[330]
	2021	2.6 GHz	21.1dB	50 dB[331]
	2021	1.5 GHz	28 dB	80 dB[332]
	2021	1.7 GHz	14 dB	52 dB[333]
	2023	//	19.42 dB	86.9 dB[334]

domain[143,188,282–284,286]. Both quadratures can be simultaneously distilled with down conversion in analog domain or digitally, while a full architecture is still required to avoid the image band issue. Here we remark that the heterodyne detector in CV-QKD represents the dual-homodyne structure, which has different meanings of that in coherent optical communications.

The homodyne detector can be divided into two types, with direct output and the integral output[329,334,335]. The integral-output homodyne detector is widely used in the early CV-QKD system since the signal and LO are both pulsed light. Therefore, it requires the integration of each laser pulse and output a field quadrature signal. At this stage, the homodyne detector is heading towards the high bandwidth, balance, and common mode rejection ratio[323,328,336–338]. Later, since the CV-QKD system adopts the continuous-wave light, the direct-output homodyne detector is enough, which has less requirement on the balance, and it is easier to realize a high-speed homodyne detection.

The bandwidth, detection efficiency, electronic noise and quantum to classical noise ratio (QCNR) are the key parameters of homodyne detectors. The bandwidth of the receiver directly affects the settings of the system in frequency domain, including the multiplexing and processing of the quantum and phase reference signals. The detection efficiency is another crucial parameter of the practical homodyne detector, corresponding to the detector parameter η in Eq. (28). It is limited by the photodiodes, and the balance of the two arms of the homodyne detectors. The electronic noise of the practical homodyne detector is vital in the CV-QKD systems, which corresponds to v_{ele} in Eq. (28). Since the power of the quantum signal is extremely small, a high electronic noise can significantly reduce the SNR, therefore resulting in a low-quality detection. The last parameter that are normally used to describe the homodyne detector is the quantum to classical noise ratio (QCNR). The QCNR demonstrate how good the weak quantum signals can be amplified while suppressing the electronic noise. The general requirement for the QCNR is that it should be at least 10 dB. We also list some reported homodyne detectors with their parameters in Table. VII, common-mode rejection ratio is introduced to reflect the balance of the detector.

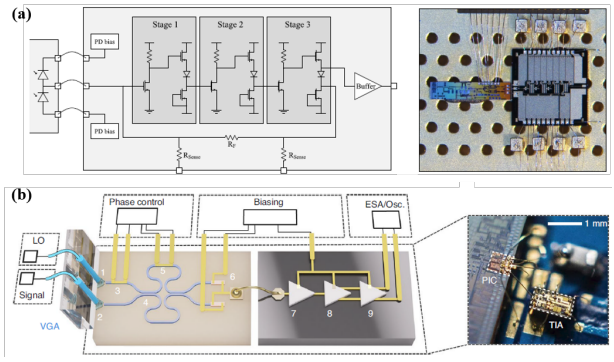

FIG. 14. (a) The chip-based homodyne detector for beyond 20 GHz shot-noise-limited measurements. From C. Bruynsteen et al.[332]. (b) The chip-based homodyne detector for 9 GHz measurement of squeezed light. From J. Tasker et al.[333]. (a) Reproduced with permission from Optica 8, 1146 (2021). Copyright 2021 Optica Publishing Group. (b) Reproduced with permission from Nat. Photonics 15, 11 (2021). Copyright 2021 Springer Nature Limited.

The homodyne detector can be integrated on chip driven by the photonics integrated circuit techniques, as shown in Fig. 14. The highly balanced photonics circuit, photodiode with high detection efficiency, and the low noise transimpedance amplifier are the core issues. The 3 dB bandwidth of the chip-based homodyne detector can break 1.5 GHz, the clearance between the shot noise and the electronic noise can reach 28 dB, and the common-mode rejection ratio can reach 80 dB[271]. These meaningful parameters show that the homodyne detectors on chip have achieved high-speed, low electronic noise and excellent balance.

D. Shot noise unit calibration

As we mentioned before, the electrical modulation data is transformed to the phase space based on the source monitoring. Correspondingly, the electrical detection data also requires the transformation, which is realized by SNU calibration.

SNU is defined as the variance of the shot noise. In security analysis, the variance of the quantum fluctuation on phase space is defined as unity, while in a practical system, this fluctuation can be measured and recorded as electrical signals, simply by measuring the vacuum. With enough electrical de-

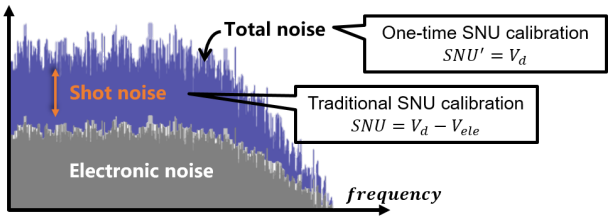

FIG. 15. The power density of measurement. The electronic noise and the superposition of electronic and shot noise (vacuum noise) can be achieved in practical measurements. V_d: the variance of total noise, V_{ele}: the variance of the electronic noise. SNU: shot noise unit, which is the variance of the shot noise.

tection data of vacuum state, the variance of the shot noise measurement result can be estimated in a practical system and used for the normalization of the detection data of coherent states. In this way, the electrical detection output can be transformed to the data for security analysis. Therefore, accurate SNU calibration is crucial for the security of the CV-QKD system[335].

However, SNU calibration of a practical system needs to consider the additive electronic noise, which is introduced inevitably by a practical measurement, shown in Fig. 15. Usually, the variance of electronic noise, V_{ele}, can be calibrated independently. Therefore, SNU can be achieved in a practical CV-QKD system with twice measurements. As shown in Fig. 16 (a), the electronic noise in the CV-QKD systems can be directly calibrated as follows: fisrt, turn on the electric power of the homodyne detector, and cut off the two optical input ports, the measured variance is the raw electronic noise. Then, total noise can be calibrated with LO on, shown in Fig. 16 (b). The difference of the two variables is the SNU, denoted as u.

Specifically, considering the limited detection efficiency η_d, the detection results of the quantum signal before normalization can be written as

$$X_{out} = AX_{LO}(\sqrt{\eta_d}\hat{x}_s + \sqrt{1-\eta_d}\hat{x}_v) + X_{ele}. \tag{52}$$

Here, $\hat{x}_s$ $\hat{x}_v$ and X_{ele} are the quadrature information of quantum signal, vacuum state (shot noise), and electronic noise. X_{LO} represents the effect of local oscillator, and A is the amplification coefficient of circuits. Therefore, the SNU calibrated with the method we mentioned before is $(AX_{LO})^2$. In this way,

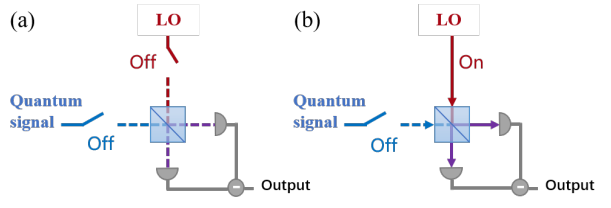

FIG. 16. The calibration of electronic noise and total noise with a practical balanced homodyne detector (BHD). (a) The calibration of electronic noise, where the signal and LO path are cut off. (b) The calibration of the total noise with LO inputted.

TABLE VIII. The SNU calibration schemes in CV-QKD systems.

Calibration	Strategy	Procedures
Traditional two-time[339]	Pre-calibration	1) Calibration of electronic noise 2) Calibration of total noise (assuming a stable SNU)
Traditional two-time[133,134]	Real-time	1) Calibration of electronic noise 2) Calibration of total noise with different LO power (monitoring the real-time LO power)
One-time[137,340]	Real time	1) Calibration of total noise with different LO power before system operation (monitoring the real-time LO power)

after normalization we can get

$$x_{out} = \frac{X_{out}}{\sqrt{u}} = (\sqrt{\eta_d}\hat{x}_s + \sqrt{1-\eta_d}\hat{x}_v) + \frac{X_{ele}}{AX_{LO}}. \tag{53}$$

Based on this normalized output, we can establish the trusted detector module detailed in Section II. The variance of the electronic noise after normalization with SNU, v_{ele}, is the variance of $X_{ele}/(AX_{LO})$. The scheme of the trusted detector is shown in Fig. 17 (a).

In fact, this SNU calibration method has been widely applied in the early experimental demonstrations[134,339] through different implementation schemes. However, the LO power and electronic noise are not constant in the practical CV-QKD operations, it tends to drift with the time or temperature changes. Thus, the SNU calibration should be performed in real-time. For example, in the Ref.[339], the SNU calibration is performed before the CV-QKD operation, which is called a pre-calibration scheme. The SNU would be calibrated through the above method, the raw data which is obtained in the later running of the CV-QKD can be normalized by using the calibrated SNU. This implementation scheme is surely fine in the proof-of-principle demonstrations, but in reality, the fading of SNU may may cause severe security issues. Therefore, monitor scheme that can trace the SNU change

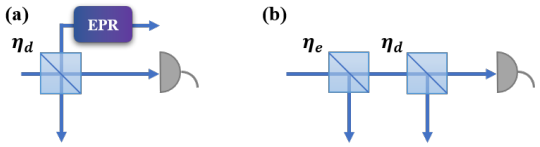

FIG. 17. The traditional trusted detector module (a) and the trusted detector module of one-time SNU calibration (b).

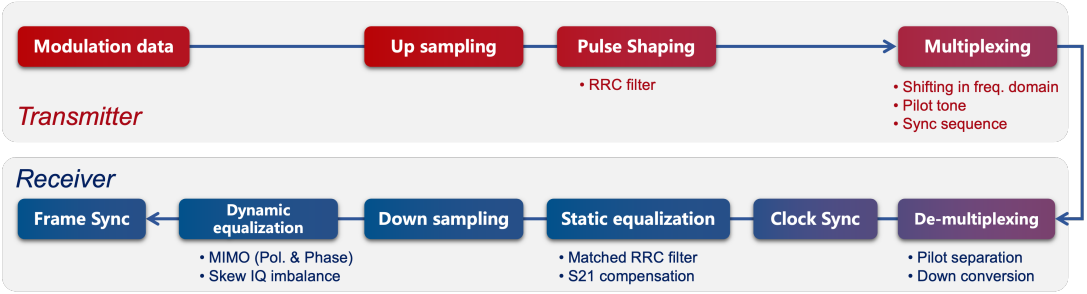

FIG. 18. The DSP routine of a CV-QKD system, which includes upsampling, pulse shaping and multiplexing in transmitter side, as well as de-multiplexing, clock synchronization (sync), static equalization, dwon sampling, dynamic equalization and frame sync in receiver side. RRC means Root-Rasied-Cosine, freq. means frequency, and Pol. means polarization.

should be applied.

The implementation scheme based on the combination of the pre-calibration scheme as well as the LO monitor scheme is adopted[133,134]. In this scheme, the pre-calibration still runs before the CV-QKD operation. Also, before the system running, Bob will measure a series of SNU according to different powers of the LO transmitted from Alice. These data would later form a linear relation between the optical power and the SNU. During the CV-QKD system operating, a small portion of the LO is separated and constantly measured. Then, based on the obtained optical power, Bob adjusts the SNU according to the linear relation that has been formed previously. The raw data obtained from the CV-QKD operation can be then normalized by the modified SNU.

Although the conventional SNU calibration method has been applied in many experimental demonstrations, there are still several issues that are unsolved. First, the SNU calibration process is rather complicated, two steps are required at the optical paths. What's more, with the deeper studies on the practical security of CV-QKD, it makes us realize that the existing SNU calibration method can have security loopholes.

Recently, the SNU calibration method has been improved to meet the needs of the practical implementations of CV-QKD systems, and to reduce the complexity of SNU calibration. An improved security analysis with one-time SNU calibration method has been proposed by redefining SNU as

$$u' = V_d = u + V_{ele}. \tag{54}$$

In this way, SNU can be achieved by just measuring the total noise, which significantly simplifies the procedure[340,343–345]. Therefore, we get

$$u' = (AX_{LO})^2 + V_{ele}. \tag{55}$$

Here, V_{ele} is the variance of the electronic noise before normalization. Further, we can get the output after the normalization with SNU' as $x'_{out} = X_{out}/\sqrt{u'}$. If we use another vacuum state to represent the electronic noise as $X_{ele} = \sqrt{V_{ele}}\hat{x}'_v$, then we can get

$$\begin{aligned} x'_{out} &= \frac{AX_{LO}}{\sqrt{(AX_{LO})^2 + V_{ele}}}(\sqrt{\eta_d}\hat{x}_s + \sqrt{1-\eta_d}\hat{x}_v) \\ &\quad + \sqrt{\frac{V_{ele}}{(AX_{LO})^2 + V_{ele}}}\hat{x}'_v \\ &= \sqrt{\eta_e}(\sqrt{\eta_d}\hat{x}_s + \sqrt{1-\eta_d}\hat{x}_v) + \sqrt{1-\eta_e}\hat{x}'_v, \end{aligned} \tag{56}$$

where

$$\eta_e = \frac{(AX_{LO})^2}{(AX_{LO})^2 + V_{ele}} = \frac{1}{1+\nu_{ele}}. \tag{57}$$

This means the imperfect detector scheme in security analysis can be built with two beam splitters, one represents the detection efficiency, the other one represents the electronic noise, as shown in Fig. 17 (b). The beamsplitters represent the electronic noise and the detection efficiency can be can be exchanged in order. Note that, since electronic noise is not estimated in one-time SNU calibration, the output mode of the beamsplitter representing the electronic noise cannot be seen as trusted. This means the loss introduced by electronic noise is untrusted, which is the reason that the performance of the protocol with one-time SNU calibration is slightly lower than that using the traditional calibration method[340].

With this novel SNU calibration method, it is possible to achieve a real-time SNU calibration, since we only need to monitor the power of the split LO, without the demand of constantly measuring the electronic noise to finish the calibration procedure. Several experimental demonstrations[137,340] have successfully adopted this SNU calibration methods. A conclusion of the SNU calibration methods in CV-QKD systems is shown in Table VIII.

E. Digital signal processing

For the early systems, DSP is mainly used for the compensation in optical layer, such as providing the feedback information for phase and polarization control. Later in the high-speed local LO systems, the DSP is gradually becoming widely used, which is applied to the transmitter and re-

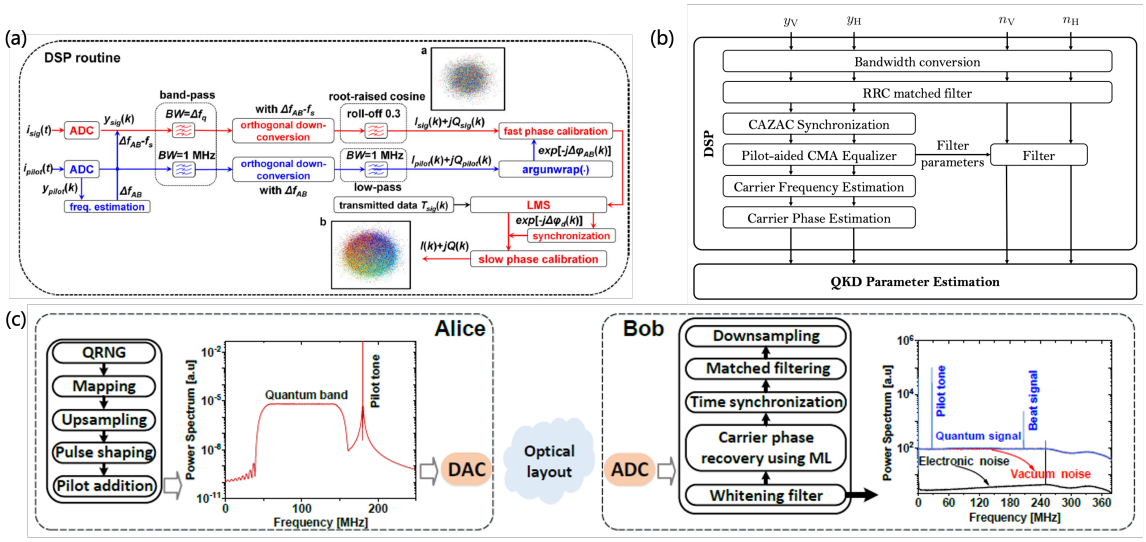

FIG. 19. The state-of-the-art digital signal processing routines of different local LO CV-QKD systems. (a) The routine of a Gaussian modulated system with polarization and frequency division multiplexing of quantum and pilot signals[143]. (b) The routine of a discrete modulated dual-polarization system where the polarization compensation is finished digitally[145]. (c) The routine of a Gaussian modulated system with frequency division multiplexing of quantum and pilot signals. Machine learning (ML) is used for high-quality phase compensation with a wide range of pilot signal-to-noise ratios[341,342]. (a) H. Wang et al., Commun. Phys., 5, 162, 2022; licensed under a Creative Commons Attribution (CC BY) license. (b) F. Roumestan et al., arXiv, 2207.11702, 2022; licensed under a Creative Commons Attribution (CC BY) license. (c) H. Chin et al., npj Quantum Inf., 7, 20, 2021; licensed under a Creative Commons Attribution (CC BY) license.

ceiver, including the clock synchronization, the static equalization, the dynamic equalization and the frame synchronization. The ultimate purpose of DSP in a CV-QKD system is to maximize the data correlation between the transmitter and receiver, which is consistent with the traditional optical communication algorithm to improve SNR. Therefore, CV-QKD system can widely use the algorithms in classical optical communications, and finally form the current routine, as shown in Fig. 18.

At the transmitter site, for raising the accuracy of the modulation, upsampling is performed before the Root-Raised-Cosine (RRC) pulse shaping[346]. Then, the pulse shaping of the quantum signal is processed to reduce the correlation between each quantum signal and satisfying the definition of a quantum pulse in a CV-QKD protocol. Practically, the signal pulse should be bounded in frequency domain so that the modulation and detection with limited bandwidth will not affect the shape of the signal in time domain. But, this will result in the infinite expansion in time domain. The mostly used solution is the RRC filter, where the integration of each two quantum signal pulse is 0 in time domain while the frequency band is limited, which both satisfies the requirements of the temporal mode of a CV-QKD protocol and the practical implementation. After that, the quantum signal is digitally shifted in frequency domain at the transmitter site, and the pilot tone for phase reference is added. Also, for frame synchronization, a Const Amplitude Zero Auto-Corelation (CAZAC) sequence is added at the beginning of each frame. The widely used CAZAC sequence is the Zadoff-Chu sequence.

For the receiver, the frequency division multiplexed quantum and pilot signal are firstly separated from the output of the detection data, then the quantum signals are down converted to the baseband corresponding to the frequency shift at the transmitter. Secondly, clock synchronization is processed, which is a digital alternative to the hardware solution mentioned before. Subsequently, the static equalization algorithms are performed to compensate the impairments, including the IQ imbalance compensation and S21 compensation, and to recover the signal pulse with matched RRC filter. Down-sampling at the best sampling point is then performed to achieve the information with the best SNR. Then, the dynamic equalization is processed to compensate the phase and polarization mismatch, normally using Multiple-Input Multiple-Output (MIMO) algorithms[303–305,347–350]. Finally, frame synchronization is performed to align the beginning of the modulation and detection data. The final output of the DSP is treated as the raw data, which is then sent to the post-processing process.

The order of the DSP steps can be exchanged for the linearity of the algorithms. The coefficients in DSP is normally adjusted dynamically with the system situation for better performance, especially in long-distance or high-noise scene. For this purpose, machine learning is recently introduced to achieve consistently excellent phase estimation under a wide range of pilot SNR[341,342]. The compatibility with classical coherent optical algorithms significantly promotes the development of CV-QKD, which provides a large number of tools and experience when developing towards high speed and long distance.

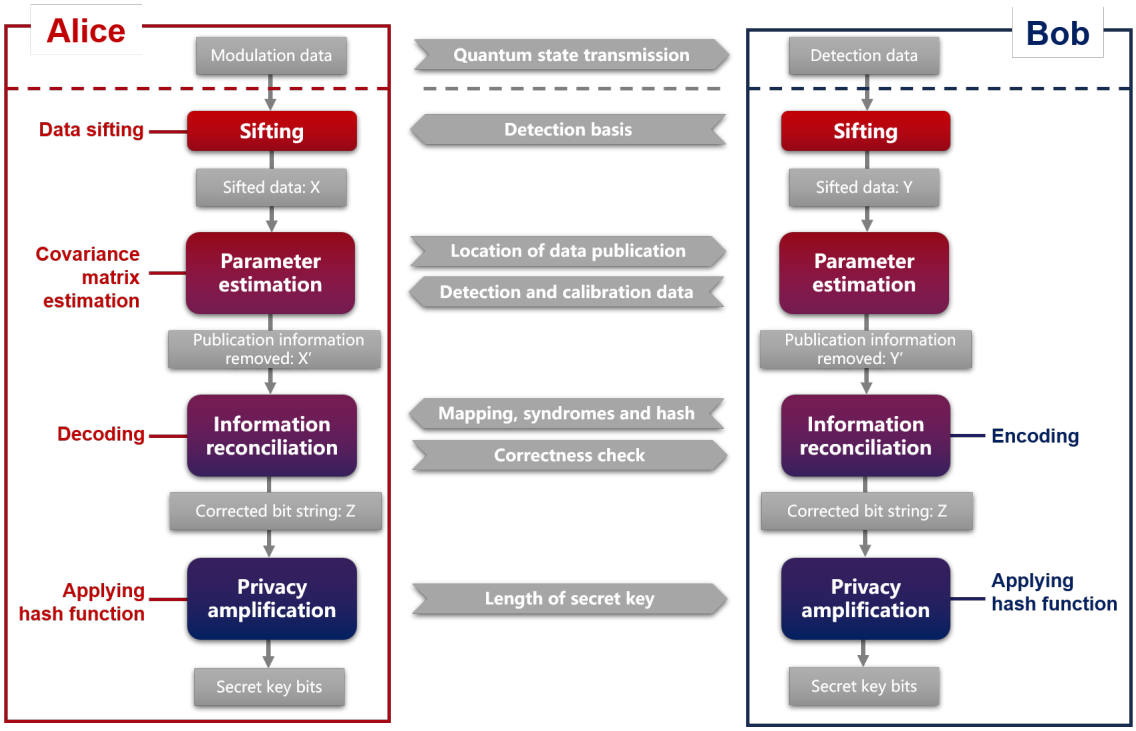

FIG. 20. The postprocessing steps in CV-QKD systems, where reverse reconciliation is adopted. Before postprocessing, Alice and Bob establish correlation by means of modulation, transmission and detection of quantum states. They then process sifting, parameter estimation, information reconciliation and privacy amplification to obtain the final secret key bits.

F. Postprocessing

The quantum stage is followed by classical data processing steps (normally called postprocessing) as is illustrated in Fig. 20, which includes four steps: base sifting, information reconciliation, parameter estimation, and privacy amplification[351–353]. For this purpose, Alice and Bob use an authenticated channel on which Eve cannot modify the communicated messages but can learn their content. Also, after the steps in postprocessing process, Alice and Bob will perform verification to ensure that the step is successful processed[354].

1. *Sifting*

Base sifting is required for systems with homodyne detection or squeezed states, where only one quadrature can used for each measurement. Bob announces the detection basis after a round, and Alice save the corresponding quadrature data. Further developments of CV-QKD systems such as the heterodyne detection scheme can save the data of both quadratures, resulting in a system without sifting. The procedure is significantly simplified since the switching and sifting of detection basis is removed.

2. *Parameter estimation*

The parameter estimation requires Alice and Bob to estimate the security parameters of the system for getting the secret key rate, based on the modulation and detection data. Take the Gaussian modulated CV-QKD system as an example, the key point is to obtain the covariance matrix we detailed in Eq. (21). This requires firstly converting the electrical data to the information on phase space in a PM scheme (detailed in transmitter monitoring and SNU calibration), and then the conversion between a PM scheme and EB scheme. Specifically, we denote the modulation data as $(D_{x_{B_0}}, D_{p_{B_0}})$ and the normalized detection data as (D_{x_B}, D_{p_B}). For EB scheme, the sender performs heterodyne detection on one mode of the EPR state. If the detection results is (x_{A_x}, p_{A_p}), the other mode B_0 is projected onto a Gaussian state with

$$(x_{B_0}, p_{B_0}) = \sqrt{2\frac{V-1}{V+1}}(x_{A_x}, p_{A_p}). \tag{58}$$

This means (x_{B_0}, p_{B_0}) and (x_{A_x}, p_{A_p}) has a linear transformation relationship. Note that, here the x and p quadrature corresponds to the modes after a 50:50 beamsplitter, where

$$\begin{aligned} A_x &= \frac{1}{\sqrt{2}}A + \frac{1}{\sqrt{2}}N, \\ A_p &= \frac{1}{\sqrt{2}}A - \frac{1}{\sqrt{2}}N. \end{aligned} \tag{59}$$

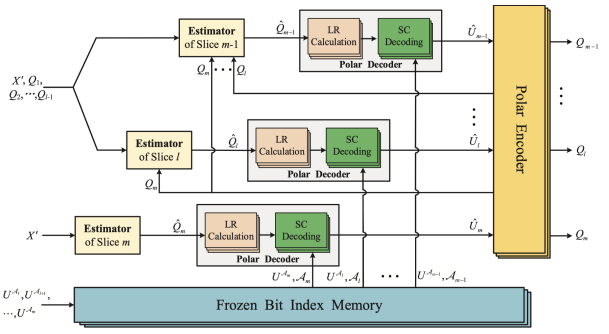

FIG. 21. The slice reconciliation in CV-QKD, where the information are sliced. From X. Wen et al.[355]. X. Wen et al., Entropy, 23, 1317, 2021; licensed under a Creative Commons Attribution (CC BY) license.

Here, A is one mode of the EPR state, N is the mode of vacuum state. A_x and A_p are the two modes after the beamsplitter. (x_{A_x}, p_{A_p}) are the x and p quadrature of A_x and A_p respectively. Therefore the calibrated data $(D_{x_{B_0}}, D_{p_{B_0}})$ can be converted to $(D_{x_{A_x}}, D_{p_{A_p}})$. With $(D_{x_{A_x}}, D_{p_{A_p}})$ and (D_{x_B}, D_{p_B}), the covariance and variance of x_{A_x}, p_{A_p}, x_B and p_B can be estimated. Since mode A_x and A_p are symmetric, the covariance and variance of x_A, p_A, x_B and p_B can be further estimated, which results in the covariance matrix γ_{AB}.

Further, for a physical existed convariance matrix, the variance of mode B can be expressed as below

$$V_B = TV_M + \xi + 1 = T(V_M + \varepsilon) + 1, \tag{60}$$

where T and ε are the two parameters ralated to the system security, estimated from the modulation and detection data.

Based on the security analysis with analytical solution we detailed in Section II, the secret key rate can be calculated. For a fiber channel, the loss and noise corresponds to the physical meanings of T and ε, which can be used for simulating the system performance.

The estimation above is based on the modulation and detection data with infinite size. However, in the practical CV-QKD systems, the length of the data should be limited. The finite-size data length leads to a fluctuation of the estimated parameter. The secret key rate under the finite-size analysis is

$$K = \frac{n}{N}[\beta I_{AB} - \chi_{BE}^{\varepsilon_{PE}} - \Delta(n)]. \tag{61}$$

Here, n/N represents the proportion of the preserved data, since part of the data, $m = N - n$, is publicized for parameter estimation. $\chi_{BE}^{\varepsilon_{PE}}$ is the Holevo bound considering the effect of finite size, and the probability that the expression is wrong is ε_{PE}, meaning that the true parameters lie within a certain confidence interval around the estimated channel parameters.

The estimation of $\chi_{BE}^{\varepsilon_{PE}}$ is based on the parameters, t_{min} and σ_{max}^2, which lead to the worst-case secret key rate. Here, t_{min} means the minimum square root of the channel transmittance, and σ_{max}^2 means the maximum of the variance of noise. Specifically,

$$\begin{aligned} t_{min} &\approx \sqrt{T} - z_{\varepsilon_{PE}/2}\sqrt{\frac{1+T\varepsilon}{mV_M}}, \\ \sigma_{max}^2 &\approx 1 + T\varepsilon + z_{\varepsilon_{PE}/2}\frac{(1+T\varepsilon)\sqrt{2}}{\sqrt{m}}. \end{aligned} \tag{62}$$

Here, $z_{\varepsilon_{PE}/2}$ should satisfy

$$1 - erf(z_{\varepsilon_{PE}/2}/\sqrt{2})/2 = \varepsilon_{PE}/2, \tag{63}$$

where erf is the error function.

$\Delta(n)$ is related to the security of privacy amplification, which can be calculated as

$$\Delta(n) = (2dimH_X + 3)\sqrt{\frac{log_2(2/\overline{\varepsilon})}{n}} + \frac{2}{n}log_2(1/\varepsilon_{PA}). \tag{64}$$

Here, H_X corresponds to the Hilbert space of the raw key, $\overline{\varepsilon}$ is a smoothing parameter, ε_{PA} is the failure probability[356].

3. *Information reconciliation*

Information reconciliation is an essential part of CV-QKD postprocessing, which makes sure that the transmitter and receiver share a same bit string. It consists of two parts, mapping the quadrature results to several bits, and error correction. The reconciliation in practical systems requires the public transmission of part of the information, therefore causes the loss of the secret information, leading to the efficiency lower than 100 %, which can be written as β,

$$\beta = \frac{H(X) - leak}{I_{AB}}. \tag{65}$$

Here, $H(X)$ is the Shannon information of the target bit string, $leak$ represents the information leakage during the public transmission (usually the syndrome), and I_{AB} is the mutual information between Alice and Bob. The efficiency of information reconciliation plays a crucial role in the final system's secret key rate and the maximal transmission distance, which is seriously affected by the reconciliation strategy.

The early reconciliation strategy corrects the detection data to make it consistent with the modulation data, so called the direct reconciliation[106]. However, the system cannot go beyond 3 dB loss since the potentially leaked information is larger than the information can be utilized be the receiver, which corresponds to the 15 km fiber transmission distance. Aiming at this problem, reverse reconciliation is proposed, where the modulation data is corrected to match the detection data. This enables the system to break the 3 dB limit, making reverse reconciliation the most common information reconciliation strategy in CV-QKD system. The main parameters of the information reconciliation in a CV-QKD system includes the reconciliation efficiency, the frame error rate, the throughput and the SNR range. Different approaches have been explored to increase the reconciliation efficiency for a

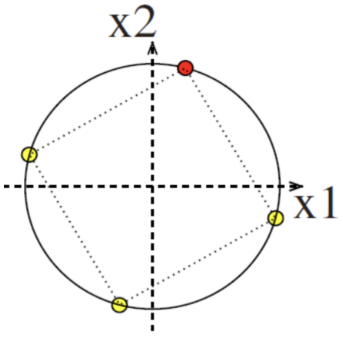

FIG. 22. The multidimensional reconciliation in CV-QKD, where the information are mapped to the sphere, which can be well separated and the symmetry is preserved. From A. Leverrier et al.[131]. Reproduced with permission from Phys. Rev. A 77, 042325 (2008). Copyright 2008 American Physical Society.

Gaussian modulation, especially in the regime of a low SNR, detailed in Table IX.

Usually the detection data is converted to discrete format first, then the error correction code for discrete data is used. A first approach is the slice reconciliation using multilevel coding and multistage decoding, as shown in Fig. 21. It is suitable for the detection signal with large SNR, normally more than 0 dB. In principle, this method can extract more than 1 bit of information per pulse. When slice reconciliation is used, the SNR of each layer of data is different, so different error correction codes need to be used for subsequent error correction steps, such as the LDPC code or the Polar code.

The other method called multidimensional reconciliation was proposed to be employed for low SNRs, i.e., below 0 dB[131,368], which reduces the Gaussian variables reconciliation problem to the discrete variable channel coding problem, shown in Fig. 22. It is suitable for the SNR lower than 0, even to -26 dB, which is the crucial technique for a long-distance CV-QKD system. The multidimensional reconciliation can be combined with the LDPC code or the other codes such as the Raptor codes[369]. The final reconciliation efficiency one obtains with such a scheme depends on two things: The intrinsic efficiency of the error correcting code used on the virtual channel on the Binary Input Additive White-Gaussian-Noise Channel (BIAWGNC). The quality of the approximation between the virtual channel and the BIAWGNC. One can therefore improve the reconciliation efficiency based on these two points.

In a long distance system, where the SNR is low, LDPC code is usually used[370–375]. The graphical representation of typical multi-edge-type LDPC code is shown in Fig. 23. Towards the practical application, the rate adaptive error correction is proposed to support the system with fading SNR[376–378]. In addition, to raise the utilization rate of the raw data, exchanging the order of parameter estimation and reconciliation is proposed. One can process the parameter estimation after the error correction. In this way, the abandoned data for parameter estimation can be reduced.

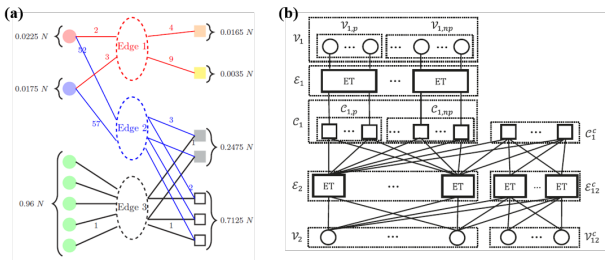

FIG. 23. The graphical representation of typical MET-LDPC. (a) from H. Mani et al.[366]. (b) from S. Jeong et al.[367]. (a) Reproduced with permission from Phys. Rev. A 103, 062419 (2021). Copyright 2021 American Physical Society. (b) S. Jeong, npj Quantum Inf, 8, 6, 2022; licensed under a Creative Commons Attribution (CC BY) license.

4. *Privacy amplification*

The output of the error correction is a same bit string between Alice and Bob, which can be denoted as K_n with n bits. Privacy amplification is finally processed to realize the distillation of secret key, of which the requirements are consistent between CV-QKD and DV-QKD. The initial proposed method is aiming at the case of asymptotic limit[379], after that, the leftover hashing is used which extends the it to the finite-size case[380]. We denote this operation as G, which is a universal hash function mapping the bit string with length N to L. If the mutual information between eavesdropper and K_n is known, a proper privacy amplification can make the eavesdropper's knowledge on the final secret key, $K_l = G(K_n)$, close to 0. For practical implementation, the speed of privacy amplification is crucial[381,382].

The most common method is using Toeplitz matrix, which can be written as

$$\gamma_{Toepliz} = \begin{pmatrix} t_0 & t_n & t_{n+1} & \cdots & t_{2n-2} \\ t_1 & t_0 & t_n & \cdots & \cdots \\ t_2 & t_1 & \cdots & t_n & t_{n+1} \\ \cdots & \cdots & t_1 & t_0 & t_n \\ t_{n-1} & \cdots & t_2 & t_1 & t_0 \end{pmatrix} \tag{66}$$

The elements on the main diagonal of the Toplitz matrix are equal, and the elements on the lines parallel to the main diagonal are also equal. In this way, a Toeplitz matrix can be easily constructed. With the calculated secret key rate after parameter estimation, the length of the secret key bits can be distilled is known. Assuming the length of K'is L' and the length of K is L, G can be a L $\times$ L' Toeplitz matrix.

IV. MAINSTREAM IMPLEMENTATIONS

The main purpose of the early CV-QKD systems is to demonstrate the feasibility of the Gaussian modulation and shot-noise limited homodyne detection[130]. After that, the enhancement of system performance begins. The efficient error correction successfully supports the long distance systems, from 80 km and up to 202 km. Meanwhile, different system

TABLE IX. The reconciliation methods and performance in CV-QKD systems.

Reference	Year	Method	SNR(dB)	Reconciliation efficiency	FER
V. Assche et al.[351]	2004	Slice, Turbo	-	-	-
J. Lodewyck et al.[132]	2007	Slice, LDPC	-	88.7%	-
P. Jouguet et al.[357]	2011	MD, LDPC	0.4, -7.93, -11.25, -15.38, -18.39, -21.4	93.6%, 93.1%, 95.8%, 96.9%, 96.6%, 95.9%	-
P. Jouguet et al.[358]	2014	Slice, LDPC	0, 4.77, 7.09, 11.63, 18.2	94.2%, 94.1%, 94.40%, 95.80%, 94.8%	-
Z. Bai et al.[359]	2017	Slice, LDPC	0, 4.77	95.02%, 95.26%	-
X. Wang et al.[360]	2018	MD, LDPC	-15.24	96.46%	-
M. Milicevic et al.[361]	2018	MD, LDPC	-15.47, -7.93	99.0%, 93.0%	0.883, 0.04
S. Zhao et al.[362]	2018	MD, Polar	-0.46, -0.97, -1.55	81%, 88.4%, 97.9%	0.013, 0.019, 0.04
C. Zhou et al.[363]	2019	MD, Raptor	0, -4, -8, -12, -16, -20	95.0%, 95.0%, ∼96.0%, ∼96.0%, ∼97.0%, 98.0%	-
Y. Li et al.[364]	2020	MD, LDPC	-7.93, -11.19, -15.23	92.9% , 94.6% , 93.8%	0.17, 0.25, 0.32
S. Yang et al.[365]	2020	Slice, LDPC	0, 4.77	93.0%, 93.06%	0.14, 0.09
Y. Zhang et al.[139]	2020	MD, Raptor	-26.38	98%	0.9
		MD, LDPC	-15.11, -7.43, -3.35	96.0%, 96.0%, 96.0%	0.1, 0.1, 0.1
		Slice, Polar	0.3, 4.48	95%, 95%	0.5, 0.5
H. Mani et al.[366]	2021	MD, LDPC	-8.16, -11.34, -15.46, -18.45	97.5%, 97.8%, 98.8%, 97.7%	-
S. Jeong et al.[367]	2022	MD, LDPC	-15.25, -14.25, -14.2	-	-

strctures are proposed and implemented to suppress the excess noise, where the most representative one is the local LO scheme. The overview of the CV-QKD system development is shown in Fig. 24.

The CV-QKD system is heading towards high secret key rate at long distance. For the early CV-QKD systems, the quantum signal and LO are generated by the same laser in the transmitter and co-propagate through the quantum channel. However, the longer transmission distance raises the requirement of the power of LO, which leads to more excess noise caused by the LO leakage. Meanwhile, the transmission of LO in an unsecure quantum channel makes it easy for the manipulation of LO by an eavesdropper, leading to a security loophole. To solve the issues above, the local LO system with the LO generated at the receiver side is proposed. Here the LO no longer needs to be transmitted through the quantum channel, therefore it never affects the quality of quantum signals and the practical security of the system. However, the system is seriously affected by the phase mismatch between the LO and quantum signal since they are not generated from the same laser source, thus a classical pilot tone generated by the transmitter is necessary in most of the local LO systems for phase recovery.

Though the local LO system still requires the co-propagation of quantum and classical signals, the leakage of the pilot tone will not seriously affect the excess noise, since the requirement of the power of the pilot tone is much lower than the LO. Therefore, the multiplexing of the quantum signal and pilot tone is more flexible. Various multiplexing schemes are proposed to adapt to different hardware configurations and system requirements, such as using the frequency division multiplexing, or further combined with polarization multiplexing in high isolation scenarios. Naturally, raising the repetition frequency contributes to the accuracy of phase

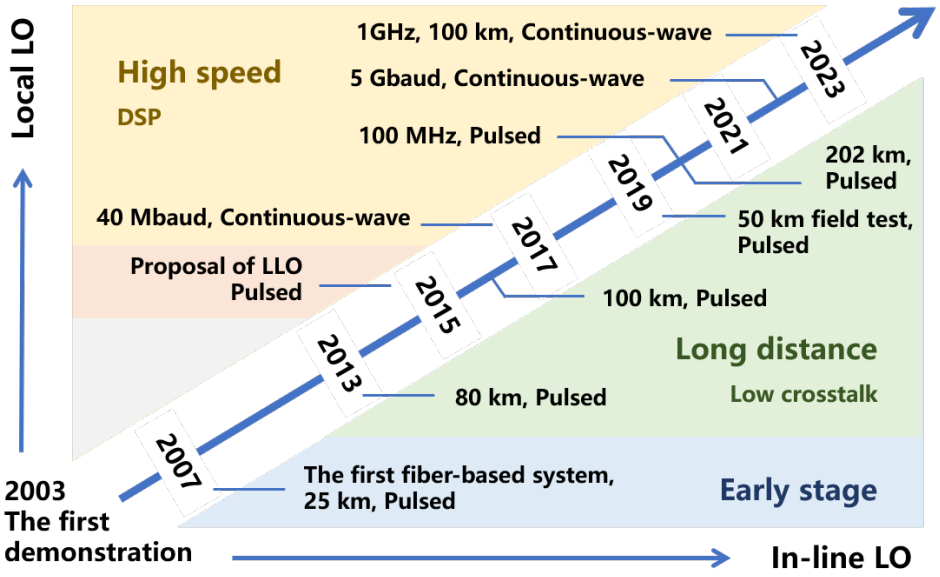

FIG. 24. The overview of the CV-QKD system development. Since the first demonstration in 2003, the in-line LO system has been subsequently developed. After the early stage development, the in-line LO scheme has effectively supported the long-distance system, by reducing the crosstalk from LO to quantum signals. In 2015, the local LO scheme was proposed, which then heads towards high speed system with advance DSP technique.

tracking and phase noise suppression as we mentioned before. To compensate the influence from the limited hardware resources, DSP is introduced. A highly digitized system can compensate both of the polarization and phase change in digital domain, which significantly simplifies the system structure and leads to a more practical system. In this section, we review the development of the in-line LO and local LO systems, as well as the system co-existed with classical network and the other system schemes such as the free space system and the entanglement-based systems.

A. In-line LO systems

The main feature of the in-line LO CV-QKD system is that the quantum signal and LO are generated by the same laser, therefore the interference at the receiver is not seriously affected by the signal mismatch. However, the large power difference between the quantum signal and LO makes the leakage of LO significantly affect the quantum signal, which is the main noise source of the system. For instance, the average photon number of a quantum signal is no more than 20, but the average photon number of LO is usually higher than 10^7 at the receiver site to provide sufficient power for a high-quality shot-noise limited homodyne detection. The leakage of LO leads to the increase of excess noise. Moreover, longer transmission distance requires higher LO launch power. Therefore, higher isolation between quantum signal and LO is required by the long-distance in-line LO system.

The key to reduce the LO leakage is using multiplexing including time-division multiplexing, the polarization multiplexing and the frequency-division multiplexing. The quantum signal and LO are encoded on different dimensions for co-transmission in fiber (that's why we call the in-line LO), and de-multiplexed in physical layer at the receiver[130,132–139,292,383–386]. Now we review the development of in-line LO CV-QKD systems, including the early systems, the long-distance achievements, the chip-based systems, and the field tests. The details of the representative in-line LO system experiments are concluded in Table. X.

1. *Early systems*

The first CV-QKD system implementation is realized in 2003, as shown in Fig. 25 (a), where the secret key rate can reach 1.7 Mbps in a loss free channel and 75 kbps in a channel with 3.1 dB loss[130]. The system is based on the free space optical devices, working at the wavelength of 780 nm. Reverse reconciliation is firsly implemented to support a secret key distillation beyond 3-dB limit. The quantum signal and LO are generated from the same laser, where the light outputs from Alice's laser is firstly divided, part of the light is Gaussian modulated as the quantum signal of coherent states, and the other part of the light is used to provide the LO signal. The Gaussian modulation is realized based on the amplitude and phase modulation method with pulsed light. To compensate the phase difference between quantum signal and LO since they go through different path, training sequence is introduced. These features are reserved and improved in the later fiber based CV-QKD systems.

The first all-fiber CV-QKD system is realized in 2007,

TABLE X. A Comparison Between Different in-line LO CV-QKD Systems. β is the reconciliation efficiency, L_{max} is the maximum transmission distance or loss, and SKR is the secret key rate corresponds to L_{max}. MD means multidimensional reconciliation.

	Years	Key modules		Key indicators		
		Multiplexing	Reconciliation	β	L_{max}	SKR
Lab system	2003	Transmitting separately	Slice	85 %	3.1 dB	75 kbps[130]
	2007	Time	Slice	89.8 %	25 km	2 kbps[132]
	2007	Polarization and frequency	Slice	89.8 %	5 km	0.3 bit/pulse[292]
	2013	Time and polarization	MD	95 %	80 km	0.2 kbps[133]
	2016	Time and polarization	MD	95.6 %	100 km	0.5 kbps[136]
	2020	Time and polarization	MD	98 %	202.81 km	6.214 bps[139]
Field test system	2012	Time and polarization	Slice	∼90 %	17.7 km	0.3 kbps[134]
	2016	Time and polarization	MD	∼ 95 %	17.52 km	0.2 kbps[135]
	2019	Time and polarization	MD	95.1 %	49.85 km	5.77 kbps[137]
Chip-based system	2019	Time and polarization	MD	97.99 %	2 m	0.25 Mbps[138]

where 2 kbps secret key rate is achieved with a 25 km (5.2 dB) optical fiber channel[132]. The most important enhancement is that the quantum signal and the LO are co-transmitted in the same fiber to reduce the accumulation of phase noise caused by the seperate transmission. As shown in Fig. 25 (b), the multiplexing strategy is the time division multiplexing using an unbalanced Mach Zender interferometer (MZI) structure. Specifically, the light from the pulsed laser is divided by a 1:99 beamsplitter, where the 1 % weak light path is used to generate the modulated coherent states with amplitude and phase modulators, and the strong light is used as the LO. With a variable optical attenuator, the modulated coherent states are attenuated to the quantum level, which is then time-division multiplexed with the LO by combining with a 99:1 coupler, and then transmitted to the receiver side. The optical delay line deployed in the LO path is used to adjust the gap between quantum signal and LO. This time division multiplexing strategy is reserved in the long distance system to enhance the isolation between quantum signal and LO. The de-multiplexing is realized with an unbalanced beamsplitter (10:90) to reduce the loss of quantum signal, where the quantum signal with high power is interfered with the low power LO after the beamsplitter. A delay line is deployed at the quantum signal path to align the signal pulses. Besides, the automatic system control is introduced into the system, where the average power of the quantum signal is monitored and real-time adjusted to adapt the SNR requirement of error correction. The training sequence is used for synchronizing Alice and Bob, and determining the relative phase between the signal and the LO. An automatic adjustment of the bias voltages that need to be applied to the amplitude modulators in Alice's site is performed in every 10 s. The repetition rate of the system is 350 kHz, the detection efficiency of the detector is 0.606. The modulation variance of the system is 18.5, and the excess noise is 0.005.

B. Qi et al. realized a CV-QKD system over 5 km fibers using polarization and frequency division multiplexing to co-transmit the quantum signals and LO[292]. The final secret key rate at 5 km is 0.3 bit/pulse. As shown in Fig. 25 (c), the quantum signals and LO in different polarizations are combined with a polarization coupler, and de-multiplexed at the receiver by another polarization beam splitter. The frequency division multiplexing is realized with an acousto-optic modulator. By applying both polarization and frequency division multiplexing, the isolation between quantum signal and LO comes up to 70 dB, well preventing the LO leakage. An isolator is placed in the signal arm of Bob's MZI to reduce the noise due to multiple reflections of LO. The phase compensation on hardware layer is replaced by a digital compensation at Alice's site. The noise from the receiver is assumed to be independent from Eve's control, which contributes to the performance enhancement.

2. *Long distance achievements*

In 2013, the first long-distance CV-QKD system shown in Fig. 26 (a) is realized by P. Jouguet et al., which achieves the secret key rate of over 100 bps at 80 km[133]. Such an improvement is supported by the optimized reconciliation strategy and system architecture. The multi-dimensional reconciliation firsly introduced into the practical experiment significantly enhances the reconciliation efficiency of a CV-QKD

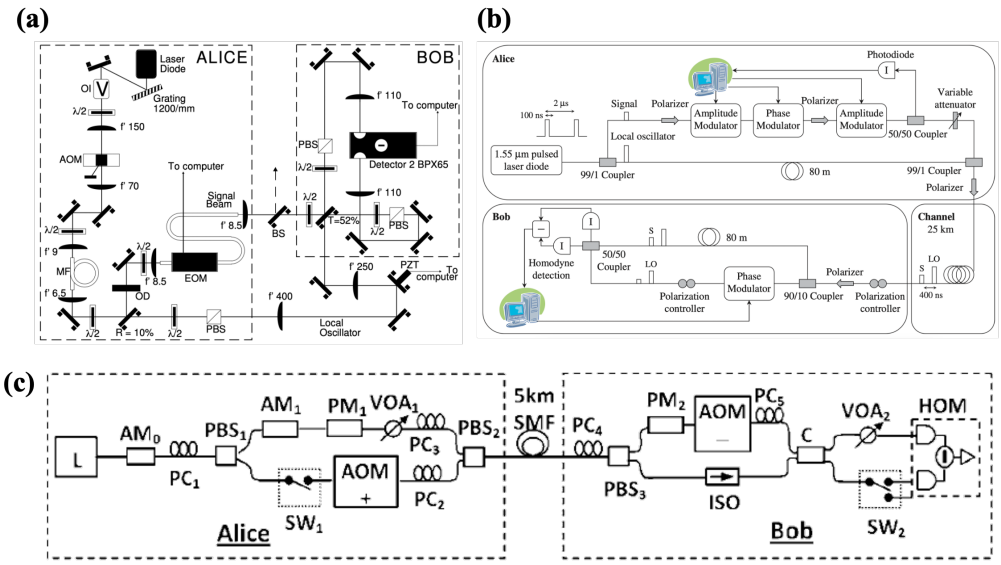

FIG. 25. The early in-line LO CV-QKD systems. (a) The first CV-QKD system, from F. Grosshans et al.[130]. (b) The first all-fiber CV-QKD system with time division multiplexing, from J. Lodewyck et al.[132]. (c) The first all-fiber CV-QKD system with polarization and frequency-division multiplexing, from B. Qi et al.[292]. (a) Reproduced with permission from Nature 421, 238-241 (2003). Copyright 2003 Nature Publishing Group. (b) Reproduced with permission from Phys. Rev. A 76, 042305 (2007). Copyright 2007 American Physical Society. (c) Reproduced with permission from Phys. Rev. A 76, 052323 (2007). Copyright 2007 American Physical Society.

system, from no more than 90 % to 95 %. This promotes the developments of long-distance CV-QKD system and supports all of the long-distance CV-QKD system until now. The main features of this experimental system include the polarization and time division multiplexing, the trusted detection noise, the polarization control using a dynamic polarization controller and the clock synchronization with part of the LO. The multiplexing scheme used in this system is widely used for achieving high isolation between quantum signal and LO in most of the long-distance systems.

As shown in Fig. 26 (b), D. Huang et al. later realized a CV-QKD system with transmission distance over 100 km and more than 300 bps secret key rate by controlling the excess noise to low level[136]. An efficient scheme is proposed to perform high-precision phase compensation under low SNR conditions which contributes to the excess noise of 0.015. For system hardware, they developed a low-noise detector, which reduces the requirement of the high LO power.

As shown in Fig. 26 (c), the CV-QKD system with the longest transmission distance is realized by Y. Zhang et al. at 2020, where the transmission distance can reach 202.81 km, which doubles the previous transmission distance record[139]. In this work, two amplitude modulators are used for generating pulsed light, then an amplitude and a phase modulator are used for Gaussian modulation, and an amplitude modulator is used to attenuate the modulated light signal to quantum level, as well as enhancing the SNR of frame sequence. Time-division multiplexing and polarization multiplexing are used to ensure sufficient isolation between the co-transmit of quantum signals and LO. Moreover, LO is amplified at the receiver site therefore the requirement of the launch power of LO at the transmitter site is reduced, which is beneficial for reducing the cross talk. Automatic feedback systems are used to overcome the channel perturbations, and high-precision phase compensation is adopted to supress the excess noise and highly efficient postprocessing is realized to achieve long transmission distances at sufficiently high secret key rates. Besides the transmission distance of 202.81 km, the system was also tested with the link distance of 27.27, 49.30, 69.53, 99.31 and 140.52 km, where the secret key rate reached 278, 62, 4.28, 1.18 and 0.318 kbps.

The key modules of an in-line LO CV-QKD system are the multiplexing module and the reconciliation module. It can be seen that the development of the reconciliation directly supports the long-distance transmission, where the long transmission distance always combines with high reconciliation efficiency. The multiplexing scheme finally evolves into the time and polarization division multiplexing, since this is the simplest method to achieve sufficient isolation between quantum signal and LO.

Besides the reconciliation and multiplexing, the modulation, monitoring, sampling and compensation techniques are also well developed. The generation of light pulses with high extinction ratio is demonstrated in 2015[281], where the extinction ratio overpasses 80 dB by using a double cascaded MZI modulation. Later, the imperfect quantum state preparation is theoretically and experimentally investigated in 2017, which demonstrates that the incorrect calibration of the working parameters for the amplitude modulator and phase modulator can lead to a significant increase of the excess noise and misestimate of the channel loss. Schemes for calibrating the working parameters of the modulators are proposed and demonstrated to solve the imperfect state preparation issue. An LO monitoring scheme is proposed to enhance the

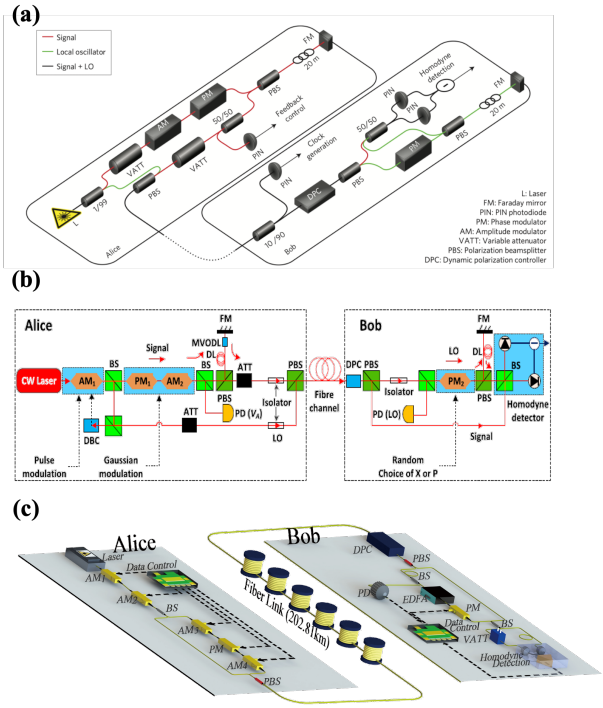

FIG. 26. The in-line LO CV-QKD systems with long distance. (a) 80 km CV-QKD system from P. Jouguet et, al.[133]. (b) 100 km CV-QKD system from D. Huang et al.[136]. (c) 202.81 km CV-QKD system from Y. Zhang et al.[139]. (a) Reproduced with permission from Nat. Photonics 7, 378-381 (2013). Copyright 2013 Macmillan Publishers Limited. (b) D. Huang, Sci. Rep., 6, 1-9, 2016; licensed under a Creative Commons Attribution (CC BY) license. (c) Reproduced with permission from Phys. Rev. Lett. 125, 010502 (2020). Copyright 2020 American Physical Society.

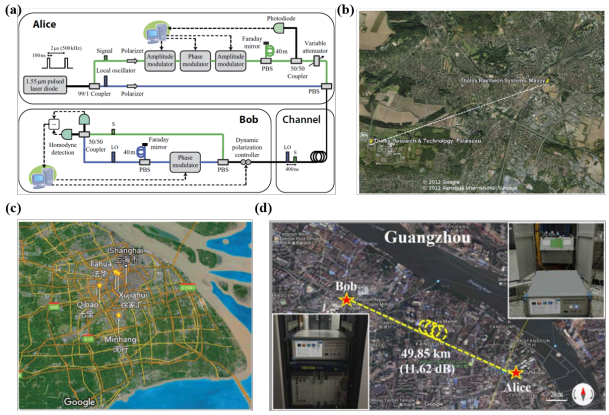

FIG. 27. The field tests of in-line LO CV-QKD systems. (a) The first field test of CV-QKD system, from S. Fossier et al.[339]. (b) The field test of using CV-QKD for classical symmetric encryption, from P. Jouguet et al.[134]. (c) Field demonstration of a CV-QKD network, from D. Huang et al.[135]. (d) The longest field test of CV-QKD with 50 km commercial fiber, from Y. Zhang et al.[137]. (a) Reproduced with permission from New J. Phys. 11, 045023 (2009). Copyright 2009 IOP Publishing Ltd. (b) Reproduced with permission from Opt. Express 20, 14030 (2012). Copyright 2012 Optical Society of America. (c) Reproduced with permission from Opt. Lett. 41, 3511 (2016). Copyright 2016 Optical Society of America. (d) Reproduced with permission from Quantum Sci. Technol. 4, 035006 (2019). Copyright 2019 IOP Publishing Ltd.

practical security of a CV-QKD system[300]. The LO is monitored by the balanced photodiode, and the SNU is real-time calibrated. The excess noise in the system and its impact on the performance is also investigated[387]. Finite sampling bandwidth of the analog-to-digital (AD) converter may lead to inaccurate results of pulse peak sampling, which is solved by a dynamic delay adjusting module and a statistical power feedback-control algorithm[388].

As for polarization compensation, a feedback algorithm is proposed to stable the system, where a polarization feedback signal is produced by an amplified Root Mean Square to Direct Current conversion by picking out a 10 % portion of the LO light in real time[389]. With the output data, one can estimate the mean value and the standard deviation of the polarization drift. Then a dynamic polarization controller is deployed at the receiver's site to stable the polarization automatically. For phase noise compensation, a widely used scheme is to insert one frame of training sequence into the quantum signal path, to calculate the expectations and evaluate the phase difference[389]. Long term stable phase locking is employed to seperately compensate the fast-fading and the slow-fading phase mismatch by adjusting the phase modulator and fiber length[390]. Later, a novel phase compensation scheme based on an optimal iteration algorithm is proposed to realize the fast-fading phase compensation accurately[391].

3. *Field tests*

Besides the system in laboratory, field tests of the in-line CV-QKD system are also widely performed. The first field test CV-QKD system is realized by S. Fossier in 2009[339], the system structure is shown in Fig. 27 (a). It was automatically operated over 57 h, and achieved a secret key rate of 8 kbps over a 3 dB loss optical fiber. The system is part of the SECOQC network[94], where its practical fiber length is 9 km. Later, the system was used for the encryption of point-to-point communications, which demonstrated the reliability of a CV-QKD system over a long period of time in a server room environment[134]. The map of the CV-QKD link is shown in Fig. 27 (b). The stability of this field test system is studied in detail, and the results show that, the birefringence, and consequently the polarization, in the installed fibre typically varied ten times slower than a laboratory fibre spool of equivalent length, while the phase drift linked to temperature changes in the devices is typically of 2π every 30 s and these vibrations have a typical frequency of 50-1000 Hz.

A full-mesh 4-node CV-QKD field test is realized in 2016 by D. Huang et al.[135], where 6 point-to-point CV-QKD links with distances of 19.92, 35.35, 37.44, 15.34, 17.52 and 2.08 km connect 4 nodes together, as shown in Fig. 27 (c). This work adopts wavelength division multiplexing to co-transmit the quantum signal and the essential classical signals for clock

FIG. 28. The long-term field test in Qingdao, China, from Y. Zhang et al.[140]. (a) The layer structure of the 3-node network. (b) A Bird's-eye view of the field test environment. (c) 28-day continuous test results.

synchronization and the forward and backward classical data communication. The reflection caused by the connectors of the field fiber links is well studied, and the results show that the connectors feature a nominal reflectance of -40 dB, and more than 20 reflective events are measured in the experiments.

The longest field test of CV-QKD system is realized in 2019, by Y. Zhang[137], through 49.85 km commercial fiber, as shown in Fig. 27 (d). By applying an efficient calibration model with one-time evaluation, a rate-adaptive reconciliation method which maintains high reconciliation efficiency with high success probability in fluctuated environments, and a fully automatic control system which stabilizes system noise, a secret key rate which is two orders-of-magnitude higher than the previous field test demonstrations is achieved.

Later, the first network application demonstration with clear application scenarios over a long period of time through existing commercial optical fiber links is tested in Qingdao, China, as shown in Fig. 28 (a) and (b)[140]. The performance of the 3-node network is tested for a month, where the the total length of the application demonstration link is 71.03 km, with a trusted relay in the middle. As shown in Fig. 28 (c), the average secret key rate achieves higher than 12.00 kbps over 71.03 km optical fiber line, which paves the way to deploy CV-QKD in metropolitan settings.

4. *System on chip*

Photonic integrated circuit is a promising way to realize a large scale and cost effective system. After the design is finalized, the production cost of the chip will sharply decrease with the increase of production. Therefore, in addition to miniaturizing the system, chipization can also greatly promote the low-cost mass production for the cost sensitive CV-QKD system. The earliest attempt to chip-based CV-QKD systems is in 2015, where a silicon photonic chip comprising all major CV-QKD components as well as complete subsystems is designed and fabricated[392].

Later the first chip-based CV-QKD platform is demonstrated in 2019[138], where most of the active devices such as the phase modulator, amplitude modulator, optical variable attenuator and homodyne detector are integrated on Silicon-On-Insulator chip, as shown in Fig. 29. The phase and amplitude modulator have a 90 % switching time of 2.5 ns, corresponding to a 200-MHz modulation frequency. However, the homodyne detector limits the bandwidth of the system to 10 MHz, mainly affected by the two-stage transimpedance amplifier. The shot noise is 5 dB higher than the electronic noise, and the detection efficiency is 0.498. With these on-chip devices, an in-line LO system is demonstrated. A grating coupler introduces the light from an external laser source into the chip, then an 1:99 directional coupler splits it into two path, where the weak one is used for quantum signal modulation, while the stronger one is the LO. After that, the Gaussian modulated quantum signal and LO are multiplexed into two orthogonal polarization states with a 2D grating coupler, and output to the channel. The receiver uses a 2D grating coupler to seperate the quantum signal and LO, then the quantum signal is homodyne detected. The system is tested with a 2 m fiber for proof-of-principle demonstration, the secret key rate can reach 0.25 Mbps.

This work demonstrate that the Silicon-On-Insulator platform can basically satisfy the requirement of a CV-QKD system. A two-dimensional grating coupler integrated on chip can be directly used for the polarization multiplexing and demultiplexing. The pulse generation, the Gaussian modulation,

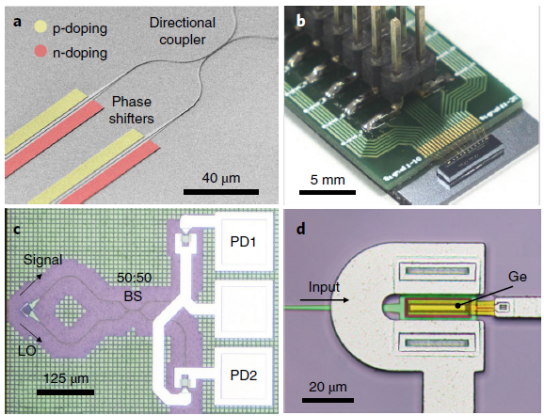

FIG. 29. The first chip-based CV-QKD system. From G. Zhang et al.[138]. Reproduced with permission from Nat. Photonics 13, 839 (2019). Copyright 2019 Springer Nature Limited.

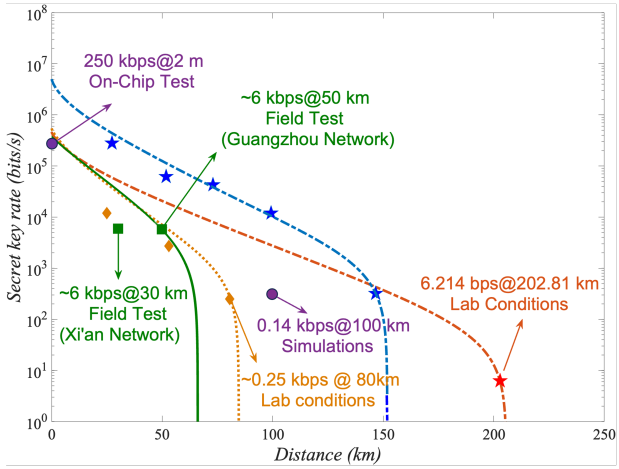

FIG. 30. The overview of the key achievements of the secret key rate in the in-line CV-QKD systems. The longest transmission distance is 202.81 km in laboratory, and 50 km with field test. The back-to-back test of the on-chip system is demonstrated, and the estimated parameters can support the 100 km system.

the variable optical attenuator and the detector are all realized with chip-based components. The insertion loss of the grating coupler, the detection efficiency and the bandwidth of the chip-based detector are the concerns, where a part of these issues are solved in the later works, and we detailed them in the local LO system part. A comparison of the secret key rate of different systems is shown in Fig. 30.

5. *Other in-line LO systems*

Besides Gaussian modulation, discrete modulation and unidimensional modulation is also realized with in-line LO system, as shown in Fig. 31. The discrete modulation format has lower requirement for digital to analog conversion, and the unidimensional modulation can be realized with a single amplitude modulator, which are suitable for cost-effective applications. Polarization multiplexing is also used in these systems. The four-state modulation CV-QKD system from X. Wang et al. can reach 1 kbps secret key rate with the transmission distance of 30.2 km[393], the four-state modulation CV-QKD system from T. Hirano et al. can reach 50 kbps secret key rate with the transmission distance of 10 km[394], and the unidimensional modulated system achieves 5.4 kbps and 0.7 kbps secret key rate at 30 and 50 km[395].

B. Local LO systems

Though the in-line LO system has developed for a long time, some problems are still inevitable. The most critical issue is the security loophole caused by the LO accessible to a potential eavesdropper[405–408]. The manipulation of LO can make the sender and receiver perform parameter estimation mistakenly, leading to an overestimate of secret key rate.

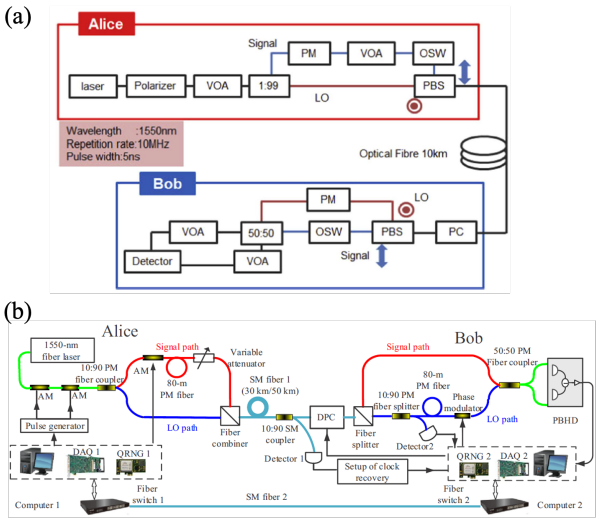

FIG. 31. The in-line LO CV-QKD systems with particular modulation format. (a) The 4-state modulated in-line LO CV-QKD system[394], from T. Hirano et al. (b) The unidimensional modulated in-line LO CV-QKD system[395], from X. Wang et al. (a) Reproduced with permission from Quantum Sci. Technol. 2, 024010 (2017). Copyright 2017 IOP Publishing Ltd. (b) Reproduced with permission from Phys. Rev. A 95, 062330 (2017). Copyright 2017 American Physical Society.

Monitoring the LO can defend part of the attacks, but the loophole still exists and more attacking strategies aiming at it can be continuously developed. Besides, from the system development, when we hope to achieve high key rate by raising the repetition frequency or achieve long distance overcoming the large channel loss, the crosstalk from LO to quantum signal will increase, which weakens the system performance. Therefore, after more than a decade of development, the local LO CV-QKD system without the transmission of LO is proposed.

The local LO system is firstly proposed in 2015, intends to solve the problems above by generating LO inside the receiver, which is a once and for all solution. Since the quantum signal and the LO are generated by different lasers, a fast-fading phase noise is introduced, leading to the increase of excess noise. The key of a local LO system is to establish a reliable phase reference between the sender and receiver, usually realized by a classical reference signal, namely pilot tone. When heading towards high-speed system with high repetition rate, the pulsed system with time division multiplexing is no more effective. Considering that the power of pilot tone is low enough so that its leakage is not as much as the in-line transmitted LO, the frequency division multiplexed quantum and pilot tone signals with continuous-wave light becomes the mainstream scheme of the local LO system. In addition, the DSP is introduced to the local LO system for more accurate phase recovery, high speed modulation with continuous-wave light and simpler detection. A review of the evolution of local LO CV-QKD system is shown in Table. XI, including the typical systems with different settings, and there are also some noteworthy local LO systems.[409–411]

TABLE XI. A Comparison Between Different Local LO CV-QKD Systems. Here, f means the repetition frequency, L_{max} means the maximum transmission distance and SKR is the secret key rate corresponding to L_{max}.

	Years	Key modules			Key indicators		
		Modulation format	Modulator	Multiplexing	f	L_{max}	SKR
Lab systems	2017	8-PSK	DP-MZM	Frequency	40 MBaud	40 km	0.006 bit/symbol[283]
	2020	Gaussian	AM+PM	Frequency and polarization	100 MHz	25 km	1.85 Mbps[284]
	2022	QPSK	IQ modulator	Frequency and polarization	5 GBaud	25 km	2.48 Mbps[143]
	2022	256 QAM	IQ modulator	Frequency	600 MBaud	25 km	24 Mbps[145]
	2022	256 QAM	IQ modulator	Frequency and polarization	1 GBaud	50 km	9.212 Mbps[285]
	2022	Gaussian	Sagnac fiber loop	Time	10 MHz	50 km	0.08 Mbps[396]
	2023	Gaussian	IQ modulator	Frequency	100 MHz	20 km	0.0471 bit/symbol[286]
	2023	16 state	IQ modulator	Frequency	2.5 GBaud	80 km	2.11 Mbps[397]
	2023	Gaussian	IQ modulator	Frequency and polarization	1 GHz	100 km	0.51 Mbps[398]
	2024	Gaussian	IQ modulator	Frequency	100 MBaud	100 km	0.0254 Mbps[399]
Field tests	2019	//	//	//	//	3.9 km	0.07 Mbps[144]
	2023	Gaussian	//	//	12.5 MBaud	22.5 dB	0.01 kbps[400]
	2023	Gaussian	Sagnac fiber loop	Time	50 kHz	10.4 km	1.6 kbps[401]
Chip-based systems	2023	Gaussian	IQ modulator	Frequency	100 MHz	6.9 km	0.28 Mbps[402]
	2023	Gaussian	IQ modulator	Time	8 MHz	11 km	0.4 Mbps[403]
	2023	Gaussian	IQ modulator	Time	0.25 GBaud	50 km	0.75 Mbps[404]

1. *The early systems*

The early experiments adopt a pulsed laser source with LiNbO3 amplitude and phase modulators for generating quantum and pilot tone signals[141,142]. In the work finished by B. Qi et al.[141], the quantum signals and pilot tones are time-division multiplexed and then detected by receivers using heterodyne detection. The sender's and receiver's LO laser sources are free running without any connections, and the heterodyne detection results of the pilot tone provide the phase reference for data rotation. In D. Soh's work[142], the signal and LO are generated from one laser for proof-of-principle demonstration. Homodyne detection is used for detecting the quantum signal and pilot tone. Each pilot tone is sent twice in a pair for the receiver to get both quadratures with homodyne detection.

In the above works, continuous-wave LO signals are adopted, while in Huang's work[279], an amplitude modulator is deployed inside the receiver side for generating pulsed LO. The quantum and pilot tone signals are also generated by the same modulation module with time division multiplexing. The commonalities of these early systems are using pulsed light, and time-division multiplexed quantum and pilot tone signals are generated by the same modulation module. The key role of these early systems is verifying the possibility of compensating the phase mismatch between the quantum and LO signal with high precision required in a CV-QKD system using a pilot tone.

2. *Systems with continuous-wave light*

As we mentioned above, the most crucial issue of a local LO CV-QKD system is the phase recovery with pilot tone. To improve the accuracy of the phase recovery, raising the repetition frequency of the quantum and pilot tone signals for a more accurate track of the phase shift is a direct and effective way. However, the pulsed system with time division multiplexing significantly limits the system repetition frequency. Therefore, it is a general trend to use continuous-wave light instead of pulsed light to support a high speed system[282,283]. Without time division multiplexing, the repetition rate of the system is significantly enhanced, resulting in a high-rate system with 1 GHz repetition rate[143,284,285].

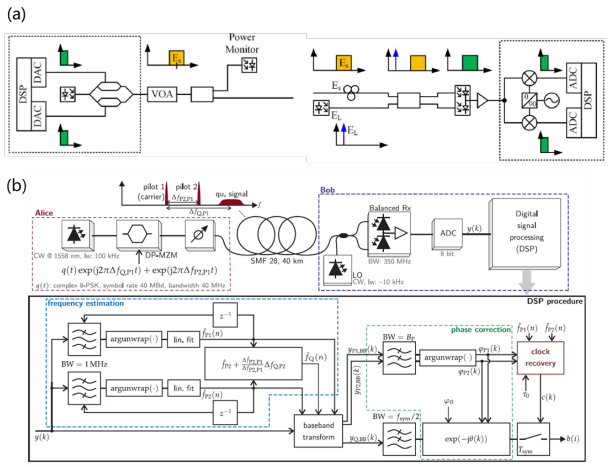

FIG. 32. The continuous-wave local LO CV-QKD system. (a) The software defined CV-QKD transmitter and receiver. From H. H. Brunner et al.[282]. (b) The local LO CV-QKD system with DSP where the quantum signal and two pilot tones are frequency division multiplexed. From S. Kleis et al.[283]. (a) Reproduced with permission from ICTON 1-4 (2017). Copyright 2017 IEEE. (b) Reproduced with permission from Opt. Lett. 42, 1588 (2017). Copyright 2017 Optical Society of America.

Besides, for the multiplexing of quantum signal and pilot tone, since the high power pilot tone is not necessary required, the quantum signal and pilot tone can be modulated simultaneously with the same modulation module in a frequency division multiplexed scheme[282,283]. Naturally, by introducing a frequency difference between the quantum signal and LO, a digital heterodyne detection can be realized, where we can use the detection results from one homodyne detector to recover both information of quadratures[143,282–285,398]. In this way, the experimental demonstration of the system is significantly simplified.

H. H. Brunner et al. demonstrated a local LO CV-QKD system as shown in Fig. 32 (a)[282]. The 4-state discrete modulation of coherent states is realized with quadrature phase-shift keying modulation used in classical communications, and a variable optical attenuator is used to adjust the power to the quantum level. No amplitude modulator for pulse generation is used, instead, a RRC filter in the digital domain completes the pulse shaping. Moreover, combined with an analog electronic low-pass filter at the output of the digital-to-analog (DA) convertor, the quantum signal is concentrated in the 10 MHz bandwidth. Digitally, the quantum signal is up-converted and combined with a pilot tone. To reduce the quantization noise since the weak quantum signal is produced and detected together with a much stronger pilot tone, the DA and AD convertor bit width are 16 bits and 14 bits respectively. The heterodyne detection is also performed digitally, the LO is set to have a frequency difference with the quantum signal, and a down conversion in digital domain is then performed to recover the information on both quadratures.

As shown in Fig. 32 (b), S. Kleis et al. realized a complete system with the simultaneous modulation of 8 phase-shift keying discrete modulated quantum signal and two pilot tones using a dual-parallel Mach-Zehnder modulator[283]. Digital heterodyne detection is used to get both quadratures with a single homodyne detector. This work achieved the secret key rate of 6×10^{-3} bit/symbol at 40 km, which shows the way of low-complexity QKD system demonstration within metropolitan distances. The core ideas of the above works is to realize CV-QKD system with continuous-wave light and a structure similar to the classical coherent communications, DSP is widely used in the system, which opens the new way of CV-QKD systems.

Subsequently, the discrete local LO CV-QKD system is extended to high-order modulation formats for better performance. As theoretically analyzed, the increasing of modulation order results in higher secret key rate with most of the security framework of discrete-modulation CV-QKD. Moreover, when the constellation is similar to the Gaussian distribution, the secret key rate of the system can be better than the constellation with uniform distribution. In this guidance, a high-order discrete modulated CV-QKD system is realized with 16-order two-ring phase shift key modulated coherent states[397]. Compared with the high-order quadrature amplitude modulation, 16-order two-ring phase shift key modulation can be realized with less DA requirements, contributing to suppressing the modulation noise. The achieved secret key rates are 49.02 Mbps, 11.86 Mbps and 2.11 Mbps over 25-km, 50-km, and 80-km optical fiber. 67.4 %, 70.0 % and 66.5 % of the performance of a Gaussian modulated protocol can be achieved with this simpler scheme.

3. *Systems with polarization multiplexing*

Besides modulating the quantum signals together with pilot tone, the quantum signals can also be modulated individually and combined with the pilot tone in different polarization directions[284,294,398,412,413].

As shown in Fig. 33 (a), the optical carrier is firstly amplitude modulated to generate 250 MHz signal pulses, then sent into the dual-polarization IQ modulator for the modulation of the discrete coherent states and the pilot tone. The quantum signal and pilot tone are multiplexed in different frequency and polarization directions. The receiver performs heterodyne detection of both polarizations after the compensation of a polarization controller. This scheme can help to reduce the excess noise since the isolation between the quantum signal and pilot tone is more sufficient than the frequency division multiplexed method.

Further, a Gaussian modulated system with frequency division multiplexing and polarization multiplexing is realized by H. Wang et al.[284], shown in Fig. 33 (b). Digital heterodyne detection is used for detecting quantum and pilot tone signals respectively. It can achieve 7.04 Mbps asymptotic-limit secret key rate at 25 km and 1.85 Mbps with finite-size.

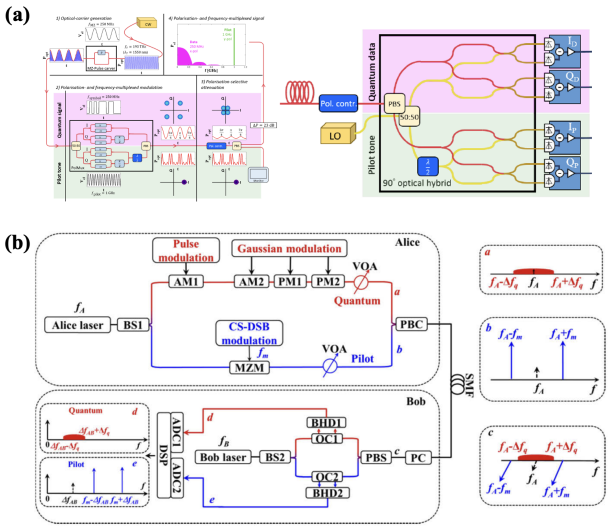

FIG. 33. Local LO CV-QKD system with polarization multiplexed quantum signal and pilot tone. (a) From F. Laudenbach et al.[413]. (b) From H. Wang et al.[284]. (a) F. Laudenbach, Quantum, 3, 193, 2019; licensed under a Creative Commons Attribution (CC BY) license. (b) Reproduced with permission from Opt. Express 28, 32882 (2020). Copyright 2020 Optical Society of America.

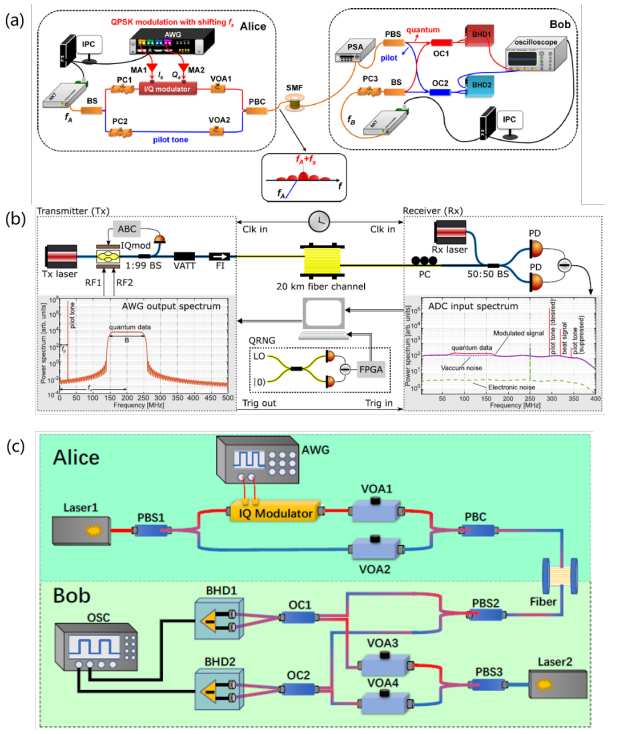

FIG. 34. The high-speed, composable-security and long-distance local LO CV-QKD systems. (a) The high-speed system with 4-state modulation format. From H. Wang et al.[143]. (b) The system which generates composable secret keys. From N. Jain et al.[286].(c) The system supporting 100 km transmission distance considering finite-size effect. From Y. Pi et al.[398]. (a) H. Wang et al., Commun. Phys., 5, 162, 2022; licensed under a Creative Commons Attribution (CC BY) license. (b) N. Jain et al., Nat. Commun., 13, 4740, 2022; licensed under a Creative Commons Attribution (CC BY) license. (c) Reproduced with permission from Opt. Lett. 48, 1766 (2023). Copyright 2023 Optica Publishing Group.

4. *Recent progress*

Based on the digital modulation and detection scheme, local LO CV-QKD system is heading towards high secret key rate[143], composable security[286] and long distance[342].

As shown in Fig. 34 (a), in H. Wang's work[143], using frequency division multiplexing and polarization multiplexing to transmit the quantum and pilot signal, as well as two digital heterodyne detector for measuring, a system with 4-state discrete modulated coherent states achieved 233.87 Mbps, 133.6 Mbps and 21.53 Mbps secret key rate at 5 km, 10 km and 25 km. This increases the asymptotic secret key rate to sub-Gbps level, which can satisfy the one-time pad cryptographic task. The further investigation on optimizing the practical system parameters shows an effective way to the high-performance system[414].

N. Jain's system with composable security realized 0.0471 bits/symbol secret key rate at 20.3 km with extremely simple devices shown in Fig. 34 (b), an IQ modulator produces frequency division multiplexed quantum and pilot signals which are detected by a digital heterodyne detector[286]. The system is able to generate composable secret keys with 2×10^8 coherent states, which is far less than the previous requirements due to improvements to the security proof.

A recent work with the structure shown in Fig. 34 (c) can realize a transmission distance over 100 km, and the asymptotic secret key rate can reach 10.36 Mbps, 2.59 Mbps and 0.69 Mbps over transmission distance of 50 km, 75 km and 100 km[398]. This work significantly increases the transmission distances of a local LO CV-QKD system, and shows a promising way to realize long-distance and high-speed QKD using telecom devices.

C. CV-QKD systems co-existed with classical communication environment

The homodyne and heterodyne detection in CV-QKD system act as a matched filter since the LO naturally introduce a frequency selection on the received signal, therefore the filter in time and frequency domain is unnecessary. Moreover, the devices in a CV-QKD system is compatible with the classical coherent optical communications. Therefore, CV-QKD is suitable for coexisting with classical signals, which is easy for deployments.

The test of the system co-existing with classical channels was firstly demonstrated in 2010[419], and has been further developed in recent years[277,415,420–423]. The further test results show that, over a 25 km fiber, a CV-QKD operated over the 1530.12 nm channel can tolerate the noise arising from up to 11.5 dBm classical channel at 1550.12 nm in the forward direction and 9.7 dBm in backward[277]. The system with 75 km transmission distance can work in the channel with -3 dBm forward classical signals or -9 dBm backward classical signals. These results demonstrate the outstanding capacity of

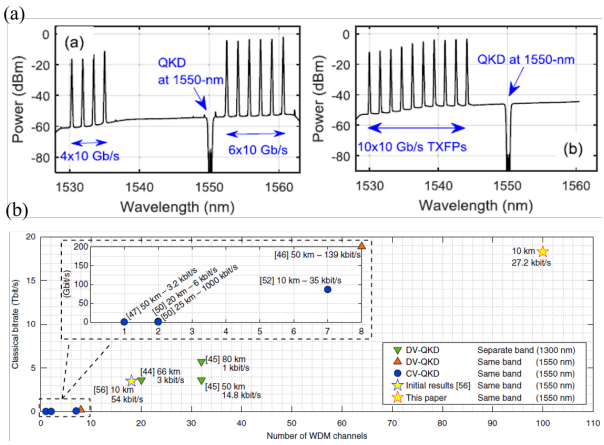

FIG. 35. The CV-QKD systems coexisting with classical signals. (a) The frequency spectrum of the CV-QKD system co-existing with classical communication systems, from F. Karinou et al.[415]. (b) The performance of the CV-QKD system co-existing with 18.3 Tbps data channels, from T. A. Eriksson et al.[278]. (a) Reproduced with permission from IEEE Photon. Technol. Lett. (2018). Copyright 2018 IEEE. (b) T. Eriksson, Commun. Phys., 2, 1-8, 2019; licensed under a Creative Commons Attribution (CC BY) license.

CV-QKD to coexist with classical signals of realistic intensity in optical networks. In 2018, the spontaneous Raman scattering noise of a CV-QKD system co-exisiting with classical channels is investigated, which is the most dominant impairment in a wavelength division multiplexed co-existence environment for CV-QKD[415]. The setting of the quantum signal and the classical signals in frequency domain is shown in Fig. 35. The influence of the spontaneous Raman scattering noise on a CV-QKD system under different transmission situation is investigated, resulting in a scheme which can support a secret key rate of 90 kbps over 20 km, for an ideal QKD system multiplexed with 2 mW optical power.

A CV-QKD system co-propagates with large-scale C-band DWDM channels is investigated in 2019[424]. By operating the quantum signals in S- or L-band, the number of co-propagating channels is doubled. 56 density WDM channels with a total launch power of 14.5 dBm are co-propagated with the quantum signal at the distance of 25 km. Meanwhile, CV-QKD system co-existing with 18.3 Tbps data channels is tested, which contains 100 WDM channels, more than 90 times higher classical bit rate than the previous results[278], shown in Fig. 35 (b). In 2020, B. Chu et al. investigated the LO quality of an in-line LO system in a co-existing environment, which is normally ignored in former studies. It is shown that, four-wave mixing in excess noise analysis is a visible factor causing LO fluctuation characterized by the statistical properties of the power evolution of LO[425].

D. Others

In this part, we introduce the free space and the entanglement based CV-QKD systems. The free space CV-QKD is crucial for the wide range CV-QKD, which is a promising way to connect two distant parties by using the satellite as the relay. On the other hand, for accessing multiple users in complex environment, free space links can be used to construct an access network with simple system structure. For the value in the long-distance and access network applications, the free space CV-QKD is studied, and some results have been achieved. The entanglement-based CV-QKD systems are suitable to distill secret key bits against the high excess noise, which can be used in the scenario with worse channel situation.

1. *Free space systems*

Compared to the fiber link, the free space link suffers from the disturbance of atmosphere, leading to the fading channel and the beam wandering. The fluctuation of transmission efficiency and induced extra excess noise will seriously deteriorate the secure key generation. The atmospheric effects on CV-QKD are studied[153,187,426–428], where beam wandering, broadening, deformation, and scintillation are found to be the primary effects to lead to transmittance fluctuation of horizontal link within the boundary layer, and effect of arrival time fluctuations will induce phase excess noise. Except for the fast fading of the channel parameters such as the channel loss and excess noise, the fading of phase also increases the difficulty of phase recovery. Therefore, new coding strategy and phase compensation methods should be developed.

In 2014, a free space continuous-variable quantum communication is demonstrated with a point-to-point free space link of 1.6 km in urban conditions[429]. Later, a satellite to ground experiment on the quantum limited measurement of the quadrature information is demonstrated[416], as shown in Fig. 36 (a). A series of technologies are developed to support the measurement of the coherent state generated by the laser communication terminal on the geostationary Earth orbit, including the pointing, acquisition, and tracking system of the Transportable Adaptive Optical Ground Station, the adaptive optics system to process the phase front distortions for launching the beam into a single mode fiber, and an optical phase lock loop to lock the phase between the signal and the LO, where the LO is generated by the laser source inside the ground station. The feasibility of secret key establishment in a satellite-to-ground downlink configuration based on CV-QKD is further examined theoretically, where positive secret key rate can be achieved for low-Earth-orbit scenario. While for higher orbits, no secure keys will be generated when considering the finite-size effects[430].

In 2019, the effective resistance against background noise of CV-QKD is theoretically and experimentally demonstrated[431]. In 2020, as shown in Fig. 36 (b), a phase compensation strategy is developed and experimental demonstrated[417]. This work checks the correlation between data held by Alice and Bob in a free space channel, and proves that the fluctuation of transmittance disappears in the correlation, thus enabling phase compensation for signals over fluctuant channels. Later, a series of methods for free space polarization compensation[432], data and transmittance

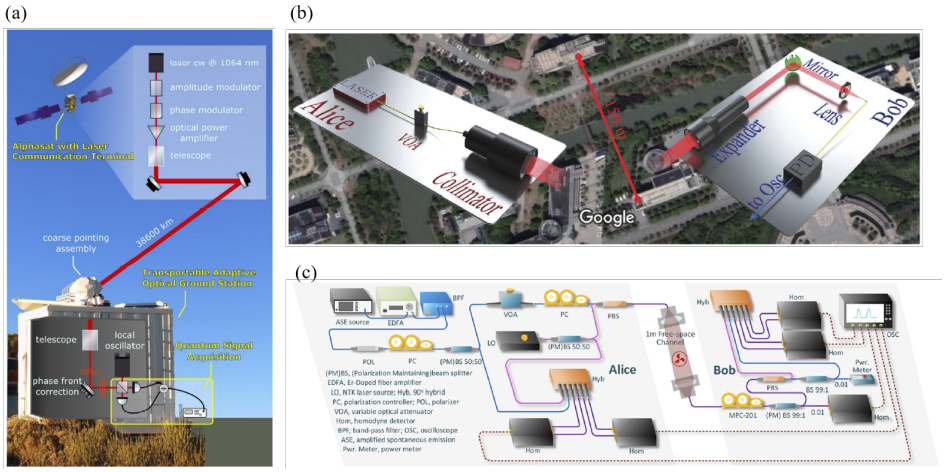

FIG. 36. The free space CV-QKD key techniques and systems. (a) The demonstration of the satellite to ground quantum limited experiment[416]. (b) Phase compensation for a free space CV-QKD system[417]. (c) Passive-state-preparation CV-QKD system with free space channel[418]. (a) Reproduced with permission from Optica. 4, 611 (2017). Copyright 2017 Optical Society of America. (b) Reproduced with permission from Opt. Express 28, 10737 (2020). Copyright 2020 Optical Society of America. (c) Reproduced with permission from Opt. Lett. 48, 1184 (2023). Copyright 2023 Optica Publishing Group.

synchronization[433], data acquisition[434] are proposed, and the feasibility of secure key distribution with free space CV-QKD through fog is experimentally demonstrated[435]. Recently, a passive-state-preparation CV-QKD system shown in Fig. 36 (c) with free space channel is experimentally demonstrated[418]. Thermal-state polarization multiplexing transmitted LO, synchronized channel transmittance monitoring and fine-grained phase compensation techniques are proposed to support a secret key rate of 1.015 Mbps with a free space channel of -15 dB simulated transmittance.

2. *Entanglement-based systems*

The entanglement-based systems have also been developed in recent years as an alternative approach of the CV-QKD system implementation[422,436–442]. The first entanglement-based CV-QKD system is realized in 2009, a pair of bright EPR entangled beams produced from a non-degenerate optical parametric amplifier is used as the source. The secret key rates of 84 kbps and 3 kbps are achieved agianst collective attack with the channel the transmission efficiency of 80 % and 40 %[436]. Later in 2012, a system using modulated fragile entangled states is realized. The system can generate secret key bits against the excess noise of 0.45, which is unable for any coherent state protocols to distill secret key bits[437]. In 2018, the performance of the entanglement-based CV-QKD system is further enhanced, which can achieve an asymptotic secret key rate of 0.03 (0.01) bit per sample at a channel excess noise level of 0.01 (0.1)[439].

V. THE ADVANCED CV-QKD SYSTEM PROGRESS FOR FUTURE APPLICATIONS

The future CV-QKD system will head towards the high-speed and compact integration, rely on full scale DSP and integration with photonic chip. Besides that, the point-to-multipoint CV-QKD system will be widely applied to support a high-speed quantum access network for end-user access.

A. Digital CV-QKD system

Impairment compensation on digital domain can significantly simplify the system structure, contributing to a simple and stable system. The study on classical coherent communications promotes the DSP algorithms in a CV-QKD system. For instance, at the transmitter side, the pulse shaping algorithm is used to raise the availability of the frequency band. For the receiver, the frequency shift is recognized and the down conversion is completed in digital domain, time recovery algorithm is used to obtain the optimal sampling points, digital filter is used to reduce the spectrum mismatch between the transmitter and receiver site, and various of algorithms are developed to distill the parameters of polarization compensation and phase compensation. Thanks to the wide application of DSP in CV-QKD systems, the speed of the system is becoming higher and higher, the latest achievement reach the baud rate of 10 GBaud[146].

With more DSP algorithms being introduced to the CV-QKD system, the security of the DSP is getting more concerns. The security of the linear DSP algorithms in CV-QKD application is proved in 2023, based on the continous-mode quantum optics theroy[443].

For the transmitter, the modulation based on the continuous-wave light and the pulse shaping can be seen as

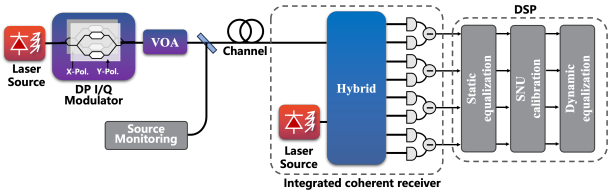

FIG. 37. The advanced point-to-point dual-polarization CV-QKD systems with digital technologies. Here, both of the polarization direction is modulated with quantum signals, the DSP is used to compensate the phase mismatch and polarization rotation. The polarization controller in the optical path is not required. DP IQ modulator: Dual polarization IQ modulator.

a sequence of coherent states with different temporal modes, which raises the requirement that the pulse shaping function in different period should be integrated orthogonality. The commonly used RRC pulse shaping function can satisfy this defination.

For the receiver, the pilot tone is individually processed for distilling the parameter for impairment compensation of quantum signals. Various algorithms can be used to raise the accuracy of distilling compensation parameters, since the process of pilot tone does not affect the quantum signal, only how to use the parameters for compensation matters. While the processing of quantum signals has two main steps, including the static and dynamic equalization. The static equalization aims at compensating the imperfections of the measurement process to provide the right quadrature measurement results, in which a proper SNU normalization is crucial. After that, the dynamic equalization is performed to compensate the mismatch of the polarization and phase during the transmission in quantum channel. This can be easily mapped to linear quantum optics, for instance, the phase or polarization rotation and beamsplitters (attenuation). Therefore, the key of the security is the static equalization, to obtain a reasonable quadrature measurement result.

The security of static equalization algorithms depends on proper calibration of SNU. The measurement result of t_j period, $\hat{D}^N_{t_j}$, is defined by a linear function of multiple sampled data $\{\hat{D}_{t_{j-k+i}}\}$,

$$\hat{D}^N_{t_j} = f_{dsp}(\hat{D}_{t_{j-k+1}},...,\hat{D}_{t_{j-k+N}}) = \Sigma^N_{i=1} f^i_{dsp}\hat{D}_{t_{j-k+i}}. \quad (67)$$

If SNU is calibrated from vacuum input following the same equalization procedure, then after SNU normalization, the measurement result forms a single-mode quadrature measurement result (with relative phase θ to LO) with certain temporal mode, $\Xi^{t_j}_{DSP}$, defined by the hardware features and equalization algorithms.

$$\hat{D}^{SNU}_{t_j} = \hat{A}^{\dagger}_{\Xi^{t_j}_{DSP}} exp(i\theta) + \hat{A}_{\Xi^{t_j}_{DSP}} exp(-i\theta) = \hat{X}^{\theta}_{\Xi^{t_j}_{DSP}}. \quad (68)$$

With digital polarization compensation, the polarization-diversity integrated coherent receiver (ICR) can be used to simplfy the system, in which optical polarization controller is no longer required, as shown in Fig. 37. Recently, a dual-polarization local LO CV-QKD system is experimentally demonstrated[145]. It performs the probability-shaping discrete-modulated 64 and 256 QAM with dual-polarization IQ modulator, and the polarization-diversity ICR is used at receiver side. With all compensation finished in digital domain, it can achieve 91.8 Mbps of secret key rate at 9.5 km and 24 Mbps at 25 km, which can support the high-speed connection within metropolitan distances.

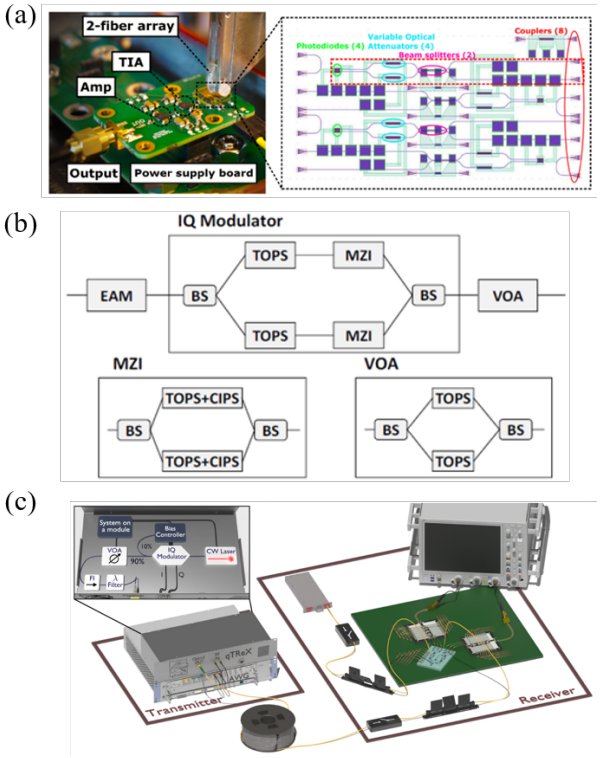

FIG. 38. The local LO CV-QKD systems with chip-based devices. (a) A silicon based receiver of the CV-QKD system. From Y. Pietri et al.[402]. (b) A InP transmitter of the CV-QKD system. From J. Aldama et al.[403]. (c) The 10 GBaud high-speed CV-QKD system with chip-based receiver. From A. Hajomer et al.[146]. (a) Reproduced with permission from OFC. M1I.2 (2023). Copyright 2023 The authors. (b) Reproduced with permission from OFC. M1I.3 (2023). Copyright 2023 The authors. (c) Reproduced with permission from arXiv 2305.19642 (2023). Copyright 2023 arXiv.

B. Chip-based local LO system

The advanced local LO CV-QKD system is developing towards compact module with photonics integration, benifiting from stability and scalability, which enables cost-effective deployments in large-scale. Recently, a seires of investigations have been carried out on high-performance chip-based transmitter and receiver for local LO CV-QKD system[146,334,402–404,444–447]. There are two mainstream fabrication platforms, Silicon-On-Insulator and III-V.

The Silicon-On-Insulator platform has the advantages of low cost and good ductility, which can utilize mature silicon

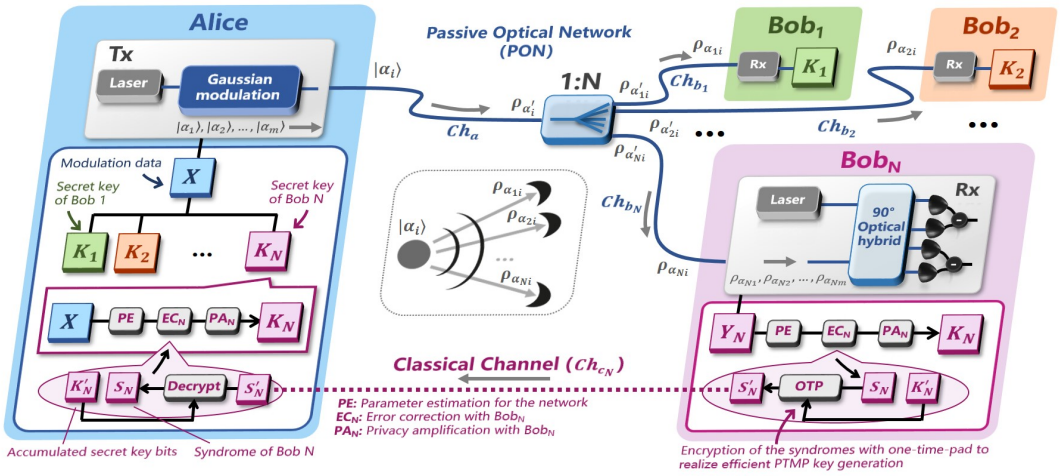

FIG. 39. The prepare-and-measure scheme of the point-to-multipoint CV-QKD protocol. From Y. Bian et al.[147]. Each coherent state prepared by Alice can be responded by all Bobs, for security analysis and secret key distillation. The syndrome is secretly transmitted to avoid the cross information leakage between different Bobs. Reproduced with permission from arXiv 2302.02391 (2023). Copyright 2023 arXiv.

CMOS processes to manufacture optical devices. The refractive index of the silicon waveguide is 3.42, which can form a significant refractive index difference with silicon dioxide, ensuring that the silicon waveguide can have a smaller waveguide bending radius, which is beneficial for high-density device integration. Recently, a Silicon-On-Insulator CV-QKD receiver shown in Fig. 38 (a) for a digital system is tested. The bandwidth is significantly enhanced to 250 MHz which makes detect the frequency division multiplexed quantum and pilot signal possible[402]. The maximal detection efficiency of the overall receiver is 0.26, with a shot noise-to-electronic-noise ratio of 20 dB at low frequencies and more than 7 dB for 250 MHz. Under the untrusted loss of 1.38 dB, a secret key rate of 280 kbps is achieved with excess noise of 0.1102 at Alice's side.

However, the Silicon-On-Insulator platform also suffers some issues, such as the low coupling efficiency for the optical signal input, which limits the detection efficiency, and the lack of an integrated high performance light source. The first issue can be solved through device optimization, such as low loss grating couplers and edge couplers. The latter issue is quite challenging, since silicon is not suitable for producing high performance integrated lasers.

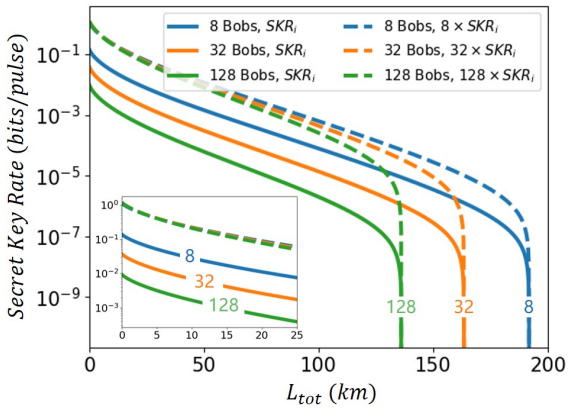

FIG. 40. The secret key rate of a single user (solid line) and the overall network (dashed line) with different number of accessed users.

One promising solution is using III-V platform such as InP, the other way is making heterogeneous integration, where the III-V chip-based laser is combined with the silicon chip via bonding or growing. Some recent researches have shown the feasibility of implementing the above two technical routines. J. Aldama et al. has demonstrated a InP CV-QKD transmitter[403] shown in Fig. 38 (b), including an electro-absorption modulator, an IQ modulator and a variable optical attenuator. These three devices are cascaded and integrated on one chip, supporting more than 1 GHz bandwidth. 0.4 and 2.3 Mbps secret key rate is achieved via a test with 11 km fiber and back-to-back connection, which verfies the possibility of using InP platform to produce a transmitter satisfying the requirement of CV-QKD. Once the laser diode is integrated to the InP chip, a fully integrated CV-QKD chip can be realized.

Recently, using the silicon based on-chip receiver with high-efficiency Ge photodiodes, a high-speed system at 10 GBaud is realized[146], as shown in Fig. 38 (c). The system is able to generate high secret key rates exceeding 0.7 Gbps over a distance of 5km and 0.3 Gbps over a distance of 10km, paving the way of the high-performance and compact CV-QKD system.

For chip-based laser diode, L. Li et al. have demonstrated two high-performance on-chip external cavity lasers based on Si3N4 platform for local LO CV-QKD system[404]. The secret key rate can reach 0.75 Mbps within 50 km fiber and the excess noise is controlled at 0.0579. In conclusion, the last obstacle to the fully chip-based CV-QKD system, which is the integrated light source, is expected to be solved through III-V platform with an overall or heterogeneous integration. The chip-based CV-QKD system is a promising way to real-

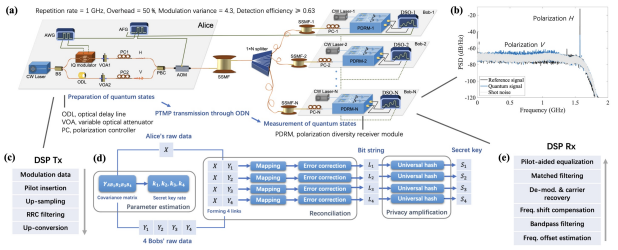

FIG. 41. The CV-QKD quantum access network using multiuser protocol. From Y. Bian et al.[451]. The network is based on the local LO scheme, where the transmitter generates quantum signal and pilot tone, which are multiplexed in different polarization directions and frequency. After the transmission in a passive optical network with an optical power splitter, different receivers at different site detects the signal independently, and distill secret key bits. Reproduced with permission from the authors. Copyright 2023 The Authors.

ize large-scale, small-size and cost-effective applications.

C. Point-to-multipoint system

Quantum access network is an efficient way to realize the point-to-multipoint connection between a network node and massive end users[448]. There are two mainstream routines, using optical switch with active time-multiplexing control between different end users[400], or passive optical nework (PON) with simpler network facilities. However, the $1 \times N$ beamsplitter in a PON significantly increases the equivalent channel loss for individual end users. Moreover, multiplexing techniques are required to seperate different users for upstream configuration[449,450]. Recently, a downstream point-to-multipoint CV-QKD scheme based on PON is proposed to solve the problems above[147]. The performance is significantly improved with a multiuser protocol, shown in Fig. 39.

The state preparation and measurement are similar to the Gaussian modulated protocols. One of the key points of this protocol is the multi-user parameter estimation and security analysis, in which all Bobs work together with Alice for a tighter estimation of the potential channel eavesdropping behavior. Specifically, Alice discloses part of the modulation data, denoted as X^{est}, and all Bobs disclose their corresponding detection data, $Y_1^{est}, Y_2^{est}, ..., Y_N^{est}$. With these data, the correlations between Alice and Bobs can be estimated, which forms a covariance matrix $\gamma_{AB_1B_2...B_N}$ consists of all trusted modes. Further, the secret key rate between Alice and each Bob can be calculated with $\gamma_{AB_1B_2...B_N}$.

The other key point is the parallel key distillation for all end users, which enhances the secret key rate of the overall network. In this protocol, each prepared quantum state can be measured by all users. Several techniques are developed to suppress the negative influence of the correlation between different end users on system performance. Therefore, all users can generate independent secret keys with the sender at the same time. The simulation results in Y. Bian et al. show the ability of supporting 128 end users with more than 100 km distance (see Fig. 40), which can well satisfy the multiuser interconnection requirements within metropolitan distances[147].

A high-rate CV-QKD access network is realized, as shown in Fig. 41. For the transmitter, quantum signal is generated with an IQ modulator, which is multiplexed with pilot tone signal with frequency division multiplexing and polarization multiplexing. For the receiver, the de-multiplexing is realized by a polarization controller and a polarization beamsplitter. Then, quantum signal and pilot tone are seperately detected by heterodyne detection. The average secret key rate of each user can reach 4.1 Mbps at 15 km when the network capacity is 4, with the repetition frequency of 500 MHz[463]. Further, the capacity of the network is extended to 8, and the secret key rate is 7.44 Mbps at 6 km for each user[451]. This result can well support the quantum access network, such as linking the end users within a campus (see Fig. 42).

VI. PRACTICAL SECURITY

The information-theoretical security of the CV-QKD protocols using ideal devices has been strictly proved. However, in practical implementations, the unperfect devices may introduce security loopholes, which can be used by Eve to attack the systems. Correspondingly, countermeasures are proposed to defense the attacks and close the security loopholes, which ensure the practical security.

A. Attacks and countermeasures

The theoretical security analysis of CV-QKD is based on the assumption that Alice and Bob are both trusted, where the attack by the eavesdropper can only be performed in channel, without affecting the devices of the legitimate parties. However, the source and the detector of a practical CV-QKD system cannot satisfy the requirement that the devices can be perfect and fully trusted, since the actual optical and electrical devices inevitably introduce the imperfections. These imperfec-

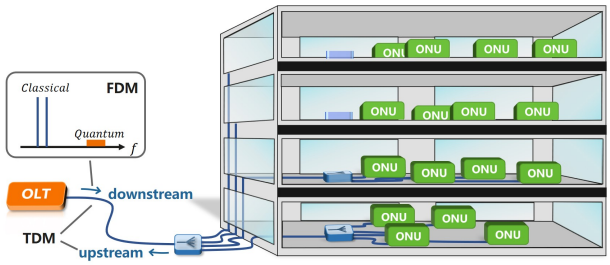

FIG. 42. The future quantum access network with point-to-multipoint protocol. The OLT means the optical line terminal, and the ONU means the optical network unit. The network can be an optical distribution network, which is widely deployed by the fiber-based classical optical communication network, using as the access network. The quantum signal and classical signals can be co-transmitted with frequency division multiplexing (FDM), while the downstream and upstream signals can be transmitted with time division multiplexing.

TABLE XII. The attacks and the corresponding countermeasures of CV-QKD systems.

Attack	**Year**	**Transmitter / Receiver**	**Target component**	**Countermeasures**
Imperfect coherent source attack[452]	2013	Transmitter	Coherent source	Monitoring Gaussian modulation
LO fluctuation attack[405]	2013	Receiver	LO	Monitoring LO intensity
Calibration attack[408]	2013	Receiver	LO	Monitoring LO intensity
Wavelength attack[407]	2013	Receiver	Detector	Monitoring LO wavelength
Trojan-horse attack[453]	2015	Transmitter	Back reflection light	Adding isolators
Saturation attack[454]	2016	Receiver	Detector	Monitoring detector status
Polarization attack[455]	2018	Receiver	LO	Monitoring SNU calibration
Homodyne-detector-blinding attack[456]	2018	Receiver	Detector	Monitoring detector status
Laser seeding attack[457]	2019	Transmitter	Laser diode	Monitoring output signal intensity
Reduced optical attenuation attack[458]	2019	Transmitter	Variable optical attenuator	Monitoring signal attenuation level
Reference pulse attack[459–461]	2019	Receiver	Reference pulse	Monitoring SNU calibration
Modified LO fluctuation attack[462]	2023	Receiver	LO / pilot tone	Real-time LO intensity monitoring

tions can be used by the eavesdropper to increase the knowledge to the legitimate parties, which weakens the security of the system. According to the different attack targets, the hacking schemes against the CV-QKD system can be classified into hacking schemes against the LO, the source, and the measurement devices. The related attack and defense schemes are summarized in Table XII. At present, all the hacking schemes can be defended, and the research of hacking is mainly to better improve the practical security of the system.

By manipulating the LO, the representative attack strateiges against the CV-QKD systems, such as the local oscillator fluctuation attack[405,462], calibration attack[408], polarization attack[455] and so on, can be performed. It is assumed in the theoretical security analysis of CV-QKD that the LO is trustworthy and will not be controlled by the eavesdropper, but in the actual in-line LO system, since the LO needs to be transmitted over the channel, it is very likely to be controlled by an eavesdropper. Variations in the intensity of the LO can cause the SNU calibrated with the measurement results to be different from the system's true value, which leads to a biased estimation of the system's excess noise, leaving a security loophole. These attack schemes can be defended by monitoring the mean and variance of the intensity of the LO.

The local LO system is proposed to defend the attack at the LO by generating LO locally. Moreover, since the classical pilot tone is transmitted in the unsecured channel, some attacking schemes at the pilot tone are proposed such as the reference pulse attack and so on[459–461].

Aiming at the source, the imperfect coherent source attack[452], Trojan-horse attack[453], laser seeding attack[457] and reduced optical attenuation attack[458] are developed. In a Trojan-horse attack, Eve detects modulation information in the CV-QKD system by injecting bright light pulses and analyzing the reflected pulses. These reflected pulses originate from refractive index changes, such as density fluctuations at the junction between two optical devices or inside the optical devices. The reflected pulse signals contain the markings of the optical modulator (used to encode the quantum state), which allows Eve, the eavesdropper, to extract part of the original key. The counter measure of the source attack is using an optical isolator to prevent the injected light and a source monitoring detector to achieve the output of the system.

Exploiting the unlinear behavior of the homodyne or heterodyne detectors, the detector saturation attack[454] and the homodyne-detector-blinding attack[456] are developed. A detector saturation attack involves saturating the detector by increasing the light intensity so as to reduce the output signal variance, which reduces the increase in excess noise caused by interception-retransmission operations, making it impossible for the legitimate parties to detect the eavesdropping behavior. A strategy to defend against the detector saturation attack scheme can be realized by monitoring the operating state of the detector by detecting the relationship between the output signal and the channel transmittance.

Taking advantage of the vulnerability that the beam splitting ratio of the beam splitter at both output ends depends on the wavelength, a wavelength attack scheme for real CV-QKD systems has been proposed. The strategy to defend against this attack scheme can be realized by adding filters in front of the detector and monitoring the intensity of the LO in real time.

Researchers have also proposed a series of corresponding countermeasures to address the potential security loopholes in

TABLE XIII. The grading levels and methodologies of countermeasures.

Level	Evaluation	Description
C_3	Solution secure	The imperfections of devices in the CV-QKD system has been included in the security analysis, or there is no security risk.
C_2	Solution robust	It can effectively defense the specific attack in experiments, but it has not yet been included in the security analysis.
C_1	Solution partially effective	This solution is effective only for certain attack strategies, but is ineffective for others or modified versions of original attack.
C_0	Insecure	Security vulnerabilities have been proven to exist, but there is currently no effective countermeasures.
C_X	No test	The imperfections of the practical devices are suspected to exist, but testing and verification have not yet been conducted.

the practical CV-QKD system, including recognizing whether the system is under the attack[464]. In order to better evaluate the degree of harm caused by different attack strategies and the effectiveness of corresponding countermeasures, it is necessary to conduct grading evaluation for different countermeasures, and quantify their defense performance[465]. The effectiveness of countermeasures is divided into four levels, with specific levels and grading methodologies as shown in Table. XIII.

The above grading scheme for countermeasures mainly focuses on their effectiveness, without paying attention to the "cost" of countermeasures. We focuses on the attacker's point of view, and is more concerned with the effect of countermeasures on the risk of attack. The "cost" is mainly related to needs of users whose devices are being attacked. For example, when the security demand for users is high, that is, they need to protect to national-level secrets, the defender will not consider the "cost" of defense, but rather the the effectiveness of countermeasures as the main consideration. When the user demand is low, that is, only personal information needs to be protected, defenders need to primarily consider the "cost" of countermeasures. Here, a certain amount of cost is discussed concerning practical CV-QKD devices. The CV-QKD equipment is a set of communication equipment that integrates electronics and optical devices, and the "cost" of countermeasures can be discussed and analyzed in the following aspects: the price of the equipment, the difficulty of integrating the defense scheme, the difficulty of the technical implementation, the computational power and the number of original keys sacrificed in the postprocessing process required for defense.

In summary, the relationship between defense "cost" and defense effectiveness is a trade-off, requiring experts from multiple fields to combine different practical application scenarios to form a more comprehensive evaluation system.

B. Measurement-device-independent system

In order to completely eliminate the security loopholes due to the imperfection of devices, completely device-independent QKD protocols have been proposed. This type of protocol does not rely on any security assumptions for QKD devices, and thus is one of the most secure protocols that can guarantee its security even when the device is completely controlled by an eavesdropper. However, completely device-independent protocol face significant experimental challenges since they require key acquisition using the loophole-free Bell test. The key rate of such protocols is too low under the existing experimental conditions, which makes it difficult to meet the usage requirements. As a result, the concept of semi-device-independent CV-QKD protocols has been proposed, which is a good compromise between security and performance, and can have high security and high key generation rate at the same time. The main idea of the semi-device-independent CV-QKD protocol is that the security of some devices in the system is not required, while other devices are considered to be trusted. Typical semi-device-independent protocols are the CV-SDI QKD protocol and the CV-MDI QKD protocol. In this part, we mainly introduce the process of the CV-MDI QKD system.

In an CV-MDI QKD, both two legitimate parties, namely Alice and Bob, are the transmitter, while the detection is performed by the untrusted third party. Therefore, the protocol is naturally immune to any attacks at the receiver's side. For the coherent state CV-MDI QKD, normally the legitimate parties adopt Gaussian modulation, they send the Gaussian modulated coherent states to the third party Charlie, who performs the continuous-variable Bell-state detection. Specifically, Charlie uses a beamsplitter to interfere the two received coherent state, then uses two homodyne detectors to measure the output results. After that, Charlie announces the detection results, and the legitimate parties correct their data with the results announced by Charlie. Finally, Alice and Bob use their corrected data to perform the postprocessing and get final secret keys. During the above process, the legitimate parties can both correct their data, or correct the data by only one side. The theroetical analysis shows that the CV-MDI QKD is limited by the symmetry of the protocol. When Charlie is deployed at the center, where the loss of the Alice-Charlie link is equal to that of the Bob-Charlie link, the transmisson distance of the protocol is the worst. When Charlie is near one of the legitimate parties, the performance of the protocol is enhanced.

The first proof-of-principle of CV-MDI QKD system is demonstrated in 2015, shown in Fig. 43 (a). With free space optical devices working in 1064 nm band, it demonstrates the high-rate characteristic of CV-MDI QKD[177]. Compared with the qubit-based protocols, the secret key rate increases by 3

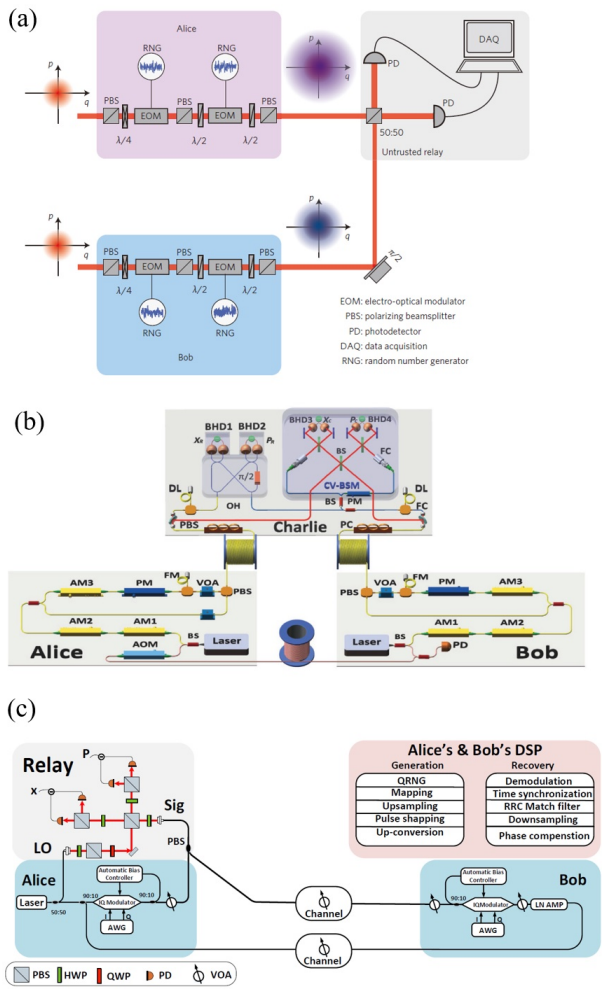

FIG. 43. The experimental schemes of the CV-MDI QKD. (a) The first experimental demonstration. From S. Pirandola et al.[177]. (b) The first CV-MDI QKD with optical fiber links. From Y. Tian et al.[466]. (c) The first experimental demonstration without locking systems. From A. Hajomer et al.[467]. (a) Reproduced with permission from Nat. Photonics 9, 397 (2015). Copyright 2015 Nature Publishing Group. (b) Reproduced with permission from Optica 9, 492 (2022). Copyright 2022 Optica Publishing Group. (c) Reproduced with permission from OFC. M2I.2 (2023). Copyright 2023 The Authors.

orders of magnitude within metropolitan distances, providing a promising way of building the pratical secure metropolitan CV-QKD network. The difficulties of the experimental CV-MDI QKD is the implementation of the CV Bell detection, which requires highly efficient photodetectors, locking systems, and the free space devices.

Later, the recent progresses of CV-MDI QKD system solve the issues left above. As shown in Fig. 43 (b), the CV-MDI QKD with optical fiber links is realized in 2022, where the optical phase locking, phase estimation, real-time phase feedback and quadrature remapping are developed to realize an accurate CV Bell-state measurement. In this work, the optical phase-locked loop is a key technique to make the two lasers used for Alice's and Bob's QKD laser source have the identical center frequency. Part of the Alice's laser beam is frequency-up-shifted by 80 MHz and sent to Bob's station for frequency-locking. Moreover, a free space time-domain homodyne detector is developed, which can reach the detection efficiency of 99%. The secret key rate can break 0.19 bit/pulse over a 10 km optical fiber, which paves the way of a high-rate metropolitan MDI-QKD network[466].

In 2023, the frequency and optical phase locking in a CV-MDI QKD system is removed by using a new relay structure based on a polarization-based 90-degree optical hybrid and a well-designed DSP pipeline[467], shown in Fig. 43 (c). Moreover, this system uses continuous-wave laser with digital pulse shaping and digital time synchronization, therefore the additional amplitude modulation for pulse generation and a delay line for time synchronization is unneccessary. A secret key rate of 600 kbps over 2 dB loss channel is achieved.

VII. SUMMARY AND OUTLOOK

In this review, we have presented the development of the continuous-variable quantum key distribution system, including basic protocols and security analysis, system structures and demonstrations, advanced system development directions, as well as practical security. The key challenges facing by different system schemes and solutions are summarized, showing the methodology towards a high-performance system.

There is still the need to develop and design high-performance protocol, including the deep exploration on the insight between shot-noise-unit and security, and developing novel protocols with the secret key rate exceeding Gaussian protocols under same launch energy, which further approaching the fundamental rate-distance limit of point-to-point quantum key distribution while still keeps simple system structure. In practice, different secret key rates might be considered, for instance, with respect to individual, collective, or fully coherent attacks. The choice of these rates may also be associated with a specific sublevel of security to be reached.

Furthermore, the system implementations should move toward higher integration, higher speed and longer transmission distances. Firstly, miniaturization of the system by photonic integrated circuit is crucial, which significantly reduces the system size and broadens the application scenarios. Thanks to the well compatibility, the on-chip integration of CV-QKD systems can draw on classical chip-based optical communication systems. But for the receivers, the detection of weak quantum signals significantly raises the requirements on coherent detectors for high gain and low noise, where the performance of trans-impedance amplifier is the main bottleneck, which requires more attentions. Secondly, high speed system requires high repetition frequency quantum signal modulation, wide bandwidth detection and high throughout data processing. The high repetition frequency introduces new sources of excess noise, such as the dispersion, therefore compensations in physical layer or digital layer are further required for reduce the excess noise. It's crucial to design the better digital algorithms and frame structures to compen-

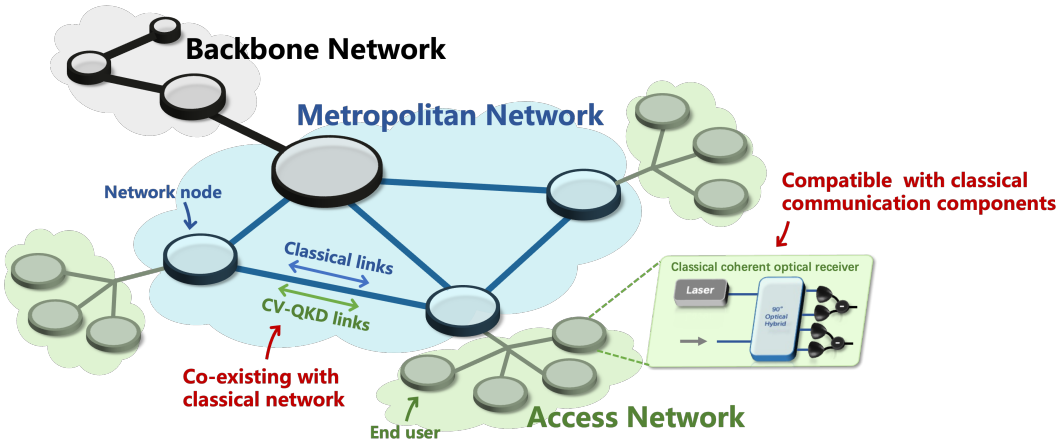

FIG. 44. Structure of the future quantum secure network, which consists of the backbone network, the metropolitan network and the access network. Here, the backbone network connects the main network node of different cities, the metropolitan network connects the nodes in a city, and the access network connects the network node with end users.

sate the impairments caused by the low effective-number-of-bits AD converter, which works at high speed. In the aspect of data processing, the pressure on computational resources comes mainly from error correction, wherefore we will need to develop the high throughout and high-efficient error correction strategies in the suitable hardware platform. Thirdly, to achieve a long-distance system, we need to design the high-performance error correction codes that can operate at extremely lower SNR (such as -30 dB), and develop novel system structure to decrease the crosstalk and excess noise.

Finally, quantum hacking and countermeasures are an important and growing area. Closing the side channel at the transmitter site and the accurate SNU calibration are two crucial points for the practical security of the system.

In general, up to now, the potential of using continuous-variable quantum key distribution technique to support high-performance quantum networks within metropolitan and access distances has been demonstrated by the high-speed system implementations, chip-based integrations and field networking tests, and as shown in Fig. 44, it is expected to be highly compatible with the existing optical network infrastructures, enabling the large-scale and cost-effective deployments, and will bring this technology a step closer to a wide range of applications within future quantum networks[468].

ACKNOWLEDGMENTS

We are thankful for the enlightening discussions with and helpful comments from reviewers and numerous colleagues, including R. Goncharov, P. Huang, L. Huang, Y. Li, Q. Liao, T. Matsuura, S. Pirandola, S. Sarmiento, A. Vidiella-Barranco, T. Wang, X. Wang and B. Xu. This work was supported by the National Natural Science Foundation of China (62001044, 62201013), the Basic Research Program of China (JCKY2021210B059), the Equipment Advance Research Field Foundation (315067206), and the Fund of State Key Laboratory of Information Photonics and Optical Communications (IPOC2021ZT02).

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing , 175–179 (1984).
[2] A. K. Ekert, "Quantum cryptography based on bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, *et al.*, "The security of practical quantum key distribution," Rev. Mod. Phys. **81**, 1301–1350 (2009).
[5] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, *et al.*, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
[6] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, *et al.*, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
[7] Y. Cao, Y. Zhao, Q. Wang, J. Zhang, S. X. Ng, *et al.*, "The evolution of quantum key distribution networks: On the road to the qinternet," IEEE Commun. Surv. Tutor. **24**, 839–894 (2022).
[8] C. Portmann and R. Renner, "Security in quantum cryptography," Rev. Mod. Phys. **94**, 025008 (2022).
[9] W. K. Wootters, W. K. Wootters, and W. H. Zurek, "A single quantum cannot be cloned," Nature **299**, 802–803 (1982).
[10] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, "Practical challenges in quantum key distribution," npj Quantum Inf. **2**, 1–12 (2016).
[11] N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304 (2000).
[12] K. Inoue, E. Waks, and Y. Yamamoto, "Differential phase shift quantum key distribution," Phys. Rev. Lett. **89**, 037902 (2002).
[13] W.-Y. Hwang, "Quantum key distribution with high loss: toward global secure communication," Phys. Rev. Lett. **91**, 057901 (2003).
[14] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations," Phys. Rev. Lett. **92**, 057901 (2004).
[15] J. Barrett, L. Hardy, and A. Kent, "No signaling and quantum key distribution," Phys. Rev. Lett. **95**, 010503 (2005).
[16] D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, "Fast and simple one-way quantum key distribution," Appl. Phys. Lett. **87** (2005).
[17] X.-B. Wang, "Beating the photon-number-splitting attack in practical quantum cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
[18] H.-K. Lo, X. Ma, and K. Chen, "Decoy state quantum key distribution," Phys. Rev. Lett. **94**, 230504 (2005).
[19] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, *et al.*, "Device-independent security of quantum cryptography against collective attacks," Phys. Rev. Lett. **98**, 230501 (2007).

[20]H. Inamori, N. Lütkenhaus, and D. Mayers, "Unconditional security of practical quantum key distribution," Eur. Phys. J. D **41**, 599–627 (2007).

[21]S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, *et al.*, "Device-independent quantum key distribution secure against collective attacks," New J. Phys. **11**, 045021 (2009).

[22]L. Masanes, S. Pironio, and A. Acín, "Secure device-independent quantum key distribution with causally independent measurement devices," Nat. Commun. **2**, 238 (2011).

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

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

[25]T. Sasaki, Y. Yamamoto, and M. Koashi, "Practical quantum key distribution protocol without monitoring signal disturbance," Nature **509**, 475–478 (2014).

[26]M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, "Overcoming the rate–distance limit of quantum key distribution without quantum repeaters," Nature **557**, 400–403 (2018).

[27]R. Arnon-Friedman, F. Dupuis, O. Fawzi, R. Renner, and T. Vidick, "Practical device-independent quantum cryptography via entropy accumulation," Nat. Commun. **9**, 459 (2018).

[28]U. Vazirani and T. Vidick, "Fully device independent quantum key distribution," Commun. ACM **62**, 133–133 (2019).

[29]Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental quantum key distribution with decoy states," Phys. Rev. Lett. **96**, 070502 (2006).

[30]C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, *et al.*, "Experimental long-distance decoy-state quantum key distribution based on polarization encoding," Phys. Rev. Lett. **98**, 010505 (2007).

[31]D. Rosenberg, J. W. Harrington, P. R. Rice, P. A. Hiskett, C. G. Peterson, *et al.*, "Long-distance decoy-state quantum key distribution in optical fiber," Phys. Rev. Lett. **98**, 010503 (2007).

[32]T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, *et al.*, "Experimental demonstration of free-space decoy-state quantum key distribution over 144 km," Phys. Rev. Lett. **98**, 010504 (2007).

[33]Z. Yuan, A. Sharpe, and A. Shields, "Unconditionally secure one-way quantum key distribution using decoy pulses," Appl. Phys. Lett. **90** (2007).

[34]Z.-Q. Yin, Z.-F. Han, W. Chen, F.-X. Xu, Q.-L. Wu, *et al.*, "Experimental decoy state quantum key distribution over 120 km fibre," Chinese Phys. Lett. **25**, 3547 (2008).

[35]Q. Wang, W. Chen, G. Xavier, M. Swillo, T. Zhang, *et al.*, "Experimental decoy-state quantum key distribution with a sub-poissionian heralded single-photon source," Phys. Rev. Lett. **100**, 090501 (2008).

[36]A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, "Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate," Opt. Express **16**, 18790–18797 (2008).

[37]D. Rosenberg, C. G. Peterson, J. Harrington, P. R. Rice, N. Dallmann, *et al.*, "Practical long-distance quantum key distribution system using decoy levels," New J. Phys. **11**, 045009 (2009).

[38]Z. Yuan, A. Dixon, J. Dynes, A. Sharpe, and A. Shields, "Practical gigahertz quantum key distribution based on avalanche photodiodes," New J. Phys. **11**, 045019 (2009).

[39]Y. Liu, T.-Y. Chen, J. Wang, W.-Q. Cai, X. Wan, *et al.*, "Decoy-state quantum key distribution with polarized photons over 200 km," Opt. Express **18**, 8587–8594 (2010).

[40]T.-Y. Chen, J. Wang, H. Liang, W.-Y. Liu, Y. Liu, *et al.*, "Metropolitan all-pass and inter-city quantum communication network," Opt. Express **18**, 27217–27225 (2010).

[41]J.-Y. Wang, B. Yang, S.-K. Liao, L. Zhang, Q. Shen, *et al.*, "Direct and full-scale experimental verifications towards ground–satellite quantum key distribution," Nat. Photonics **7**, 387–393 (2013).

[42]A. Boaron, G. Boso, D. Rusca, C. Vulliez, C. Autebert, *et al.*, "Secure quantum key distribution over 421 km of optical fiber," Phys. Rev. Lett. **121**, 190502 (2018).

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

[44]Y. Liu, T.-Y. Chen, L.-J. Wang, H. Liang, G.-L. Shentu, *et al.*, "Experimental measurement-device-independent quantum key distribution," Phys. Rev. Lett. **111**, 130502 (2013).

[45]T. F. Da Silva, D. Vitoreti, G. Xavier, G. Do Amaral, G. Temporão, *et al.*, "Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits," Phys. Rev. A **88**, 052303 (2013).

[46]Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, *et al.*, "Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution," Phys. Rev. Lett. **112**, 190503 (2014).

[47]Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, *et al.*, "Measurement-device-independent quantum key distribution over 200 km," Phys. Rev. Lett. **113**, 190501 (2014).

[48]Y.-L. Tang, H.-L. Yin, S.-J. Chen, Y. Liu, W.-J. Zhang, *et al.*, "Field test of measurement-device-independent quantum key distribution," IEEE J. Quantum Electron. **21**, 116–122 (2014).

[49]C. Wang, X.-T. Song, Z.-Q. Yin, S. Wang, W. Chen, *et al.*, "Phase-reference-free experiment of measurement-device-independent quantum key distribution," Phys. Rev. Lett. **115**, 160502 (2015).

[50]R. Valivarthi, I. Lucio-Martinez, P. Chan, A. Rubenok, C. John, *et al.*, "Measurement-device-independent quantum key distribution: from idea towards application," J. Mod. Opt. **62**, 1141–1150 (2015).

[51]H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, *et al.*, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. Rev. Lett. **117**, 190501 (2016).

[52]Y.-L. Tang, H.-L. Yin, Q. Zhao, H. Liu, X.-X. Sun, *et al.*, "Measurement-device-independent quantum key distribution over untrustful metropolitan network," Phys. Rev. X **6**, 011024 (2016).

[53]G.-Z. Tang, S.-H. Sun, F. Xu, H. Chen, C.-Y. Li, *et al.*, "Experimental asymmetric plug-and-play measurement-device-independent quantum key distribution," Phys. Rev. A **94**, 032326 (2016).

[54]L. Comandar, M. Lucamarini, B. Fröhlich, J. Dynes, A. Sharpe, *et al.*, "Quantum key distribution without detector vulnerabilities using optically seeded lasers," Nat. Photonics **10**, 312–315 (2016).

[55]F. Kaneda, F. Xu, J. Chapman, and P. G. Kwiat, "Quantum-memory-assisted multi-photon generation for efficient quantum information processing," Optica **4**, 1034–1037 (2017).

[56]C. Wang, Z.-Q. Yin, S. Wang, W. Chen, G.-C. Guo, *et al.*, "Measurement-device-independent quantum key distribution robust against environmental disturbances," Optica **4**, 1016–1023 (2017).

[57]R. Valivarthi, Q. Zhou, C. John, F. Marsili, V. B. Verma, *et al.*, "A cost-effective measurement-device-independent quantum key distribution system for quantum networks," Quantum Sci. Technol. **2**, 04LT01 (2017).

[58]H. Liu, J. Wang, H. Ma, and S. Sun, "Polarization-multiplexing-based measurement-device-independent quantum key distribution without phase reference calibration," Optica **5**, 902–909 (2018).

[59]K. Wei, W. Li, H. Tan, Y. Li, H. Min, *et al.*, "High-speed measurement-device-independent quantum key distribution with integrated silicon photonics," Phys. Rev. X **10**, 031030 (2020).

[60]M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, *et al.*, "Experimental quantum key distribution beyond the repeaterless secret key capacity," Nat. Photonics **13**, 334–338 (2019).

[61]S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, *et al.*, "Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system," Phys. Rev. X **9**, 021046 (2019).

[62]Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, *et al.*, "Experimental twin-field quantum key distribution through sending or not sending," Phys. Rev. Lett. **123**, 100505 (2019).

[63]X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, "Proof-of-principle experimental demonstration of twin-field type quantum key distribution," Phys. Rev. Lett. **123**, 100506 (2019).

[64]X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, *et al.*, "Implementation of quantum key distribution surpassing the linear rate-transmittance bound," Nat. Photonics **14**, 422–425 (2020).

[65]J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, *et al.*, "Sending-or-not-sending with independent lasers: Secure twin-field quantum key distribution over 509 km," Phys. Rev. Lett. **124**, 070501 (2020).

[66]M. Pittaluga, M. Minder, M. Lucamarini, M. Sanzaro, R. I. Woodward, *et al.*, "600-km repeater-like quantum communications with dual-band stabilization," Nat. Photonics **15**, 530 – 535 (2020).

[67]J.-P. Chen, C. Zhang, Y. Liu, C. Jiang, W.-J. Zhang, *et al.*, "Twin-field quantum key distribution over a 511 km optical fibre linking two distant metropolitan areas," Nat. Photonics **15**, 570–575 (2021).

[68]S. Wang, Z.-Q. Yin, D.-Y. He, W. Chen, R.-Q. Wang, *et al.*, "Twin-field

quantum key distribution over 830-km fibre," Nat. Photonics **16**, 154–161 (2022).
[69]Y. Liu, W.-J. Zhang, C. Jiang, J.-P. Chen, C. Zhang, *et al.*, "Experimental twin-field quantum key distribution over 1000 km fiber distance," Phys. Rev. Lett. **130**, 210801 (2023).
[70]C. Ma, W. D. Sacher, Z. Tang, J. C. Mikkelsen, Y. Yang, *et al.*, "Silicon photonic transmitter for polarization-encoded quantum key distribution," Optica **3**, 1274–1278 (2016).
[71]P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, *et al.*, "Chip-based quantum key distribution," Nat. Commun. **8**, 13984 (2017).
[72]P. Sibson, J. E. Kennard, S. Stanisic, C. Erven, J. L. O'Brien, *et al.*, "Integrated silicon photonics for high-speed quantum key distribution," Optica **4**, 172–177 (2017).
[73]D. Bunandar, A. Lentine, C. Lee, H. Cai, C. M. Long, *et al.*, "Metropolitan quantum key distribution with silicon photonics," Phys. Rev. X **8**, 021009 (2018).
[74]Y. Ding, D. Bacco, K. Dalgaard, X. Cai, X. Zhou, *et al.*, "High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits," npj Quantum Inf. **3**, 25 (2017).
[75]T. K. Paraïso, I. De Marco, T. Roger, D. G. Marangon, J. F. Dynes, *et al.*, "A modulator-free quantum key distribution transmitter chip," npj Quantum Inf. **5**, 42 (2019).
[76]C. Lee, Z. Zhang, G. R. Steinbrecher, H. Zhou, J. Mower, *et al.*, "Entanglement-based quantum communication secured by nonlocal dispersion cancellation," Phys. Rev. A **90**, 062331 (2014).
[77]J.-Y. Guan, Z. Cao, Y. Liu, G.-L. Shen-Tu, J. S. Pelc, *et al.*, "Experimental passive round-robin differential phase-shift quantum key distribution," Phys. Rev. Lett. **114**, 180502 (2015).
[78]H. Takesue, T. Sasaki, K. Tamaki, and M. Koashi, "Experimental quantum key distribution without monitoring signal disturbance," Nat. Photonics **9**, 827 (2015).
[79]S. Wang, Z.-Q. Yin, W. Chen, D.-Y. He, X.-T. Song, *et al.*, "Experimental demonstration of a quantum key distribution without signal disturbance monitoring," Nat. Photonics **9**, 832–836 (2015).
[80]T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, *et al.*, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," New J. Phys. **17**, 022002 (2015).
[81]B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, *et al.*, "Provably secure and practical quantum key distribution over 307 km of optical fibre," Nat. Photonics **9**, 163–168 (2015).
[82]M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, *et al.*, "High-dimensional quantum cryptography with twisted light," New J. Phys. **17**, 033033 (2015).
[83]A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, *et al.*, "High-dimensional intracity quantum cryptography with structured photons," Optica **4**, 1006–1010 (2017).
[84]Y.-H. Li, Y. Cao, H. Dai, J. Lin, Z. Zhang, *et al.*, "Experimental round-robin differential phase-shift quantum key distribution," Phys. Rev. A **93**, 030302 (2016).
[85]Z. Yuan, B. Fröhlich, M. Lucamarini, G. Roberts, J. Dynes, and A. Shields, "Directly phase-modulated light source," Phys. Rev. X **6**, 031044 (2016).
[86]N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier, "Provably secure and high-rate quantum key distribution with time-bin qudits," Sci. Adv. **3**, e1701491 (2017).
[87]S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," Nature communications **8**, 15043 (2017).
[88]A. Tanaka, M. Fujiwara, K.-i. Yoshino, S. Takahashi, Y. Nambu, *et al.*, "High-speed quantum key distribution system for 1-mbps real-time key generation," IEEE J. Quantum Electron. **48**, 542–550 (2012).
[89]M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, *et al.*, "Efficient decoy-state quantum key distribution with quantified security," Opt. Express **21**, 24550–24565 (2013).
[90]B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, *et al.*, "Long-distance quantum key distribution secure against coherent attacks," Optica **4**, 163–167 (2017).
[91]Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, *et al.*, "10-mb/s quantum key distribution," J. Light. Technol. **36**, 3427–3433 (2018).
[92]W. Li, L. Zhang, H. Tan, Y. Lu, S.-K. Liao, *et al.*, "High-rate quantum key distribution exceeding 110 mb s–1," Nat. Photonics **17**, 416–421 (2023).
[93]C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, *et al.*, "Current status of the darpa quantum network," in *Quantum Information and Computation III*, Vol. 5815 (SPIE, 2005) pp. 138–149.
[94]M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, *et al.*, "The secoqc quantum key distribution network in vienna," New J. Phys. **11**, 075001 (2009).
[95]T.-Y. Chen, H. Liang, Y. Liu, W.-Q. Cai, L. Ju, *et al.*, "Field test of a practical secure communication network with decoy-state quantum cryptography," Opt. Express **17**, 6540–6549 (2009).
[96]M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, *et al.*, "Field test of quantum key distribution in the tokyo qkd network," Opt. Express **19**, 10387–10409 (2011).
[97]T.-Y. Chen, X. Jiang, S.-B. Tang, L. Zhou, X. Yuan, *et al.*, "Implementation of a 46-node quantum metropolitan area network," npj Quantum Inf. **7**, 134 (2021).
[98]J. Yin, Y. Cao, Y. Li, S. Liao, L. Zhang, *et al.*, "Satellite-based entanglement distribution over 1200 kilometers," Science **356**, 1140 – 1144 (2017).
[99]S.-K. Liao, W.-Q. Cai, W.-Y. Liu, L. Zhang, Y. Li, *et al.*, "Satellite-to-ground quantum key distribution," Nature **549**, 43–47 (2017).
[100]J.-G. Ren, P. Xu, H.-L. Yong, L. Zhang, S. Liao, *et al.*, "Ground-to-satellite quantum teleportation," Nature **549**, 70–73 (2017).
[101]J. Yin, Y. Cao, Y. Li, J.-G. Ren, S. Liao, *et al.*, "Satellite-to-ground entanglement-based quantum key distribution," Phys. Rev. Lett. **119 20**, 200501 (2017).
[102]S. Liao, W. Cai, J. Handsteiner, B. Liu, J. Yin, *et al.*, "Satellite-relayed intercontinental quantum network." Phys. Rev. Lett. **120 3**, 030501 (2018).
[103]Y.-A. Chen, Q. Zhang, T.-Y. Chen, W.-Q. Cai, S.-K. Liao, *et al.*, "An integrated space-to-ground quantum communication network over 4,600 kilometres," Nature **589**, 214–219 (2021).
[104]T. C. Ralph, "Continuous variable quantum cryptography," Phys. Rev. A **61**, 010303 (1999).
[105]N. J. Cerf, M. Lévy, and G. V. Assche, "Quantum distribution of gaussian keys using squeezed states," Phys. Rev. A **63**, 052311 (2001).
[106]F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
[107]C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, *et al.*, "Quantum cryptography without switching," Phys. Rev. Lett. **93**, 170504 (2004).
[108]S. L. Braunstein and P. van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513–577 (2005).
[109]X.-B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with gaussian states," Phys. Rep. **448**, 1–111 (2007).
[110]C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, *et al.*, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621–669 (2012).
[111]P. K. Lam and T. C. Ralph, "Continuous improvement," Nat. Photonics **7**, 350 (2013).
[112]E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: principle, security and implementations," Entropy **17**, 6072–6092 (2015).
[113]N. J. Cerf, G. Leuchs, and E. S. Polzik, *Quantum information with continuous variables of atoms and light* (World Scientific, 2007).
[114]A. Furusawa and N. Takei, "Quantum teleportation for continuous variables and related quantum information processing," Phys. Rep. **443**, 97–119 (2007).
[115]U. L. Andersen, G. Leuchs, and C. Silberhorn, "Continuous-variable quantum information processing," Laser Photonics Rev. **4**, 337–354 (2010).
[116]R. Van Meter, *Quantum networking* (John Wiley & Sons, 2014).
[117]G. Adesso, S. Ragy, and A. R. Lee, "Continuous variable quantum information: Gaussian states and beyond," Open Syst. Inf. Dyn. **21**, 1440001 (2014).
[118]U. L. Andersen, J. S. Neergaard-Nielsen, P. Van Loock, and A. Furusawa, "Hybrid discrete-and continuous-variable quantum information," Nat. Phys. **11**, 713–719 (2015).
[119]G. Kurizki, P. Bertet, Y. Kubo, K. Mølmer, D. Petrosyan, *et al.*, "Quantum technologies with hybrid systems," Proc. Natl. Acad. Sci. **112**, 3866–3873 (2015).
[120]A. Serafini, *Quantum continuous variables: a primer of theoretical meth-*

ods (CRC press, 2017).
[121] R. García-Patrón and N. J. Cerf, "Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution," Phys. Rev. Lett. **97**, 190503 (2006).
[122] M. Navascués, F. Grosshans, and A. Acín, "Optimality of gaussian attacks in continuous-variable quantum cryptography," Phys. Rev. Lett. **97**, 190502 (2006).
[123] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Phys. Rev. Lett. **114**, 070501 (2015).
[124] A. Leverrier, "Security of continuous-variable quantum key distribution via a gaussian de finetti reduction," Phys. Rev. Lett. **118**, 200501 (2017).
[125] Z. Li, Y.-C. Zhang, and H. Guo, "User-defined quantum key distribution," (2018), arXiv:1805.04249 [quant-ph].
[126] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, "Asymptotic security of continuous-variable quantum key distribution with a discrete modulation," Phys. Rev. X **9**, 021059 (2019).
[127] J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution," Phys. Rev. X **9**, 041064 (2019).
[128] A. Denys, P. Brown, and A. Leverrier, "Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation," Quantum **5**, 540 (2021).
[129] T. Matsuura, K. Maeda, T. Sasaki, and M. Koashi, "Finite-size security of continuous-variable quantum key distribution with digital signal processing," Nat. Commun. **12**, 252 (2021).
[130] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, *et al.*, "Quantum key distribution using gaussian-modulated coherent states," Nature **421**, 238–241 (2003).
[131] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, "Multidimensional reconciliation for a continuous-variable quantum key distribution," Phys. Rev. A **77**, 042325 (2008).
[132] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, *et al.*, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**, 042305 (2007).
[133] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**, 378–381 (2013).
[134] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, *et al.*, "Field test of classical symmetric encryption with continuous variables quantum key distribution," Opt. Express **20**, 14030–14041 (2012).
[135] D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, *et al.*, "Field demonstration of a continuous-variable quantum key distribution network," Opt. Lett. **41**, 3511–3514 (2016).
[136] D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Rep. **6**, 1–9 (2016).
[137] Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, *et al.*, "Continuous-variable qkd over 50 km commercial fiber," Quantum Sci. Technol. **4**, 035006 (2019).
[138] G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, *et al.*, "An integrated silicon photonic chip platform for continuous-variable quantum key distribution," Nat. Photonics **13**, 839–842 (2019).
[139] Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, *et al.*, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Phys. Rev. Lett. **125**, 010502 (2020).
[140] Y. Zhang, Z. Chen, B. Chu, C. Zhou, X. Wang, *et al.*, "Continuous-variable qkd network in qingdao," Bulletin of the American Physical Society **65** (2020).
[141] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," Phys. Rev. X **5**, 041009 (2015).
[142] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, *et al.*, "Self-referenced continuous-variable quantum key distribution protocol," Phys. Rev. X **5**, 041010 (2015).
[143] H. Wang, Y. Li, Y. Pi, Y. Pan, Y. Shao, *et al.*, "Sub-gbps key rate four-state continuous-variable quantum key distribution within metropolitan area," Commun. Phys. **5**, 162 (2022).
[144] A. Aguado, V. Lopez, D. Lopez, M. Peev, A. Poppe, *et al.*, "The engineering of software-defined quantum key distribution networks," IEEE Commun. Mag. **57**, 20–26 (2019).
[145] F. Roumestan, A. Ghazisaeidi, J. Renaudier, L. T. Vidarte, A. Leverrier, *et al.*, "Experimental demonstration of discrete modulation formats for continuous variable quantum key distribution," (2022), arXiv:2207.11702 [quant-ph].
[146] A. A. Hajomer, C. Bruynsteen, I. Derkach, N. Jain, A. Bomhals, *et al.*, "Continuous-variable quantum key distribution at 10 gbaud using an integrated photonic-electronic receiver," arXiv preprint arXiv:2305.19642 (2023).
[147] Y. Bian, Y.-C. Zhang, C. Zhou, S. Yu, Z. Li, *et al.*, "High-rate point-to-multipoint quantum key distribution using coherent states," (2023), arXiv:2302.02391 [quant-ph].
[148] R. Simon, N. Mukunda, and B. Dutta, "Quantum-noise matrix for multimode systems: U(n) invariance, squeezing, and normal forms," Phys. Rev. A **49**, 1567–1583 (1994).
[149] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?" Phys. Rev. **47**, 777–780 (1935).
[150] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," Quantum Inf. Comput. **3**, 535–552 (2003).
[151] R. Renner and J. I. Cirac, "de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," Phys. Rev. Lett. **102**, 110504 (2009).
[152] S. Pirandola, "Composable security for continuous variable quantum key distribution: Trust levels and practical key rates in wired and wireless networks," Phys. Rev. Research **3**, 043014 (2021).
[153] S. Pirandola, "Limits and security of free-space quantum communications," Phys. Rev. Research **3**, 013279 (2021).
[154] S. Pirandola and P. Papanastasiou, "Improved composable key rates for cv-qkd," arXiv preprint arXiv:2301.10270 (2023).
[155] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, "Security of continuous-variable quantum key distribution against general attacks," Phys. Rev. Lett. **110**, 030502 (2013).
[156] F. Furrer, "Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle," Phys. Rev. A **90**, 042325 (2014).
[157] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, *et al.*, "Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks," Phys. Rev. Lett. **109**, 100502 (2012).
[158] A. Leverrier and P. Grangier, "Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation," Phys. Rev. Lett. **102**, 180504 (2009).
[159] V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution," Phys. Rev. A **92**, 062337 (2015).
[160] Q. Liao, Y. Guo, C. Xie, D. Huang, P. Huang, *et al.*, "Composable security of unidimensional continuous-variable quantum key distribution," Quantum Inf. Process. **17**, 113 (2018).
[161] R. García-Patrón and N. J. Cerf, "Continuous-variable quantum key distribution protocols over noisy channels," Phys. Rev. Lett. **102**, 130501 (2009).
[162] A. Vidiella-Barranco and L. Borelli, "Continuous variable quantum key distribution using polarized coherent states," Int. J. Mod. Phys. B **20**, 1287–1296 (2006).
[163] R. Filip, "Continuous-variable quantum key distribution with noisy coherent states," Phys. Rev. A **77**, 022310 (2008).
[164] P. Papanastasiou, C. Ottaviani, and S. Pirandola, "Gaussian one-way thermal quantum cryptography with finite-size effects," Phys. Rev. A **98**, 032314 (2018).
[165] J. Fiurášek and N. J. Cerf, "Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution," Phys. Rev. A **86**, 060302 (2012).
[166] N. Walk, T. C. Ralph, T. Symul, and P. K. Lam, "Security of continuous-variable quantum cryptography with gaussian postselection," Phys. Rev. A **87**, 020303 (2013).
[167] N. Hosseinidehaj, A. M. Lance, T. Symul, N. Walk, and T. C. Ralph, "Finite-size effects in continuous-variable quantum key distribution with gaussian postselection," Phys. Rev. A **101**, 052335 (2020).
[168] Z. Li, Y. Zhang, X. Wang, B. Xu, X. Peng, *et al.*, "Non-gaussian postselection and virtual photon subtraction in continuous-variable quantum key

distribution," Phys. Rev. A **93**, 012310 (2016).
[169]L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," Nat. Commun. **3**, 1–6 (2012).
[170]S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Continuous-variable quantum cryptography using two-way quantum communication," Nat. Phys. **4**, 726–730 (2008).
[171]S. Ghorai, E. Diamanti, and A. Leverrier, "Composable security of two-way continuous-variable quantum key distribution without active symmetrization," Phys. Rev. A **99**, 012311 (2019).
[172]M. Sun, X. Peng, Y. Shen, and H. Guo, "Security of a new two-way continuous-variable quantum key distribution protocol," Int. J. Quantum Inf. **10**, 1250059 (2012).
[173]Y. Zhao, Y. Zhang, Z. Li, S. Yu, and H. Guo, "Improvement of two-way continuous-variable quantum key distribution with virtual photon subtraction," Quantum Inf. Process. **16**, 184 (2017).
[174]C. Li, R. Miao, X. Gong, Y. Guo, and G. He, "Performance improvement of two-way quantum key distribution by using a heralded noiseless amplifier," Int. J. Theor. Phys. **55**, 2199–2211 (2016).
[175]Y. Bian, L. Huang, and Y. Zhang, "Unidimensional two-way continuous-variable quantum key distribution using coherent states," Entropy **23**, 294 (2021).
[176]Z. Li, Y.-C. Zhang, F. Xu, X. Peng, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution," Phys. Rev. A **89**, 052301 (2014).
[177]S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, *et al.*, "High-rate measurement-device-independent quantum cryptography," Nat. Photonics **9**, 397–402 (2015).
[178]X. Zhang, Y. Zhang, Y. Zhao, X. Wang, S. Yu, *et al.*, "Finite-size analysis of continuous-variable measurement-device-independent quantum key distribution," Phys. Rev. A **96**, 042334 (2017).
[179]C. Lupo, C. Ottaviani, P. Papanastasiou, and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution: Composable security against coherent attacks," Phys. Rev. A **97**, 052327 (2018).
[180]Y.-C. Zhang, Z. Li, S. Yu, W. Gu, X. Peng, *et al.*, "Continuous-variable measurement-device-independent quantum key distribution using squeezed states," Phys. Rev. A **90**, 052325 (2014).
[181]Z. Chen, Y. Zhang, G. Wang, Z. Li, and H. Guo, "Composable security analysis of continuous-variable measurement-device-independent quantum key distribution with squeezed states for coherent attacks," Phys. Rev. A **98**, 012314 (2018).
[182]L. Huang, Y. Zhang, Z. Chen, and S. Yu, "Unidimensional continuous-variable quantum key distribution with untrusted detection under realistic conditions," Entropy **21**, 1100 (2019).
[183]D. Bai, P. Huang, Y. Zhu, H. Ma, T. Xiao, *et al.*, "Unidimensional continuous-variable measurement-device-independent quantum key distribution," Quantum Inf. Process. **19**, 53 (2020).
[184]H.-X. Ma, P. Huang, D.-Y. Bai, T. Wang, S.-Y. Wang, *et al.*, "Long-distance continuous-variable measurement-device-independent quantum key distribution with discrete modulation," Phys. Rev. A **99**, 022322 (2019).
[185]Y. Zhao, Y. Zhang, B. Xu, S. Yu, and H. Guo, "Continuous-variable measurement-device-independent quantum key distribution with virtual photon subtraction," Phys. Rev. A **97**, 042328 (2018).
[186]A. Leverrier and P. Grangier, "Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation," Phys. Rev. A **83**, 042312 (2011).
[187]S. Pirandola, "Satellite quantum communications: Fundamental bounds and practical security," Phys. Rev. Research **3**, 023130 (2021).
[188]R. Goncharov, I. Vorontsova, D. Kirichenko, I. Filipov, I. Adam, *et al.*, "The rationale for the optimal continuous-variable quantum key distribution protocol," Optics **3**, 338–351 (2022).
[189]Y. Bian, L. Huang, Y. Zhang, and S. Yu, "Unidimensional two-way continuous-variable quantum key distribution," OSA Frontiers in Optics + Laser Science APS/DLS **FM7A.5** (2020).
[190]C. Weedbrook, "Continuous-variable quantum key distribution with entanglement in the middle," Phys. Rev. A **87**, 022308 (2013).
[191]P. Wang, X. Wang, and Y. Li, "Continuous-variable measurement-device-independent quantum key distribution with source-intensity errors," Phys. Rev. A **102**, 022609 (2020).
[192]Y. Zhang, Z. Chen, C. Weedbrook, S. Yu, and H. Guo, "Continuous-variable source-device-independent quantum key distribution against general attacks," Sci. Rep. **10**, 1–10 (2020).
[193]B. Qi, P. G. Evans, and W. P. Grice, "Passive state preparation in the gaussian-modulated coherent-states quantum key distribution," Phys. Rev. A **97**, 012317 (2018).
[194]S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," Phys. Rev. Lett. **102**, 050503 (2009).
[195]I. Devetak and A. J. Winter, "Distillation of secret key and entanglement from quantum states," Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207 – 235 (2003).
[196]S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. Cope, *et al.*, "Theory of channel simulation and bounds for private communication," Quantum Sci. Technol. **3**, 035009 (2018).
[197]A. S. Holevo, "Bounds for the quantity of information transmitted by a quantum communication channel," Problemy Peredachi Informatsii **9**, 3–11 (1973).
[198]M. M. Wolf, G. Giedke, and J. I. Cirac, "Extremality of gaussian quantum states," Phys. Rev. Lett. **96**, 080502 (2006).
[199]M. Almeida, D. Pereira, N. J. Muga, M. Facão, A. N. Pinto, *et al.*, "Secret key rate of multi-ring m-apsk continuous variable quantum key distribution," Opt. Express **29**, 38669–38682 (2021).
[200]C. Lupo and Y. Ouyang, "Quantum key distribution with nonideal heterodyne detection: composable security of discrete-modulation continuous-variable protocols," PRX Quantum **3**, 010341 (2022).
[201]J. Lin and N. Lütkenhaus, "Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution," Phys. Rev. Appl. **14**, 064030 (2020).
[202]W.-B. Liu, C.-L. Li, Y.-M. Xie, C.-X. Weng, J. Gu, *et al.*, "Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance," PRX Quantum **2**, 040334 (2021).
[203]T. Upadhyaya, T. van Himbeeck, J. Lin, and N. Lütkenhaus, "Dimension reduction in quantum key distribution for continuous-and discrete-variable protocols," PRX Quantum **2**, 020325 (2021).
[204]F. Kanitschar and C. Pacher, "Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection," Phys. Rev. Appl. **18**, 034073 (2022).
[205]P. Wang, Y. Zhang, Z. Lu, X. Wang, and Y. Li, "Discrete-modulation continuous-variable quantum key distribution with a high key rate," New J. Phys. **25**, 023019 (2023).
[206]F. Kanitschar, I. George, J. Lin, T. Upadhyaya, and N. Lütkenhaus, "Finite-size security for discrete-modulated continuous-variable quantum key distribution protocols," arXiv preprint arXiv:2301.08686 (2023).
[207]S. Yamano, T. Matsuura, Y. Kuramochi, T. Sasaki, and M. Koashi, "Finite-size security proof of binary-modulation continuous-variable quantum key distribution using only heterodyne measurement," arXiv preprint arXiv:2208.11983 (2022).
[208]S. Bäuml, C. P. García, V. Wright, O. Fawzi, and A. Acín, "Security of discrete-modulated continuous-variable quantum key distribution," arXiv preprint arXiv:2303.09255 (2023).
[209]P. Papanastasiou and S. Pirandola, "Continuous-variable quantum cryptography with discrete alphabets: Composable security under collective gaussian attacks," Phys. Rev. Research **3**, 013047 (2021).
[210]S. Pirandola, "Quantum discord as a resource for quantum cryptography," Sci. Rep. **4**, 6956 (2014).
[211]V. C. Usenko and R. Filip, "Trusted noise in continuous-variable quantum key distribution: a threat and a defense," Entropy **18**, 20 (2016).
[212]S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, "Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers," J. Phys. B: At., Mol. Opt. Phys. **42**, 114014 (2009).
[213]Y. Zhang, Z. Li, C. Weedbrook, S. Yu, W. Gu, *et al.*, "Improvement of two-way continuous-variable quantum key distribution using optical amplifiers," J. Phys. B: At., Mol. Opt. Phys. **47** (2013).
[214]Y. Zhang, Z. Li, C. Weedbrook, K. Marshall, S. Pirandola, *et al.*, "Noiseless linear amplifiers in entanglement-based continuous-variable quantum key distribution," Entropy **17**, 4547–4562 (2015).

[215] Y. Zhang, S. Yu, and H. Guo, "Application of practical noiseless linear amplifier in no-switching continuous-variable quantum cryptography," Quantum Information Process. **14**, 4339–4349 (2015).

[216] H. Wu, X. Liu, H. Zhang, X. Ruan, and Y. Guo, "Performance analysis of continuous variable quantum teleportation with noiseless linear amplifier in seawater channel," Symmetry **14**, 997 (2022).

[217] M. N. Bera, A. Acín, M. Kuś, M. W. Mitchell, and M. Lewenstein, "Randomness in quantum mechanics: philosophy, physics and technology," Rep. Prog. Phys. **80**, 124001 (2017).

[218] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," npj Quantum Inf. **2**, 1–9 (2016).

[219] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," Rev. Mod. Phys. **89**, 015004 (2017).

[220] T. Symul, S. M. Assad, and P. K. Lam, "Real time demonstration of high bitrate quantum random number generation with coherent laser light," Appl. Phys. Lett. **98** (2011).

[221] Z. Zheng, Y. Zhang, W. Huang, S. Yu, and H. Guo, "6 gbps real-time optical quantum random number generator based on vacuum fluctuation," Rev. Sci. Instrum. **90** (2019).

[222] B. Bai, J. Huang, G.-R. Qiao, Y.-Q. Nie, W. Tang, *et al.*, "18.8 gbps real-time quantum random number generator with a photonic integrated chip," Appl. Phys. Lett. **118** (2021).

[223] T. Gehring, C. Lupo, A. Kordts, D. Solar Nikolic, N. Jain, *et al.*, "Homodyne-based quantum random number generator at 2.9 gbps secure against quantum side-information," Nat. Commun. **12**, 605 (2021).

[224] C. Bruynsteen, T. Gehring, C. Lupo, J. Bauwelinck, and X. Yin, "100-gbit/s integrated quantum random number generator based on vacuum fluctuations," PRX Quantum **4**, 010330 (2023).

[225] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," Opt. Lett. **35**, 312–314 (2010).

[226] J. Yang, J. Liu, Q. Su, Z. Li, F. Fan, *et al.*, "5.4 gbps real time quantum random number generator with simple implementation," Opt. Express **24**, 27475–27481 (2016).

[227] Z. Yuan, M. Lucamarini, J. Dynes, B. Fröhlich, A. Plews, *et al.*, "Robust random number generation using steady-state emission of gain-switched laser diodes," Appl. Phys. Lett. **104** (2014).

[228] Y.-Q. Nie, L. Huang, Y. Liu, F. Payne, J. Zhang, *et al.*, "The generation of 68 gbps quantum random number by measuring laser phase fluctuations," Rev. Sci. Instrum. **86** (2015).

[229] T. Roger, T. Paraiso, I. De Marco, D. G. Marangon, Z. Yuan, *et al.*, "Real-time interferometric quantum random number generation on chip," J. Opt. Soc. Am. B **36**, B137–B142 (2019).

[230] M. Imran, V. Sorianello, F. Fresi, B. Jalil, M. Romagnoli, *et al.*, "On-chip tunable soi interferometer for quantum random number generation based on phase diffusion in lasers," Opt. Commun. **485**, 126736 (2021).

[231] J. Yang, M. Wu, Y. Zhang, J. Liu, F. Fan, *et al.*, "An ultra-fast quantum random number generation scheme based on laser phase noise," arXiv preprint arXiv:2311.17380 (2023).

[232] C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," Opt. Express **18**, 23584–23597 (2010).

[233] X. Li, A. B. Cohen, T. E. Murphy, and R. Roy, "Scalable parallel physical random number generator based on a superluminescent led," Opt. Lett. **36**, 1020–1022 (2011).

[234] J. Yang, F. Fan, J. Liu, Q. Su, Y. Li, *et al.*, "Randomness quantification for quantum random number generation based on detection of amplified spontaneous emission noise," Quantum Sci. Technol. **6**, 015002 (2020).

[235] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," Rev. Sci. Instrum. **71**, 1675–1680 (2000).

[236] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," J. Mod. Opt. **47**, 595–598 (2000).

[237] J. F. Dynes, Z. L. Yuan, A. W. Sharpe, and A. J. Shields, "A high speed, postprocessing free, quantum random number generator," Appl. Phys. Lett. **93** (2008).

[238] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, "Photon arrival time quantum random number generation," J. Mod. Opt. **56**, 516–522 (2009).

[239] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, *et al.*, "A generator for unique quantum random numbers based on vacuum states," Nat. Photonics **4**, 711–715 (2010).

[240] Y.-Q. Nie, J.-Y. Guan, H. Zhou, Q. Zhang, X. Ma, *et al.*, "Experimental measurement-device-independent quantum random-number generation," Phys. Rev. A **94**, 060301 (2016).

[241] Z. Cao, H. Zhou, and X. Ma, "Loss-tolerant measurement-device-independent quantum random number generation," New J. Phys. **17**, 125011 (2015).

[242] M. Avesani, D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent heterodyne-based quantum random number generator at 17 gbps," Nat. Commun. **9**, 5365 (2018).

[243] D. G. Marangon, G. Vallone, and P. Villoresi, "Source-device-independent ultrafast quantum random number generation," Phys. Rev. Lett. **118**, 060503 (2017).

[244] Z. Cao, H. Zhou, X. Yuan, and X. Ma, "Source-independent quantum random number generation," Phys. Rev. X **6**, 011020 (2016).

[245] J. B. Brask, A. Martin, W. Esposito, R. Houlmann, J. Bowles, *et al.*, "Megahertz-rate semi-device-independent quantum random number generators based on unambiguous state discrimination," Phys. Rev. Appl. **7**, 054018 (2017).

[246] T. Van Himbeeck, E. Woodhead, N. J. Cerf, R. García-Patrón, and S. Pironio, "Semi-device-independent framework based on natural physical assumptions," Quantum **1**, 33 (2017).

[247] B. Xu, Z. Chen, Z. Li, J. Yang, Q. Su, *et al.*, "High speed continuous variable source-independent quantum random number generation," Quantum Sci. Technol. **4**, 025013 (2019).

[248] H. Tebyanian, M. Avesani, G. Vallone, and P. Villoresi, "Semi-device-independent randomness from d-outcome continuous-variable detection," Phys. Rev. A **104**, 062424 (2021).

[249] M. Avesani, H. Tebyanian, P. Villoresi, and G. Vallone, "Semi-device-independent heterodyne-based quantum random-number generator," Phys. Rev. Appl. **15**, 034034 (2021).

[250] Y. Liu, Q. Zhao, M.-H. Li, J.-Y. Guan, Y. Zhang, *et al.*, "Device-independent quantum random-number generation," Nature **562**, 548–551 (2018).

[251] W.-Z. Liu, M.-H. Li, S. Ragy, S.-R. Zhao, B. Bai, *et al.*, "Device-independent randomness expansion against quantum side information," Nat. Phys. **17**, 448–451 (2021).

[252] M.-H. Li, X. Zhang, W.-Z. Liu, S.-R. Zhao, B. Bai, *et al.*, "Experimental realization of device-independent quantum randomness expansion," Phys. Rev. Lett. **126**, 050503 (2021).

[253] Y. Zhang, L. K. Shalm, J. C. Bienfang, M. J. Stevens, M. D. Mazurek, *et al.*, "Experimental low-latency device-independent quantum randomness," Phys. Rev. Lett. **124**, 010505 (2020).

[254] W. Wei, G. Xie, A. Dang, and H. Guo, "High-speed and bias-free optical random number generator," IEEE Photon. Technol. Lett. **24**, 437–439 (2011).

[255] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," J. Light. Technol. **30**, 1329–1334 (2012).

[256] L. Li, A. Wang, P. Li, H. Xu, L. Wang, *et al.*, "Random bit generator using delayed self-difference of filtered amplified spontaneous emission," IEEE Photon. J. **6**, 1–9 (2014).

[257] H. Zhou, X. Yuan, and X. Ma, "Randomness generation based on spontaneous emissions of lasers," Phys. Rev. A **91**, 062316 (2015).

[258] H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," Phys. Rev. E **81**, 051137 (2010).

[259] F. Xu, B. Qi, X. Ma, H. Xu, H. Zheng, *et al.*, "Ultrafast quantum random number generation based on quantum phase fluctuations," Opt. Express **20**, 12366–12377 (2012).

[260] C. Abellán, W. Amaya, M. Jofre, M. Curty, A. Acín, *et al.*, "Ultra-fast quantum randomness generation by accelerated phase diffusion in a pulsed laser diode," Opt. Express **22**, 1645–1654 (2014).

[261] X.-G. Zhang, Y.-Q. Nie, H. Zhou, H. Liang, X. Ma, *et al.*, "Fully integrated 3.2 gbps quantum random number generator with real-time extraction," Rev. Sci. Instrum. **87** (2016).

[262] C. Abellan, W. Amaya, D. Domenech, P. Muñoz, J. Capmany, *et al.*, "Quantum entropy source on an inp photonic integrated circuit for random number generation," Optica **3**, 989–994 (2016).

[263]J. Liu, J. Yang, Z. Li, Q. Su, W. Huang, *et al.*, "117 gbits/s quantum random number generation with simple structure," IEEE Photon. Technol. Lett. **29**, 283–286 (2016).
[264]S.-H. Sun and F. Xu, "Experimental study of a quantum random-number generator based on two independent lasers," Phys. Rev. A **96**, 062314 (2017).
[265]J.-R. Álvarez, S. Sarmiento, J. Lázaro, J. Gené, and J. Torres, "Random number generation by coherent detection of quantum phase noise," Opt. Express **28**, 5538–5547 (2020).
[266]F. Raffaelli, P. Sibson, J. E. Kennard, D. H. Mahler, M. G. Thompson, *et al.*, "Generation of random numbers by measuring phase fluctuations from a laser diode with a silicon-on-insulator chip," Opt. Express **26**, 19730–19741 (2018).
[267]T. Chrysostomidis, I. Roumpos, D. A. Outerelo, M. Troncoso-Costas, V. Moskalenko, *et al.*, "Long term experimental verification of a single chip quantum random number generator fabricated on the inp platform," EPJ Quantum Technol. **10**, 5 (2023).
[268]M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, *et al.*, "True random numbers from amplified quantum vacuum," Opt. Express **19**, 20665–20672 (2011).
[269]J.-Y. Haw, S. Assad, A. Lance, N. Ng, V. Sharma, *et al.*, "Maximization of extractable randomness in a quantum random-number generator," Phys. Rev. Appl. **3**, 054004 (2015).
[270]F. Raffaelli, G. Ferranti, D. H. Mahler, P. Sibson, J. E. Kennard, *et al.*, "A homodyne detector integrated onto a photonic chip for measuring quantum states and generating random numbers," Quantum Sci. Technol. **3**, 025003 (2018).
[271]C. Bruynsteen, M. Vanhoecke, J. Bauwelinck, and X. Yin, "Integrated balanced homodyne photonic–electronic detector for beyond 20 ghz shot-noise-limited measurements," Optica **8**, 1146–1152 (2021).
[272]M. E. Muller, "An inverse method for the generation of random normal deviates on large-scale computers," Math. Comput. **12**, 167–174 (1958).
[273]G. E. Box and M. E. Muller, "A note on the generation of random normal deviates," The annals of mathematical statistics **29**, 610–611 (1958).
[274]D. Teichroew, *Distribution sampling with high speed computers*, Ph.D. thesis, North Carolina State College (1953).
[275]P. Kabal, "Generating gaussian pseudo-random deviates," Department of Electrical and Computer Engineering, McGill University, Tech. Rep (2000).
[276]D. Knuth, "The art of computer programming, 2 (seminumerical algorithms)," (No Title) (1981).
[277]R. Kumar, H. Qin, and R. Alléaume, "Coexistence of continuous variable qkd with intense dwdm classical channels," New J. Phys. **17**, 043027 (2015).
[278]T. A. Eriksson, T. Hirano, B. J. Puttnam, G. Rademacher, R. S. Luís, *et al.*, "Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels," Commun. Phys. **2**, 1–8 (2019).
[279]D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng, "High-speed continuous-variable quantum key distribution without sending a local oscillator," Opt. Lett. **40**, 3695–3698 (2015).
[280]J. Aldama, S. Sarmiento, S. Etcheverry, R. Valivarthi, I. L. Grande, *et al.*, "Small-form-factor gaussian-modulated coherent-state transmitter for cv-qkd using a gain-switched dfb laser," Opt. Express **31**, 5414–5425 (2023).
[281]X. Wang, J. Liu, X. Li, and Y. Li, "Generation of stable and high extinction ratio light pulses for continuous variable quantum key distribution," IEEE J. Quantum Electron. **51**, 1–6 (2015).
[282]H. H. Brunner, L. C. Comandar, F. Karinou, S. Bettelli, D. Hillerkuss, *et al.*, "A low-complexity heterodyne cv-qkd architecture," in *2017 19th International Conference on Transparent Optical Networks (ICTON)* (IEEE, 2017) pp. 1–4.
[283]S. Kleis, M. Rueckmann, and C. G. Schaeffer, "Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals," Opt. Lett. **42**, 1588–1591 (2017).
[284]H. Wang, Y. Pi, W. Huang, Y. Li, Y. Shao, *et al.*, "High-speed gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation," Opt. Express **28**, 32882–32893 (2020).
[285]Y. Pan, H. Wang, Y. Shao, Y. Pi, Y. Li, *et al.*, "Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system," Opt. Lett. **47**, 3307–3310 (2022).
[286]N. Jain, H.-M. Chin, H. Mani, C. Lupo, D. S. Nikolic, *et al.*, "Practical continuous-variable quantum key distribution with composable security," Nat. Commun. **13**, 4740 (2022).
[287]P. Huang, J. Huang, Z. Zhang, and G. Zeng, "Quantum key distribution using basis encoding of gaussian-modulated coherent states," Phys. Rev. A **97**, 042311 (2018).
[288]P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, "Analysis of imperfections in practical continuous-variable quantum key distribution," Phys. Rev. A **86**, 032309 (2012).
[289]W. Liu, X. Wang, N. Wang, S. Du, and Y. Li, "Imperfect state preparation in continuous-variable quantum key distribution," Phys. Rev. A **96**, 042312 (2017).
[290]B. Qi, H. Gunther, P. G. Evans, B. P. Williams, R. M. Camacho, *et al.*, "Experimental passive-state preparation for continuous-variable quantum communications," Phys. Rev. Appl. **13**, 054065 (2020).
[291]P. Huang, T. Wang, R. Chen, P. Wang, Y. Zhou, *et al.*, "Experimental continuous-variable quantum key distribution using a thermal source," New J. Phys. **23**, 113028 (2021).
[292]B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, "Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers," Phys. Rev. A **76**, 052323 (2007).
[293]Y.-M. Li, X.-Y. Wang, Z.-L. Bai, W.-Y. Liu, S.-S. Yang, *et al.*, "Continuous variable quantum key distribution," Chinese Physics B **26**, 040303 (2017).
[294]T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, *et al.*, "High key rate continuous-variable quantum key distribution with a real local oscillator," Opt. Express **26**, 2794–2806 (2018).
[295]F. Laudenbach, C. Pacher, C.-H. F. Fung, A. Poppe, M. Peev, *et al.*, "Continuous-variable quantum key distribution with gaussian modulation: The theory of practical implementations," Adv. Quantum Technol. **1**, 1800011 (2018).
[296]B. Chu, Y. Zhang, Y. Huang, S. Yu, Z. Chen, *et al.*, "Practical source monitoring for continuous-variable quantum key distribution," Quantum Sci. Technol. **6**, 025012 (2021).
[297]C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," Phys. Rev. Lett. **105**, 110501 (2010).
[298]C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," Phys. Rev. A **86**, 022318 (2012).
[299]B. Stiller, I. Khan, N. Jain, P. Jouguet, S. Kunz-Jacques, *et al.*, "Quantum hacking of continuous-variable quantum key distribution systems: realtime trojan-horse attacks," in *Conf. on Lasers and Electro-Optics (San Jose)* (2015) p. FF1A.7.
[300]W. Liu, J. Peng, P. Huang, D. Huang, and G. Zeng, "Monitoring of continuous-variable quantum key distribution system in real environment," Opt. Express **25**, 19429–19443 (2017).
[301]T. Wang, P. Huang, S. Wang, and G. Zeng, "Polarization-state tracking based on kalman filter in continuous-variable quantum key distribution," Opt. Express **27**, 26689–26700 (2019).
[302]W. Liu, Y. Cao, X. Wang, and Y. Li, "Continuous-variable quantum key distribution under strong channel polarization disturbance," Phys. Rev. A **102**, 032625 (2020).
[303]D. Li, P. Huang, T. Wang, S. Wang, R. Chen, *et al.*, "Phase compensation based on step-length control in continuous-variable quantum key distribution," Opt. Express **27**, 20670–20687 (2019).
[304]T. Wang, P. Huang, S. Wang, and G. Zeng, "Carrier-phase estimation for simultaneous quantum key distribution and classical communication using a real local oscillator," Phys. Rev. A **99**, 022318 (2019).
[305]Z. Xing, X. Li, X. Ruan, Y. Luo, and H. Zhang, "Phase compensation for continuous variable quantum key distribution based on convolutional neural network," in *Photonics*, Vol. 9 (MDPI, 2022) p. 463.
[306]H.-M. Chin, A. A. Hajomer, N. Jain, U. L. Andersen, and T. Gehring, "Machine learning based joint polarization and phase compensation for cv-qkd," in *Optical Fiber Communication Conference* (Optica Publishing Group, 2023) pp. Th3J–2.
[307]D. Lin, P. Huang, D. Huang, C. Wang, J. Peng, *et al.*, "High performance frame synchronization for continuous variable quantum key distribution systems," Opt. Express **23**, 22190–22198 (2015).
[308]C. Liu, Y. Zhao, Y. Zhang, Z. Zheng, and S. Yu, "Synchronization schemes for continuous-variable quantum key distribution," in *International Con-*

ference on Optoelectronics and Microelectronics Technology and Application, Vol. 10244 (SPIE, 2017) pp. 40–44.
[309]R. Chen, P. Huang, D. Li, Y. Zhu, and G. Zeng, "Robust frame synchronization scheme for continuous-variable quantum key distribution with simple process," Entropy **21**, 1146 (2019).
[310]J. Dong, T. Wang, L. Li, P. Huang, and G. Zeng, "Efficient frame synchronization using a weak coherent state for continuous-variable quantum key distribution," Phys. Rev. A **105**, 052407 (2022).
[311]H. Li, H. Song, X. Liu, J. Wen, S. Sun, *et al.*, "Reliable synchronization technology for continuous variable quantum key distribution system," in *2022 International Conference on 6G Communications and IoT Technologies (6GIoTT)* (IEEE, 2022) pp. 35–41.
[312]X.-F. Mo, B. Zhu, Z.-F. Han, Y.-Z. Gui, *et al.*, "Faraday–michelson system for quantum cryptography," Opt. Lett. **30**, 2632–2634 (2005).
[313]T. F. da Silva and J. P. von der Weid, "Optical transmission of frequency-coded quantum bits with wdm synchronization," J. Microwaves, Optoelectron. Electromagn. Appl. **8**, 163S–178S (2009).
[314]A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, *et al.*, "Single photon quantum cryptography," Phys. Rev. Lett. **89**, 187901 (2002).
[315]T. Wang, Z. Zuo, L. Li, P. Huang, Y. Guo, *et al.*, "Continuous-variable quantum key distribution without synchronized clocks," Phys. Rev. Appl. **18**, 014064 (2022).
[316]H. Yuen and J. Shapiro, "Optical communication with two-photon coherent states–part iii: Quantum measurements realizable with photoemissive detectors," IEEE Trans. Inf. Theory **26**, 78–92 (1980).
[317]D. Smithey, M. Beck, M. G. Raymer, and A. Faridani, "Measurement of the wigner distribution and the density matrix of a light mode using optical homodyne tomography: Application to squeezed states and the vacuum," Phys. Rev. Lett. **70**, 1244 (1993).
[318]Z. Ou and H. Kimble, "Probability distribution of photoelectric currents in photodetection processes and its connection to the measurement of a quantum state," Phys. Rev. A **52**, 3126 (1995).
[319]H. Hansen, T. Aichele, C. Hettich, P. Lodahl, A. Lvovsky, *et al.*, "Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements," Opt. Lett. **26**, 1714–1716 (2001).
[320]O. Haderka, V. Michálek, V. Urbášek, and M. Ježek, "Fast time-domain balanced homodyne detection of light," Appl. Opt. **48**, 2884–2889 (2009).
[321]Y.-M. Chi, B. Qi, W. Zhu, L. Qian, H.-K. Lo, *et al.*, "A balanced homodyne detector for high-rate gaussian-modulated coherent-state quantum key distribution," New J. Phys. **13**, 013003 (2011).
[322]R. Kumar, E. Barrios, A. MacRae, E. Cairns, E. Huntington, *et al.*, "Versatile wideband balanced detector for quantum optical homodyne tomography," Opt. Commun. **285**, 5259–5267 (2012).
[323]X. Wang, Z. liang Bai, P. Du, Y. Li, and K. Peng, "Ultrastable fiber-based time-domain balanced homodyne detector for quantum communication," Chin. Phys. Lett. **29**, 124202–124202 (2012).
[324]H. Duan, F. Jian, W. Chao, H. Peng, and Z. Gui-Hua, "A 300-mhz bandwidth balanced homodyne detector for continuous variable quantum key distribution," Chinese Phys. Lett. **30**, 114209 (2013).
[325]M. Cooper, C. Söller, and B. J. Smith, "High-stability time-domain balanced homodyne detector for ultrafast optical pulse applications," J. Mod. Opt. **60**, 611–616 (2013).
[326]X. Zhang, Y. Zhang, Z. Li, S. Yu, and H. Guo, "1.2-ghz balanced homodyne detector for continuous-variable quantum information technology," IEEE Photon. J. **10**, 1–10 (2018).
[327]J. Liu, Y. Cao, P. Wang, S. Liu, Z. Lu, *et al.*, "Impact of homodyne receiver bandwidth and signal modulation patterns on the continuous-variable quantum key distribution," Opt. Express **30**, 27912–27925 (2022).
[328]X. Jin, J. Su, Y. Zheng, C. Chen, W. Wang, *et al.*, "Balanced homodyne detection with high common mode rejection ratio based on parameter compensation of two arbitrary photodiodes," Opt. Express **23**, 23859–23866 (2015).
[329]S. Du, Z. Li, W. Liu, X. Wang, and Y. Li, "High-speed time-domain balanced homodyne detector for nanosecond optical field applications," J. Opt. Soc. Am. B **35**, 481–486 (2018).
[330]D. Milovančev, F. Honz, N. Vokić, F. Laudenbach, H. Hübel, *et al.*, "Ultra-low noise balanced receiver with> 20 db quantum-to-classical noise clearance at 1 ghz," in *2021 European Conference on Optical Communication (ECOC)* (IEEE, 2021) pp. 1–4.
[331]F. Honz, D. Milovančev, N. Vokić, C. Pacher, and B. Schrenk, "Broadband balanced homodyne detector for high-rate (> 10 gb/s) vacuum-noise quantum random number generation," in *2021 European Conference on Optical Communication (ECOC)* (IEEE, 2021) pp. 1–4.
[332]C. Bruynsteen, M. Vanhoecke, J. Bauwelinck, and X. Yin, "Integrated balanced homodyne photonic–electronic detector for beyond 20 ghz shot-noise-limited measurements," Optica **8**, 1146–1152 (2021).
[333]J. F. Tasker, J. Frazer, G. Ferranti, E. J. Allen, L. F. Brunel, *et al.*, "Silicon photonics interfaced with integrated electronics for 9 ghz measurement of squeezed light," Nat. Photonics **15**, 11–15 (2021).
[334]Y. Jia, X. Wang, X. Hu, X. Hua, Y. Zhang, *et al.*, "Silicon photonics-integrated time-domain balanced homodyne detector in continuous-variable quantum key distribution," arXiv preprint arXiv:2305.03419 (2023).
[335]X. Wang, X. Guo, Y. Jia, Y. Zhang, Z. Lu, *et al.*, "Accurate shot-noise-limited calibration of a time-domain balanced homodyne detector for continuous-variable quantum key distribution," J. Light. Technol. (2023).
[336]J. Liu, X. Wang, Z. Bai, and Y. Li, "High precision auto-balance of the time-domain pulsed homodyne detector," Acta Phys. Sin. **65** (2016).
[337]X. Tang, R. Kumar, S. Ren, A. Wonfor, R. V. Penty, *et al.*, "Performance of continuous variable quantum key distribution system at different detector bandwidth," Opt. Commun. **471**, 126034 (2020).
[338]D. Pereira, M. Almeida, M. Facão, A. N. Pinto, and N. A. Silva, "Impact of receiver imbalances on the security of continuous variables quantum key distribution," EPJ Quantum Technol. **8**, 1–12 (2021).
[339]S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, *et al.*, "Field test of a continuous-variable quantum key distribution prototype," New J. Phys. **11**, 045023 (2009).
[340]Y. Zhang, Y. Huang, Z. Chen, Z. Li, S. Yu, *et al.*, "One-time shot-noise unit calibration method for continuous-variable quantum key distribution," Phys. Rev. Appl. **13**, 024058 (2020).
[341]H.-M. Chin, N. Jain, D. Zibar, U. L. Andersen, and T. Gehring, "Machine learning aided carrier recovery in continuous-variable quantum key distribution," npj Quantum Information **7**, 20 (2021).
[342]A. A. E. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, *et al.*, "Long-distance continuous-variable quantum key distribution over 100 km fiber with local local oscillator," (2023), arXiv:2305.08156 [quant-ph].
[343]Y. Huang, Y. Zhang, B. Xu, L. Huang, and S. Yu, "A modified practical homodyne detector model for continuous-variable quantum key distribution: detailed security analysis and improvement by the phase-sensitive amplifier," J. Phys. B: At., Mol. Opt. Phys. (2020).
[344]L. Huang, Y. Zhang, and S. Yu, "Continuous-variable measurement-device-independent quantum key distribution with one-time shot-noise unit calibration," Chinese Phys. Lett. **38** (2021).
[345]B. Chu, Y. Zhang, Y. Huang, S. Yu, Z. Chen, *et al.*, "Practical source monitoring for continuous-variable quantum key distribution," Quantum Sci. Technol. **6** (2021).
[346]E. Cubukcu, "Root raised cosine (rrc) filters and pulse shaping in communication systems," in *AIAA Conference*, JSC-CN-26387 (2012).
[347]A. Marie and R. Alléaume, "Self-coherent phase reference sharing for continuous-variable quantum key distribution," Phys. Rev. A **95**, 012316 (2017).
[348]R. Corvaja, "Phase-noise limitations in continuous-variable quantum key distribution with homodyne detection," Phys. Rev. A **95**, 022315 (2017).
[349]B. Qi and C. C. W. Lim, "Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator," Phys. Rev. Appl. **9**, 054008 (2018).
[350]M. Zou, Y. Mao, and T.-Y. Chen, "Phase estimation using homodyne detection for continuous variable quantum key distribution," J. Appl. Phys. **126**, 063105 (2019).
[351]G. Van Assche, J. Cardinal, and N. J. Cerf, "Reconciliation of a quantum-distributed gaussian key," IEEE Trans. Inf. Theory **50**, 394–400 (2004).
[352]A. G. Mountogiannakis, P. Papanastasiou, and S. Pirandola, "Data post-processing for the one-way heterodyne protocol under composable finite-size security," Phys. Rev. A **106**, 042606 (2022).
[353]S. Yang, Z. Yan, H. Yang, Q. Lu, Z. Lu, *et al.*, "Information reconciliation of continuous-variables quantum key distribution: principles, implementations and applications," EPJ Quantum Technol. **10**, 40 (2023).
[354]X. Ma, C.-H. F. Fung, J.-C. Boileau, and H. Chau, "Universally composable and customizable post-processing for practical quantum key distribution," Comput. Secur. **30**, 172–177 (2011).

[355]X. Wen, Q. Li, H. Mao, X. Wen, and N. Chen, "An improved slice reconciliation protocol for continuous-variable quantum key distribution," Entropy **23**, 1317 (2021).
[356]A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," Phys. Rev. A **81**, 062343 (2010).
[357]P. Jouguet, S. Kunz-Jacques, and A. Leverrier, "Long-distance continuous-variable quantum key distribution with a gaussian modulation," Phys. Rev. A **84**, 062317 (2011).
[358]P. Jouguet, D. Elkouss, and S. Kunz-Jacques, "High-bit-rate continuous-variable quantum key distribution," Phys. Rev. A **90**, 042329 (2014).
[359]Z. liang Bai, S. Yang, and Y. Li, "High-efficiency reconciliation for continuous variable quantum key distribution," Jpn. J. Appl. Phys. **56** (2017).
[360]X. Wang, Y. Zhang, S. Yu, and H. Guo, "High speed error correction for continuous-variable quantum key distribution with multi-edge type ldpc code," Sci. Rep. **8**, 10543 (2018).
[361]M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, "Quasi-cyclic multi-edge ldpc codes for long-distance quantum cryptography," npj Quantum Inf. **4**, 21 (2018).
[362]S. Zhao, Z. Shen, H. Xiao, and L. Wang, "Multidimensional reconciliation protocol for continuous-variable quantum key agreement with polar coding," Sci. China: Phys., Mech. Astron. **61**, 1–4 (2018).
[363]C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, *et al.*, "Continuous-variable quantum key distribution with rateless reconciliation protocol," Phys. Rev. Appl. **12**, 054013 (2019).
[364]Y. Li, X. Zhang, Y. Li, B. Xu, L. Ma, *et al.*, "High-throughput gpu layered decoder of quasi-cyclic multi-edge type low density parity check codes in continuous-variable quantum key distribution systems," Sci. Rep. **10**, 14561 (2020).
[365]S. Yang, Z. Lu, and Y. Li, "High-speed post-processing in continuous-variable quantum key distribution based on fpga implementation," J. Light. Technol. **38**, 3935–3941 (2020).
[366]H. Mani, T. Gehring, P. Grabenweger, B. Ömer, C. Pacher, *et al.*, "Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution," Phys. Rev. A **103**, 062419 (2021).
[367]S. Jeong, H. Jung, and J. Ha, "Rate-compatible multi-edge type low-density parity-check code ensembles for continuous-variable quantum key distribution systems," npj Quantum Inf. **8**, 6 (2022).
[368]Q. Li, X. Wen, H. Mao, and X. Wen, "An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution," Quantum Inf. Process. **18**, 1–20 (2019).
[369]C. Zhou, X. Wang, Y. Zhang, Z. Zhang, *et al.*, "Continuous-variable quantum key distribution with rateless reconciliation protocol," Phys. Rev. Appl. (2019).
[370]X.-Q. Jiang, S. Yang, P. Huang, and G. Zeng, "High-speed reconciliation for cvqkd based on spatially coupled ldpc codes," IEEE Photon. J. **10**, 1–10 (2018).
[371]K. Zhang, X.-Q. Jiang, Y. Feng, R. Qiu, and E. Bai, "High efficiency continuous-variable quantum key distribution based on atsc 3.0 ldpc codes," Entropy **22**, 1087 (2020).
[372]D. Guo, C. He, T. Guo, Z. Xue, Q. Feng, *et al.*, "Comprehensive high-speed reconciliation for continuous-variable quantum key distribution," Quantum Inf. Process. **19**, 320 (2020).
[373]S.-S. Yang, J.-Q. Liu, Z.-G. Lu, Z.-L. Bai, X.-Y. Wang, *et al.*, "An fpga-based ldpc decoder with ultra-long codes for continuous-variable quantum key distribution," IEEE Access **9**, 47687–47697 (2021).
[374]J. Xie, L. Zhang, Y. Wang, and D. Huang, "Deep neural network based reconciliation for cv-qkd," in *Photonics*, Vol. 9 (MDPI, 2022) p. 110.
[375]X. Sun and H. Liang, "Implementation of encoder and decoder for low-density parity-check codes in continuous-variable quantum key distribution on a field programmable gate array," Opt. Eng. **62**, 014105–014105 (2023).
[376]X.-Q. Jiang, P. Huang, D. Huang, D. Lin, and G. Zeng, "Secret information reconciliation based on punctured low-density parity-check codes for continuous-variable quantum key distribution," Phys. Rev. A **95**, 022318 (2017).
[377]C. Zhou, X. Wang, Z. Zhang, S. Yu, Z. Chen, *et al.*, "Rate compatible reconciliation for continuous-variable quantum key distribution using raptor-like ldpc codes," Sci. China: Phys., Mech. Astron. **64**, 260311 (2021).
[378]Z. Cao, X. Chen, G. Chai, K. Liang, and Y. Yuan, "Rate-adaptive polar-coding-based reconciliation for continuous-variable quantum key distribution at low signal-to-noise ratio," Phys. Rev. Appl. **19**, 044023 (2023).
[379]C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer, "Generalized privacy amplification," Proceedings of 1994 IEEE International Symposium on Information Theory , 350– (1994).
[380]M. Tomamichel, R. Renner, C. Schaffner, and A. D. Smith, "Leftover hashing against quantum side information," 2010 IEEE International Symposium on Information Theory , 2703–2707 (2010).
[381]X. Wang, Y. Zhang, S. Yu, and H. Guo, "High-speed implementation of length-compatible privacy amplification in continuous-variable quantum key distribution," IEEE Photon. J. **10**, 1–9 (2018).
[382]B.-Z. Yan, Q. Li, H.-K. Mao, H.-W. Xu, and A. A. Abd El-Latif, "Large-scale and high-speed fpga-based privacy amplification for quantum key distribution," J. Light. Technol. **41**, 169–175 (2022).
[383]D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, *et al.*, "Continuous-variable quantum key distribution with 1 mbps secure key rate," Opt. Express **23**, 17511–17519 (2015).
[384]D. Huang, P. Huang, T. Wang, H. Li, Y. Zhou, *et al.*, "Continuous-variable quantum key distribution based on a plug-and-play dual-phase-modulated coherent-states protocol," Phys. Rev. A **94**, 032305 (2016).
[385]Y.-M. Li, X.-Y. Wang, Z.-L. Bai, W.-Y. Liu, S.-S. Yang, *et al.*, "Continuous variable quantum key distribution," Chin. Phys. B **26**, 040303 (2017).
[386]X. Wang, S. Guo, P. Wang, W. Liu, and Y. Li, "Realistic rate–distance limit of continuous-variable quantum key distribution," Opt. Express **27**, 13372–13386 (2019).
[387]X. Wang, S. Guo, P. Wang, W. Liu, and Y. Li, "Realistic rate–distance limit of continuous-variable quantum key distribution," Opt. Express **27**, 13372–13386 (2019).
[388]H. Li, C. Wang, P. Huang, D. Huang, T. Wang, *et al.*, "Practical continuous-variable quantum key distribution without finite sampling bandwidth effects," Opt. Express **24**, 20481–20493 (2016).
[389]C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, *et al.*, "25 mhz clock continuous-variable quantum key distribution system over 50 km fiber channel," Sci. Rep. **5**, 1–8 (2015).
[390]Y. Shen, Y. Chen, H. Zou, and J. Yuan, "A fiber-based quasi-continuous-wave quantum key distribution system," Sci. Rep. **4**, 1–5 (2014).
[391]D. Li, P. Huang, T. Wang, S. Wang, R. Chen, *et al.*, "Phase compensation based on step-length control in continuous-variable quantum key distribution," Opt. Express **27**, 20670–20687 (2019).
[392]M. Ziebell, M. Persechino, N. Harris, C. Galland, D. Marris-Morini, *et al.*, "Towards on-chip continuous-variable quantum key distribution," in *The European Conference on Lasers and Electro-Optics* (Optica Publishing Group, 2015) p. JSV_4_2.
[393]X. Wang, Z. Bai, S. Wang, Y.-M. Li, and K. Peng, "Four-state modulation continuous variable quantum key distribution over a 30-km fiber and analysis of excess noise," Chinese Phys. Lett. **30**, 010305 (2013).
[394]T. Hirano, T. Ichikawa, T. Matsubara, M. Ono, Y. Oguri, *et al.*, "Implementation of continuous-variable quantum key distribution with discrete modulation," Quantum Sci. Technol. **2**, 024010 (2017).
[395]X. Wang, W. Liu, P. Wang, and Y. Li, "Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution," Phys. Rev. A **95**, 062330 (2017).
[396]H. Zhao, H. Li, Y. Xu, P. Huang, T. Wang, *et al.*, "Simple continuous-variable quantum key distribution scheme using a sagnac-based gaussian modulator," Opt. Lett. **47**, 2939–2942 (2022).
[397]Y. Tian, Y. Zhang, S. Liu, P. Wang, Z. Lu, *et al.*, "High-performance long-distance discrete-modulation continuous-variable quantum key distribution," Opt. Lett. **48**, 2953–2956 (2023).
[398]Y. Pi, H. Wang, Y. Pan, Y. Shao, Y. Li, *et al.*, "Sub-mbps key-rate continuous-variable quantum key distribution with local local oscillator over 100-km fiber," Opt. Lett. **48**, 1766–1769 (2023).
[399]A. A. Hajomer, I. Derkach, N. Jain, H.-M. Chin, U. L. Andersen, *et al.*, "Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator," Science Advances **10**, eadi9474 (2024).
[400]H. H. Brunner, C.-H. F. Fung, M. Peev, R. B. Méndez, L. Ortíz, *et al.*, "Demonstration of a switched cv-qkd network," EPJ Quantum Technol. **10** (2023).
[401]B. P. Williams, B. Qi, M. Alshowkan, P. G. Evans, and N. A. Peters, "Continuous-variable quantum key distribution field-test with true local

oscillator," (2023), arXiv:2309.03959 [quant-ph].
[402]Y. Piétri, L. T. Vidarte, M. Schiavon, P. Grangier, A. Rhouni, *et al.*, "Cv-qkd receiver platform based on a silicon photonic integrated circuit," in *2023 Optical Fiber Communications Conference and Exhibition (OFC)* (IEEE, 2023) pp. 1–3.
[403]J. Aldama, S. Sarmiento, S. Etcheverry, I. L. Grande, L. T. Vidarte, *et al.*, "Inp-based cv-qkd pic transmitter," in *Optical Fiber Communication Conference* (Optica Publishing Group, 2023) pp. M1I–3.
[404]L. Li, T. Wang, X. Li, P. Huang, Y. Guo, *et al.*, "Continuous-variable quantum key distribution with on-chip light sources," Photonics Res. **11**, 504–516 (2023).
[405]X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Local oscillator fluctuation opens a loophole for eve in practical continuous-variable quantum-key-distribution systems," Phys. Rev. A **88**, 022339 (2013).
[406]X.-C. Ma, S.-H. Sun, M.-S. Jiang, and L.-M. Liang, "Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol," Phys. Rev. A **87**, 052309 (2013).
[407]J.-Z. Huang, C. Weedbrook, Z.-Q. Yin, S. Wang, H.-W. Li, *et al.*, "Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack," Phys. Rev. A **87**, 062329 (2013).
[408]P. Jouguet, S. Kunz-Jacques, and E. Diamanti, "Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution," Phys. Rev. A **87**, 062313 (2013).
[409]I. L. Grande, S. Etcheverry, J. Aldama, S. Ghasemi, D. Nolan, *et al.*, "Adaptable transmitter for discrete and continuous variable quantum key distribution," Opt. Express **29**, 14815–14827 (2021).
[410]S. Sarmiento, S. Etcheverry, J. Aldama, I. Lopez, L. Vidarte, *et al.*, "Continuous-variable quantum key distribution over a 15 km multi-core fiber," New J. Phys. **24**, 063011 (2022).
[411]J. Aldama, S. Sarmiento, I. H. L. Grande, S. Signorini, L. T. Vidarte, *et al.*, "Integrated qkd and qrng photonic technologies," J. Lightwave Technol. **40**, 7498–7517 (2022).
[412]T. Wang, P. Huang, Y. Zhou, W. Liu, and G. Zeng, "Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator," Phys. Rev. A **97**, 012310 (2018).
[413]F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C.-H. F. Fung, *et al.*, "Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator," Quantum **3**, 193 (2019).
[414]L. Ma, J. Yang, T. Zhang, Y. Shao, J. Liu, *et al.*, "Practical continuous-variable quantum key distribution with feasible optimization parameters," Sci. China Inf. Sci. **66**, 1–12 (2023).
[415]F. Karinou, H. H. Brunner, C.-H. F. Fung, L. C. Comandar, S. Bettelli, *et al.*, "Toward the integration of cv quantum key distribution in deployed optical networks," IEEE Photon. Technol. Lett. **30**, 650–653 (2018).
[416]K. Günthner, I. Khan, D. Elser, B. Stiller, Ö. Bayraktar, *et al.*, "Quantum-limited measurements of optical signals from a geostationary satellite," Optica **4**, 611–616 (2017).
[417]S. Wang, P. Huang, M. Liu, T. Wang, P. Wang, *et al.*, "Phase compensation for free-space continuous-variable quantum key distribution," Opt. Express **28**, 10737–10745 (2020).
[418]M. Zhang, P. Huang, P. Wang, S. Wei, and G. Zeng, "Experimental free-space continuous-variable quantum key distribution with thermal source," Opt. Lett. **48**, 1184–1187 (2023).
[419]B. Qi, W. Zhu, L. Qian, and H.-K. Lo, "Feasibility of quantum key distribution through a dense wavelength division multiplexing network," New J. Phys. **12**, 103042 (2010).
[420]Y. Li, N. Wang, X. Wang, and Z. Bai, "Influence of guided acoustic wave brillouin scattering on excess noise in fiber-based continuous variable quantum key distribution," JOSA B **31**, 2379–2383 (2014).
[421]T. A. Eriksson, R. S. Luís, B. J. Puttnam, G. Rademacher, M. Fujiwara, *et al.*, "Wavelength division multiplexing of 194 continuous variable quantum key distribution channels," J. Light. Technol. **38**, 2214–2218 (2020).
[422]S. Du, Y. Tian, and Y. Li, "Impact of four-wave-mixing noise from dense wavelength-division-multiplexing systems on entangled-state continuous-variable quantum key distribution," Phys. Rev. Appl. **14**, 024013 (2020).
[423]D. Milovančev, N. Vokić, F. Laudenbach, C. Pacher, H. Hübel, *et al.*, "High rate cv-qkd secured mobile wdm fronthaul for dense 5g radio networks," J. Light. Technol. **39**, 3445–3457 (2021).
[424]S. Kleis, J. Steinmayer, R. H. Derksen, and C. G. Schaeffer, "Experimental investigation of heterodyne quantum key distribution in the s-band or l-band embedded in a commercial c-band dwdm system," Opt. Express **27**, 16540–16549 (2019).
[425]B. Chu, Y. Zhang, Y. Zhao, Y. Xu, X. Chen, *et al.*, "Crosstalk-induced impact of coexisting dwdm network on continuous-variable qkd," in *2020 16th International Conference on the Design of Reliable Communication Networks DRCN 2020* (2020) pp. 1–5.
[426]S. Wang, P. Huang, T. Wang, and G. Zeng, "Atmospheric effects on continuous-variable quantum key distribution," New J. Phys. **20**, 083037 (2018).
[427]P. Papanastasiou, C. Weedbrook, and S. Pirandola, "Continuous-variable quantum key distribution in uniform fast-fading channels," Phys. Rev. A **97**, 032311 (2018).
[428]M. Ghalaii and S. Pirandola, "Continuous-variable measurement-device-independent quantum key distribution in free-space channels," Phys. Rev. A **108**, 042621 (2023).
[429]B. Heim, C. Peuntinger, N. Killoran, I. Khan, C. Wittmann, *et al.*, "Atmospheric continuous-variable quantum communication," New J. Phys. **16**, 113018 (2014).
[430]D. Dequal, L. Trigo Vidarte, V. Roman Rodriguez, G. Vallone, P. Villoresi, *et al.*, "Feasibility of satellite-to-ground continuous-variable quantum key distribution," npj Quantum Inf. **7**, 3 (2021).
[431]S. Wang, P. Huang, T. Wang, and G. Zeng, "Feasibility of all-day quantum communication with coherent detection," Phys. Rev. Appl. **12**, 024041 (2019).
[432]S. Wang, P. Huang, T. Wang, and G. Zeng, "Dynamic polarization control for free-space continuous-variable quantum key distribution," Opt. Lett. **45**, 5921–5924 (2020).
[433]P. Wang, P. Huang, R. Chen, and G. Zeng, "Robust frame synchronization for free-space continuous-variable quantum key distribution," Opt. Express **29**, 25048–25063 (2021).
[434]S. Wei, P. Huang, S. Wang, T. Wang, and G. Zeng, "High-precision data acquisition for free-space continuous-variable quantum key distribution," Opt. Express **31**, 7383–7397 (2023).
[435]S. Wang, P. Huang, T. Wang, and G. Zeng, "Feasibility of continuous-variable quantum key distribution through fog," Opt. Lett. **46**, 5858–5861 (2021).
[436]X. Su, W. Wang, Y. Wang, X. Jia, C. Xie, *et al.*, "Continuous variable quantum key distribution based on optical entangled states without signal modulation," Europhys. Lett. **87**, 20005 (2009).
[437]L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with modulated entangled states," Nat. Commun. **3**, 1083 (2012).
[438]T. Gehring, V. Händchen, J. Duhme, F. Furrer, T. Franz, *et al.*, "Implementation of continuous-variable quantum key distribution with composable and one-sided-device-independent security against coherent attacks," Nat. Commun. **6**, 1–7 (2015).
[439]N. Wang, S. Du, W. Liu, X. Wang, Y. Li, *et al.*, "Long-distance continuous-variable quantum key distribution with entangled states," Phys. Rev. Appl. **10**, 064028 (2018).
[440]S. Ren, Y. Wang, and X. Su, "Hybrid quantum key distribution network," Sci. China Inf. Sci. **65**, 200502 (2022).
[441]J. Feng, Z. Wan, Y. Li, and K. Zhang, "Distribution of continuous variable quantum entanglement at a telecommunication wavelength over 20 km of optical fiber," Opt. Lett. **42**, 3399–3402 (2017).
[442]S. Du, P. Wang, J. Liu, Y. Tian, and Y. Li, "Continuous variable quantum key distribution with a shared partially characterized entangled source," Photonics Res. **11**, 463–475 (2023).
[443]Z. Chen, X. Wang, S. Yu, Z. Li, and H. Guo, "Continuous-mode quantum key distribution with digital signal processing," npj Quantum Inf. **9**, 28 (2023).
[444]J. Wang, F. Sciarrino, A. Laing, and M. G. Thompson, "Integrated photonic quantum technologies," Nature Photonics **14**, 273–284 (2020).
[445]L. Li, P. Huang, T. Wang, and G. Zeng, "Practical security of a chip-based continuous-variable quantum-key-distribution system," Phys. Rev. A **103**, 032611 (2021).
[446]X. Wang, Y. Jia, X. Guo, J. Liu, S. Wang, *et al.*, "Silicon photonics integrated dynamic polarization controller," Chinese Opt. Lett. **20**, 041301 (2022).
[447]W. Luo, L. Cao, Y. Shi, L. Wan, H. Zhang, S. Li, G. Chen, Y. Li, S. Li,

Y. Wang, *et al.*, "Recent progress in quantum photonic chips for quantum communication and internet," Light: Science & Applications **12**, 175 (2023).
[448]B. Fröhlich, J. Dynes, M. Lucamarini, *et al.*, "A quantum access network," Nature **501**, 69–72 (2013).
[449]Y. Huang, Y. Zhang, T. Shen, G. Huang, and S. Yu, "Experimental demonstration of upstream continuous-variable qkd access network," in *CLEO: QELS_Fundamental Science* (Optica Publishing Group, 2020) pp. JTu2A–24.
[450]Y. Xu, T. Wang, H. Zhao, P. Huang, and G. Zeng, "Round-trip multi-band quantum access network," Photon. Res. **11**, 1449–1464 (2023).
[451]Y. Bian, Y. Pan, L. Ma, H. Wang, J. Dou, *et al.*, "First demonstration of an 8-node mbps quantum access network based on passive optical distribution network facilities," in *Laser Science* (Optica Publishing Group, 2023) pp. JTu7A–4.
[452]P. Huang, G.-Q. He, and G.-H. Zeng, "Bound on noise of coherent source for secure continuous-variable quantum key distribution," Int. J. Theor. Phys. **52**, 1572–1582 (2013).
[453]B. Stiller, I. Khan, N. Jain, P. Jouguet, S. Kunz-Jacques, *et al.*, "Quantum hacking of continuous-variable quantum key distribution systems: realtime trojan-horse attacks," in *CLEO: 2015* (Optica Publishing Group, 2015) p. FF1A.7.
[454]H. Qin, R. Kumar, and R. Alléaume, "Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution," Phys. Rev. A **94**, 012325 (2016).
[455]Y. Zhao, Y. Zhang, Y. Huang, B. Xu, S. Yu, *et al.*, "Polarization attack on continuous-variable quantum key distribution," J. Phys. B: At., Mol. Opt. Phys. **52**, 015501 (2018).
[456]H. Qin, R. Kumar, V. Makarov, and R. Alléaume, "Homodyne-detector-blinding attack in continuous-variable quantum key distribution," Phys. Rev. A **98**, 012312 (2018).
[457]Y. Zheng, P. Huang, A. Huang, J. Peng, and G. Zeng, "Security analysis of practical continuous-variable quantum key distribution systems under laser seeding attack," Opt. Express **27**, 27369–27384 (2019).
[458]Y. Zheng, P. Huang, A. Huang, J. Peng, and G. Zeng, "Practical security of continuous-variable quantum key distribution with reduced optical attenuation," Phys. Rev. A **100**, 012313 (2019).
[459]S. Ren, R. Kumar, A. Wonfor, X. Tang, R. Penty, *et al.*, "Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise," J. Opt. Soc. Am. B **36**, B7–B15 (2019).
[460]Y. Shao, Y. Li, H. Wang, Y. Pan, Y. Pi, *et al.*, "Phase-reference-intensity attack on continuous-variable quantum key distribution with a local local oscillator," Phys. Rev. A **105**, 032601 (2022).
[461]B. Huang, Y. Huang, and Z. Peng, "Practical security of the continuous-variable quantum key distribution with real local oscillators under phase attack," Opt. Express **27**, 20621–20631 (2019).
[462]L. Fan, Y. Bian, M. Wu, Y. Zhang, and S. Yu, "Quantum hacking against discrete-modulated continuous-variable quantum key distribution using modified local oscillator intensity attack with random fluctuations," Phys. Rev. Appl. **20**, 024073 (2023).
[463]Y. Pan, Y. Bian, H. Wang, J. Dou, Y. Shao, *et al.*, "Experimental demonstration of 4-user quantum access network based on passive optical network," Accepted by ECOC 2023.
[464]Q. Liao, Z. Wang, H. Liu, Y. Mao, and X. Fu, "Detecting practical quantum attacks for continuous-variable quantum key distribution using density-based spatial clustering of applications with noise," Phys. Rev. A **106**, 022607 (2022).
[465]S. Sajeed, P. Chaiwongkhot, A. Huang, H. Qin, V. Egorov, *et al.*, "An approach for security evaluation and certification of a complete quantum communication system," Sci. Rep. **11**, 5110 (2021).
[466]Y. Tian, P. Wang, J. Liu, S. Du, W. Liu, *et al.*, "Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber," Optica **9**, 492–500 (2022).
[467]A. A. Hajomer, H. Q. Nguyen, U. L. Andersen, and T. Gehring, "High-rate continuous-variable measurement-device-independent quantum key distribution," in *Optical Fiber Communication Conference* (Optica Publishing Group, 2023) pp. M2I–2.
[468]H. Guo, Z. Li, S. Yu, and Y. Zhang, "Toward practical quantum key distribution using telecom components," Fundam. Res. **1**, 96–98 (2021).