Research Article Vol. 12, No. 10 / October 2025 / Optica 1657

OPTICA

High-rate continuous-variable quantum key distribution over 100 km fiber with composable security

Heng Wang,[1] Yang Li,[1] Ting Ye,[1] Li Ma,[1] Yan Pan,[1] Mingze Wu,[2] Junhui Li,[2] Yiming Bian,[2] Yun Shao,[1] Yaodi Pi,[1] Jie Yang,[1] Jinlu Liu,[1] Ao Sun,[1] Wei Huang,[1] Stefano Pirandola,[3,4] Yichen Zhang,[2] and Bingjie Xu[1,*]

[1]National Key Laboratory of Security Communication, Institute of Southwestern Communication, Chengdu 610041, China
[2]State Key Laboratory of Information Photonics and Optical Communications, School of Electronic Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China
[3]Department of Computer Science, University of York, York YO10 5GH, UK
[4]stefano.pirandola@york.ac.uk
*xbjpku@163.com

Received 28 April 2025; revised 15 September 2025; accepted 15 September 2025; published 16 October 2025

Quantum key distribution (QKD), providing a way to generate secret keys with information-theoretic security, is arguably one of the most significant achievements in quantum information. The continuous-variable QKD (CV-QKD) offers the potential advantage of achieving a higher secret key rate (SKR) within a metro area, as well as being compatible with the mature telecom industry. However, the SKR and transmission distance of state-of-the-art CV-QKD systems are currently limited. Here, based on the proposed orthogonal-frequency-division-multiplexing (OFDM) CV-QKD protocol, we demonstrate a high-rate multi-carrier (MC) CV-QKD with a 10 GHz symbol rate that achieves Gbps SKR within 10 km and Mbps SKR over 100 km in the finite-size regime under composable security against collective attacks. The results are achieved by suitable optimization of subcarrier number and modulation variance, well-controlled excess noise induced by both the OFDM mechanism and the efficient DSP scheme, and high-performance post-processing capacity realized by the heterogeneous computing scheme. The composable finite-size SKR reaches 1779.45 Mbps@5 km, 1025.49 Mbps@10 km, 370.50 Mbps@25 km, 99.93 Mbps@50 km, 25.70 Mbps@75 km, and 2.25 Mbps@100 km, which improves the SKR by two orders of magnitude and quintuples the maximal transmission distance compared to the most recently reported CV-QKD results [Nat. Commun. 13, 4740 (2022)]. Interestingly, it is experimentally verified that the SKR of the proposed MC CV-QKD can approach five times larger than that of the single-carrier CV-QKD with the same symbol rate without additional hardware costs. Our work constitutes a critical step toward future high-speed quantum metropolitan and access networks.

https://doi.org/10.1364/OPTICA.566359

1. INTRODUCTION

Quantum key distribution (QKD) can guarantee secure key exchange between two remote parties with information-theoretic security based on the laws of quantum physics [1–3]. QKD systems encoding information on continuous variable (CV) quadratures of coherent states and decoding by coherent receivers offer the major potential advantages of achieving higher secret key rate (SKR) within metro areas and compatibility with the mature telecom industry [4–6]. This potential has led to remarkable advancements in continuous variable QKD (CV-QKD), including protocol design [7–10], security analysis [11–17], and system implementation [18–33]. The most important key figure of merit for any QKD system is to maximize the SKR over a certain distance, or conversely, to increase the distance over which a secret key can be generated. As summarized in Table 1, the SKRs and transmission distances for state-of-the-art CV-QKD systems significantly limit their large-scale deployments in high-speed quantum metropolitan and access networks.

To increase the SKR and transmission distance even further, a CV-QKD system needs to fulfill several key requirements. First, the system must operate at a higher symbol rate (SR), e.g., 10 GHz, which in turn will result in substantial excess noises in high-speed CV quantum state preparation, transmission, and detection [35]. In particular, the fiber chromatic dispersion noise encountered over long transmission distances will significantly increase the total excess noise for high-speed CV-QKD systems [36]. The SR for most state-of-the-art CV-QKD systems is about GHz currently [26–28], and the transmission distance for CV-QKD with 10 GHz

Table 1. SKR Comparison between the MC CV-QKD Scheme and the Existing QKD Works[a]

Ref.	Attacks	SR	Modulation	L (km)	Loss (dB)	R_∞ (Mbps)	Block Size	R_{finite} (Mbps)	CS	PP
This work	Finite-size collective	10 GHz	Gaussian	5	0.95	1819.32	10^{10}	1779.45	w/	w/
				10	1.8	1078.48		1025.49		
				25	4.75	374.19		370.50		
				50	9.5	112.96		99.93		
				75	12.8	34.63		25.70		
				100	15.8	12.58		2.25		
[26]	Asymptotic collective	5 GBaud	Four states	5	1	233.87	–	–	w/o	w/
				10	2	133.6				
				25	5	21.53				
[27]	Asymptotic collective	2.5 GBaud	16APSK	25	–	49.02	–	–	w/o	w/o
				50		11.86				
				80		2.11				
[28]	Asymptotic collective	1 GHz	Gaussian	50	10	7.55	–	–	w/o	w/o
				75	15	1.87				
				100	20	0.51				
[29]	Asymptotic collective	500 MHz	Gaussian	20	3.68	10.37	–	–	w/o	w/o
				50	9.26	1.61				
				70	12.94	0.34				
				100	18.96	0.06				
[30]	Finite-size* collective	600 MBaud	256QAM	9.5	1.9	–	5×10^6	91.8	w/o	w/o
				25	4.3			24		
[31]	Finite-size* collective	10 GBaud	64QAM	5	1	920	1.6×10^7	737	w/o	w/o
				10	2	480		315		
[32]	Finite-size collective	100 MHz	Gaussian	100	15.4	–	10^9	0.0254	w/o	w/
[33]	Finite-size collective	100 MHz	Gaussian	20	4	–	2×10^8	4.71	w/	w/
[34]	Finite-size general	2.5 GHz	Decoy BB84	10	2.2	–	10^8	115.8	w/	w/

[a] L, transmission distance; R_∞, SKR in asymptotic regime; R_{finite}, finite-size SKR; SR, symbol rate; CS, composable security; PP, post-processing.

SR is only limited to 10 km [31]. Second, the post-processing throughput is a strong limiting factor for real-time key generation, especially for CV-QKD system where error correction of continuous variable raw keys with high efficiency and high throughput under ultra-low SNR is technically challenging [37–40]. The throughput of error correction for CV-QKD with a typical code rate of 0.1 currently reaches 393.33 Mbps, which is far less than GHz SR [41]. To solve these problems, a multi-carrier (MC) CV-QKD scheme, including 194 low-speed CV-QKD systems, has been demonstrated based on wavelength-division multiplexing (WDM) method [42], but this scheme based on multiple transceivers is complex and cost ineffective. More importantly, due to the stringent demands for larger block sizes and tighter excess noise control [33], current CV-QKD systems have not yet exceeded 4.7 Mbps SKRs and extended transmission distances beyond 20 km under composable security against collective attacks, significantly limiting their practical application in high-speed secure communication.

Here, based on a novel orthogonal-frequency-division-multiplexing (OFDM) protocol and an efficient digital signal processing (DSP) scheme, we demonstrate for the first time a high-rate MC CV-QKD with 10 GHz SR that achieves Gbps SKR within 10 km and Mbps SKR over 100 km in finite-size regime with universal composability against collective attacks. Specifically, the 10 GHz OFDM-based MC CV-QKD contains five parallel subcarriers with 2 GHz SR each using only one transceiver, where the inherent chromatic dispersion noise in long-distance fiber channels is naturally mitigated. Then, a precise MC phase noise compensation (PNC) scheme that integrates pilot-tone-assisted phase recovery and TS-aided time domain superimposition equalization is designed to control the excess noise to a reasonably low level. The SKR for the OFDM-based MC CV-QKD protocol is maximized by an optimal choice of subcarrier number, based on the proposed systematical excess noise model, and by a global optimization of the modulation variance for each subcarrier, under the restricted capacity of post-processing with finite reconciliation efficiency and frame error rate (FER). Furthermore, a high-performance post-processing module based on heterogeneous computing is innovatively designed to realize the capacity of secure key generation in real time for each subcarrier, particularly utilizing shuffled belief propagation (BP) decoding on parallel multiple GPUs that achieves an error correction throughput of up to 1.6 Gbps.

By leveraging these technological advancements, the proposed OFDM-based MC CV-QKD system addresses the critical limitation of SC CV-QKD systems—their unavoidable excess noise growth with higher symbol rates that severely restricts SKR and transmission distance. Specifically, the asymptotic SKR for the MC system achieves 1819.32 Mbps@5 km, 1078.48 Mbps@10 km, 374.19 Mbps@25 km, 112.96 Mbps@50 km, 34.63 Mbps@75 km, and 12.58 Mbps@100 km, which marks the first instance of CV-QKD achieving Gbps SKR within 10 km transmission distance and 10 Mbps SKR over 100 km transmission distance. Interestingly, due to the excess noise suppression mechanism introduced by the OFDM method, the SKR of the 10 GHz MC CV-QKD system can approach five times larger than that of the single-carrier (SC) CV-QKD system with the same SR without additional hardware costs. Furthermore, the composable finite-size SKR reaches 1779.45 Mbps@5 km, 1025.49 Mbps@10 km,

370.50 Mbps@25 km, 99.93 Mbps@50 km, 25.70 Mbps@75 km, and 2.25 Mbps@100 km, which achieves the first CV-QKD with Gbps SKR and 100 km transmission distance in finite-size regime with universal composability against collective attacks to date. Compared to the stat-of-the-art CV-QKD results [33], our work improves the composable finite-size SKR by two orders of magnitude and quintuples the maximal transmission distance. Compared to the latest discrete variance QKD (DV-QKD) work [34], this CV-QKD work improves the SKR by one order of magnitude over 10 km metropolitan area.

2. RESULTS

A. MC CV-QKD Protocol

Alice modulates N independent random keys on N modes (or subcarriers) coherent state as $\otimes_{k=1}^{N}|X_k + jP_k\rangle$ with Gaussian modulation scheme based on OFDM method and transmits the prepared quantum states to Bob through quantum channel. Bob measures the received quantum state with a heterodyne receiver and obtains the raw keys for each mode after digital demodulation. Then, Alice and Bob perform post-processing, including reverse reconciliation, error correction (EC), parameter estimation (PE), and privacy amplification (PA) steps [43], independently on raw keys of each mode to extract the final secure key. The SKR for the OFDM-based MC CV-QKD protocol can be expressed as

$$R_{\text{multi}} = \sum_{k=1}^{N} R_{\text{sub}}^{(k)}, \tag{1}$$

with $R_{\text{sub}}^{(k)}$ as the SKR of the kth subcarrier. To evaluate the performance of the MC CV-QKD protocol, the MC excess noise is carefully modeled, incorporating additional noise components such as intermodulation distortion (ID) noise and intercarrier interference (ICI) noise. Based on this noise model, the subcarrier number N and the modulation variance V_A for each subcarrier are optimized to maximize the SKR. The detail of excess noise model and the optimization of N and V_A can be explained in Section 5 and Supplement 1. Notably, the wideband CV-QKD system is decomposed into multiple parallel low-speed SC subsystems by OFDM method, thereby inheriting security guarantees from the SC CV-QKD security framework.

We adopt the formula for the composable key rate derived in [44], which is here assumed to be applied to each subcarrier independently. Since EC is performed before PE, all raw keys remain available for both PE and key extraction processes. Consequently, the effective key generation length n becomes equivalent to the total key-string length N_t in each subcarrier [45]. Considering the procedures of EC and PA on the n key generation point, the length of the composable secret key will be reduced to $s_n^{(k)}$, which can be bounded using the leftover hash bound as [43]

$$s_n^{(k)} \le H_{\min}^{\varepsilon_s}\left(B^n \left| E^n\right.\right)_{\sigma^n} - \text{leak}_{\text{EC}} + \log_2\left(2\varepsilon_\hbar^2\varepsilon_{\text{cor}}\right), \tag{2}$$

where $H_{\min}^{\varepsilon_s}(B^n|E^n)_{\sigma^n}$ is the smooth-min entropy of the subnormalized state σ^n of Bob's quantum system B^n conditioned on Eve's quantum system E^n with smoothing parameter ε_s. Here, $\varepsilon_\hbar$ is the security parameter related to PA, ε_{cor} is the security parameter for error verification, and leak_{EC} is the information leaked during EC.

To apply the asymptotic equipartition property (AEP) and calculate the secret key length, the smooth-min entropy of the subnormalized state σ^n after EC can be replaced by the normalized state $\rho^{\otimes n}$ before EC according to the following inequality [44]:

$$H_{\min}^{\varepsilon_s}\left(B^n \left| E^n\right.\right)_{\sigma^n} \ge H_{\min}^{\varepsilon_s}\left(B^n \left| E^n\right.\right)_{\rho^{\otimes n}}. \tag{3}$$

Thereby, the smooth-min entropy can be bounded by von Neumann entropy via the AEP as [46]

$$H_{\min}^{\varepsilon_s}\left(B^n \left| E^n\right.\right)_{\rho^{\otimes n}} \ge nH(B\,|E)_\rho - \sqrt{n}\Delta_{\text{aep}}, \tag{4}$$

where

$$\Delta_{\text{aep}} = 4\log_2\left(\sqrt{2^d}+2\right)\sqrt{-\log_2\left(1-\sqrt{1-\varepsilon_s^2}\right)}, \tag{5}$$

and d is the quantization bits of the ADC in Bob's system.

The conditional von Neumann entropy can be expanded as

$$H(B\,|E)_\rho = H(l\,|E)_\rho = H(l) - \chi(l:E)_\rho, \tag{6}$$

where l is Bob's variable, $H(l)$ is the Shannon entropy of l, and $\chi(l:E)_\rho$ is Eve's Holevo bound with respect to l. According to [44], the asymptotic SKR can be expressed as

$$R_\infty^{(k)} = H(l) - \chi(l:E)_\rho - n^{-1}\text{leak}_{\text{EC}}, \tag{7}$$

and the secret key length should satisfy the following bound:

$$s_n^{(k)} \le nR_\infty^{(k)} - \sqrt{n}\Delta_{\text{aep}} + \log_2\left(2\varepsilon_\hbar^2\varepsilon_{\text{cor}}\right). \tag{8}$$

Since EC has failure probability $\text{FER}^{(k)}$ of the kth subcarrier, and only a fraction n/N_t of the total initial systems is used for key generation, the composable SKR under collective attacks can be upper bounded as [44]

$$R^{(k)} \le R_{\text{UB}}^{(k)} = \frac{\left(1-\text{FER}^{(k)}\right)\left[nR_\infty^{(k)} - \sqrt{n}\Delta_{\text{aep}} + \log_2\left(2\varepsilon_\hbar^2\varepsilon_{\text{cor}}\right)\right]}{N_t}. \tag{9}$$

Using the direct part of the leftover hash bound [46], the lower bound of composable SKR with optimal PA can be calculated as [44]

$$R^{(k)} \ge R_{\text{LB}}^{(k)} = \frac{\left(1-\text{FER}^{(k)}\right)\left[nR_\infty^{(k)} - \sqrt{n}\Delta_{\text{aep}} + \log_2\left(2\varepsilon_\hbar^2\varepsilon_{\text{cor}}\right) - 1\right]}{N_t}, \tag{10}$$

where the asymptotic term $R_\infty^{(k)}$ should be computed as

$$R_\infty^{(k)} = \beta^{(k)}[I_{AB}]_{(T,\xi)} - [\chi_{BE}]_{(T_{\text{wc}},\xi_{\text{wc}})}, \tag{11}$$

where I_{AB} is Alice and Bob's mutual information, χ_{BE} is Eve's Holevo bound, and β^k is reconciliation efficiency. T and ξ are the estimated values of transmittance and excess noise, respectively. The worst-case values can be calculated accounting for the value ε_{pe} of the PE security parameter [44]:

$$T_{\text{wc}} \simeq T - w\sigma_T, \tag{12}$$

$$\xi_{\text{wc}} \simeq \frac{T}{T_{\text{wc}}}\xi + w\sigma_\xi, \tag{13}$$

where

$$\sigma_T = \frac{2T}{\sqrt{2m}}\sqrt{\left(\xi + \frac{2+\nu_{el}}{\eta T}\right)/V}, \tag{14}$$

$$\sigma_\xi = \frac{1}{\sqrt{m}} \frac{\eta T \xi + v_{el} + 2}{\eta T_{\mathrm{wc}}}, \tag{15}$$

$$w = \sqrt{2}\mathrm{erf}^{-1}\left(1 - 2\varepsilon_{\mathrm{pe}}\right), \tag{16}$$

with $\mathrm{erf}^{-1}(\cdot)$ being the inverse error function.

Finally, the SKR of the kth subcarrier can be expressed as

$$R_{\mathrm{sub}}^{(k)} = \sum_{k=1}^{N} f_{\mathrm{sym}}\left(1 - a^{(k)}\right) R^{(k)}, \tag{17}$$

where f_{sym} is the symbol rate, and $a^{(k)}$ denotes the overhead for training sequences (TSs) of the kth subcarrier.

Considering the steps of EC, PE, and PA, the protocol has total epsilon security,

$$\varepsilon = \varepsilon_{\mathrm{cor}} + \varepsilon_s + \varepsilon_h + 2\varepsilon_{\mathrm{pe}}, \tag{18}$$

for each subcarrier. Each epsilon is set to 10^{-10}, resulting in a total $\varepsilon = 5 \times 10^{-10}$ per subcarrier for a given block size. Notably, we build upon the technique introduced in Ref. [44] to derive a bound that accommodates parameter estimation after error correction, achieving the tightness of the SKR expressions and the low overhead caused by parameter estimation. Furthermore, our work adopts the composable security framework for Gaussian CV-QKD against collective attacks, offering a well-established and widely accepted trade-off between security rigor and experimental feasibility. While coherent-attack security represents a valuable research direction, its comprehensive investigation remains subject to advancements in system performance and finite-size analysis techniques.

3. EXPERIMENTAL SETUP

Using the setup shown in Fig. 1, we experimentally demonstrate the OFDM-based MC CV-QKD system with optimal $N = 5$ independent subcarriers over typical transmission distances of 5 km, 10, 25, 50, 75, and 100 km, respectively. At Alice's site, a continuous optical carrier at frequency f_A from Alice's laser is split into two optical paths by a polarization beam splitter (PBS). One path is Gaussian-modulated in an in-phase and quadrature (IQ) modulator (FUJITSU FTM7962EP) by the OFDM signal I_s and Q_s with shifting frequency $f_s = 8.5$ GHz and SR $f_{\mathrm{sym}} = 10$ GHz, which are generated from a two-channel digital-to-analog converter (DAC) in an arbitrary waveform generator (AWG, Keysight M8195A) with a sampling rate of 30 GSa/s. Figure 2(a) demonstrates the DSP routine of the OFDM-based MC generator at Alice's site and the desired quantum frequency spectra with 13 GHz bandwidth. Notably, the power spectra in Fig. 2(a) exhibit a mirror sideband caused by IQ gain imbalance and phase offset in AWG, which could potentially affect modulation variance estimation and introduce eavesdropping vulnerabilities [47]. However, this impact is minimal as it remains more than 20 dB below the desired OFDM spectra and is further eliminated through AWG bandpass filtering in practical implementation. The other path is directly attenuated to be a pilot tone with reasonable amplitude. The prepared MC quantum signal and pilot tone are transmitted through an SMF (ITU-T G.652) with different frequency bands and orthogonal polarization states. At Alice' site, two cascaded acousto-optic modulators (AOMs) are used as a high-speed optical switch with a 100 dB ER to realize real-time SNU calibration within a short time period (see Section 5 for more details).

In this experiment, the modulation variance for each subcarrier can be monitored and precisely controlled with a precision of 0.1 SNU. To maximize the SKR, we propose a global optimization method of modulation variance for each subcarrier under restricted capacity of post-processing with finite reconciliation efficiency and FER [48], based on which the modulation variances of the five subcarriers are independently optimized to be 3.8, 3.6, 3.8, 4.1, and 4.1 SNU over 50 km transmission distance as an example. The detailed modulation variance optimization routine and experimental results can be found in Section 5 and Supplement 1.

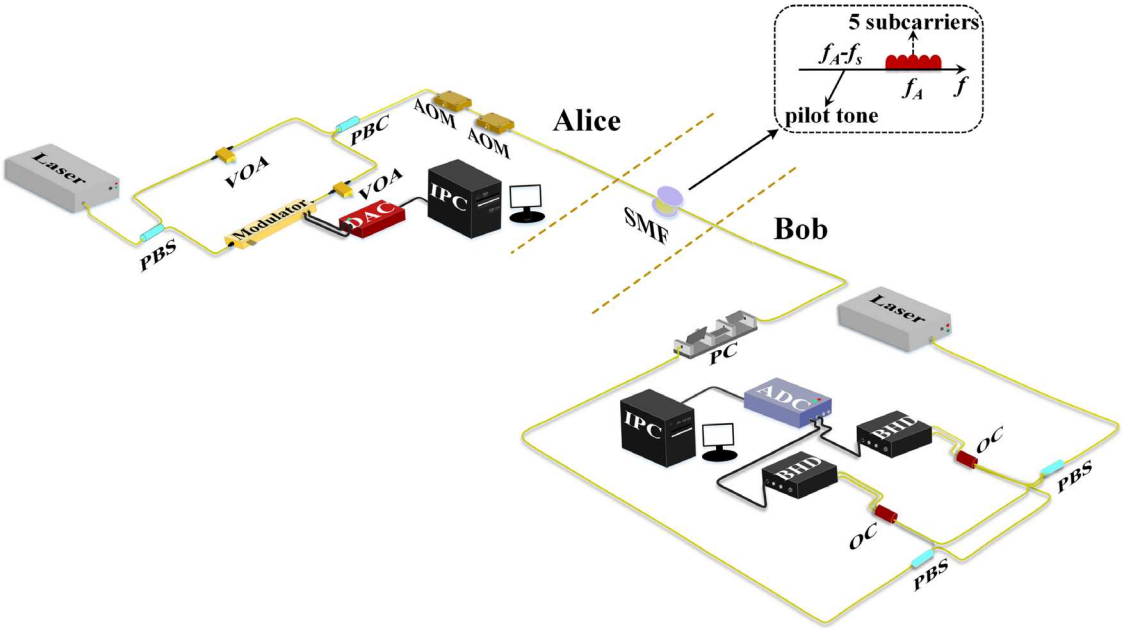

Fig. 1. Schematic setup of the proposed OFDM-based MC CV-QKD scheme. PBS: polarization beam splitter; VOA: variable optical attenuator; DAC: digital-to-analog converter; PBC: polarization beam combiner; AOM: acousto-optic modulator; SMF: single-mode fiber; PC: polarization controller; OC: optical coupler; BHD: balance homodyne detector; ADC: analog-to-digital converter; IPC: industrial personal computer.

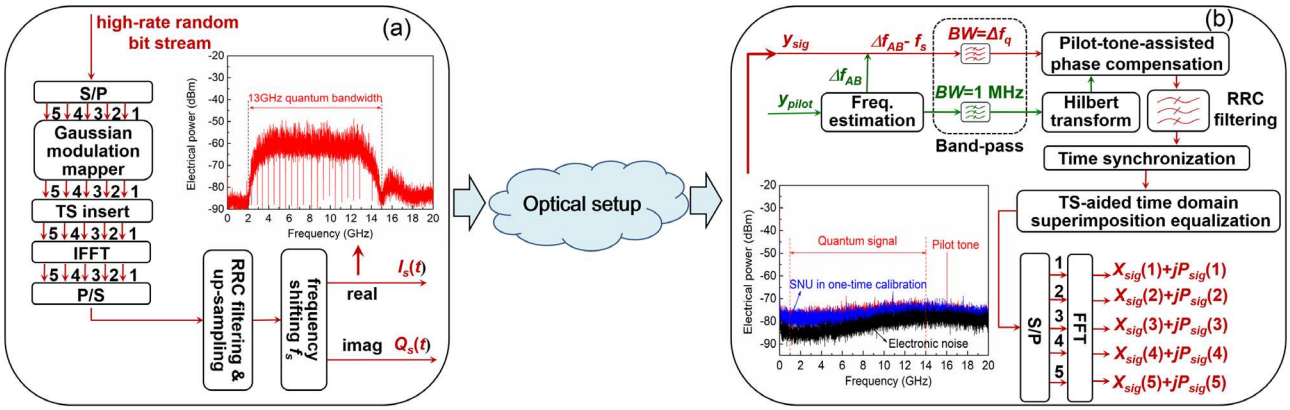

Fig. 2. DSP routine of the OFDM-based MC CV-QKD experiment, (a) OFDM-based MC generator, (b) OFDM-based MC demodulator. S/P, serial-to-parallel conversion; TS, training sequence; IFFT, inverse fast Fourier transform; P/S, parallel-to-serial conversion; CP, cyclic prefix; BW, bandwidth; RRC, root raised cosine; DAC, digital-to-analog converter; FFT, fast Fourier transform; and SNU, shot noise unit.

At Bob's site, the received MC quantum signal and pilot tone are polarization-corrected by a polarization controller (PC) and then separated by a PBS. This configuration allows the MC quantum signal and pilot tone to be separately detected using two wideband balanced homodyne detectors (BHDs, Optilab BPR-23-M) with 23 GHz bandwidth. The LLO signals used for detection are independently generated from Bob's laser, which is identical to Alice's laser (NKT Photonic Basik E15). The frequency difference Δf_{AB} between the two lasers is set to approximately 16 GHz. The output signals from the two BHDs are collected and digitized by a two-channel analog-to-digital converter (ADC) in a high-speed digital signal analyzer (DSA, Keysight DSAZ254A) with a sampling rate of 40 GSa/s. The AWG and DSA are synchronized using a 100 MHz reference clock and triggered with the switching signals of AOMs. After heterodyne detection, the measurement results of the five subcarriers can be extracted using the designed OFDM-based MC demodulator at Bob's site. The corresponding DSP routine and the detected frequency spectra are depicted in Fig. 2(b). Notably, this experiment employs two high-stability lasers with ultra-narrow linewidth and utilizes the pilot tone for real-time frequency difference estimation, enabling precise quantum signal filtering in the DSP. Moreover, the SNU is measured with the one-time calibration method when Alice's laser is off and Bob's laser is on in the experiment.

For the proposed MC CV-QKD, a real-time post-processing with throughput larger than 1.6 GHz is required for each subcarrier with 2 GHz SR excluding the disclosed 1/5 percentage of TS. To meet this requirement, we innovatively designed a high-performance post-processing module based on heterogeneous computing, which can achieve an error correction throughput exceeding 1.6 GHz by utilizing shuffled BP decoding on six parallel graphics processing units (GPUs, NVIDIA Tesla A100). Moreover, a single GPU can achieve a worst-case error correction throughput of 279.2 Mbps over typical transmission distances of 5, 10, 25, 50, 75, and 100 km. The detailed post-processing routine and results can be found in Section 5 and Supplement 1. Notably, although the 10 GHz MC CV-QKD system with five subcarriers requires the same total post-processing throughput as an SC system with the same symbol rate, the MC system performs better post-processing efficiency because each subcarrier inherently operates with low excess noise.

A. Multi-Carrier Noise Suppression

It is well known that the performance of a CV-QKD system is very sensitive to its excess noise. Compared with the traditional SC CV-QKD system, the MC system based on the OFDM scheme will introduce new types of excess noise due to the crosstalk between different subcarriers in the process of multi-carrier quantum state modulation, transmission, and detection. To evaluate the system performance and realize parameter optimization, we propose a systematical excess noise model for the OFDM-based MC CV-QKD system. The excess noise ε_k of the kth subcarrier can be mainly classified as [35]

$$\varepsilon_k = \varepsilon_{\mathrm{RIN}}(k) + \varepsilon_{\mathrm{DAC}}(k) + \varepsilon_{\mathrm{LE}}(k) + \varepsilon_{\mathrm{mod}}(k) + \varepsilon_{\mathrm{phase}}(k)\,, \quad (19)$$

where $\varepsilon_{\mathrm{RIN}}(k)$ denotes the laser intensity noise, $\varepsilon_{\mathrm{DAC}}(k)$ represents the quantization noise due to practical DAC, $\varepsilon_L(k)$ is the photon-leakage noise that mainly stems from the intense pilot tone, and $\varepsilon_{\mathrm{mod}}(k)$ denotes the modulation noise of the kth subcarrier that consists of finite modulation extinction ratio (ER) noise, IQ imbalance noise, and ID noise [49]. It is remarkable that the ID noise induced in the MC quantum state modulation process cannot be ignored when N is large enough. Additionally, this MC CV-QKD system achieves secure Gaussian-like modulation at 10 GHz with 8-bit resolution, satisfying Gaussian discretization security requirements as analyzed in [50].

The phase noise $\varepsilon_{\mathrm{phase}}(k)$ that dominates the excess noise mainly contains common phase error (CPE) noise and ICI noise. The CPE noise is mainly determined by the fiber chromatic dispersion noise, the channel phase difference, and the time-varying laser phase difference. Specifically, the fiber chromatic dispersion noise encountered over long transmission distance will significantly increase for CV-QKD systems with high SR, as shown in Fig. 3, which can be effectively reduced by operating parallelly at lower SR with the MC scheme even for long transmission distances [36]. For example, the dispersion noises for CV-QKD system with 10 GHz and 2 GHz SR correspond to 0.0294 and 4.711×10^{-5} in shot noise unit (SNU) over 50 km fiber channel, respectively. In the MC CV-QKD system, one can transform an SC quantum state with SR f_{sym} into N parallel subcarrier quantum states with SR f_{sym}/N, which in principle can naturally mitigate the inherent chromatic dispersion noise. Furthermore, the channel phase difference can be effectively managed by the proposed PNC scheme. The ICI

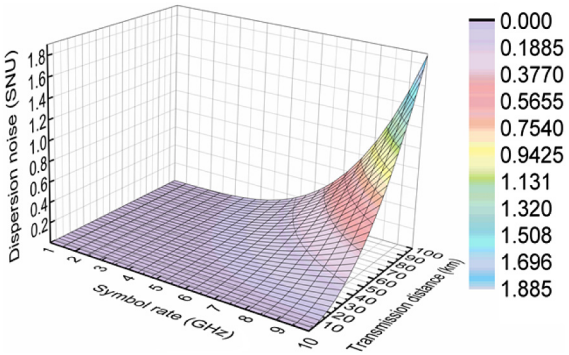

Fig. 3. Simulated dispersion noise at different symbol rates and different transmission distances.

noise of the kth subcarrier arises from the interference of other subcarriers ($i \neq k$) due to the existence of time-varying laser phase difference [51], which can be controlled to a reasonably low value for small N.

An optimal subcarrier number $N = 5$ for the best SKR is chosen based on the proposed excess noise model. The detail of excess noise model and the optimization of subcarrier number N can be explained in Section 5 and Supplement 1. This work optimizes the subcarrier number N by considering multiple MC excess noise components, expanding beyond the consideration of modulation noise in our previous work [49]. Furthermore, while fiber chromatic dispersion (affecting CPE noise) and ICI noise originate in the fiber channel, they ultimately manifest as phase differences at Bob's site, verifying the appropriateness of attributing ICI noise to phase noise. Finally, based on the proposed MC noise model, a quantified example is demonstrated that the excess noises are respectively calculated to be 0.0256 SNU for MC ($N = 5$) and 0.0550 SNU for SC ($N = 1$) at 50 km transmission distance, with modulation variance $V_A = 4$ SNU and PNC-compensated phase difference of 0.04.

In order to realize a reasonably low excess noise, a high-precision MC PNC scheme is designed to eliminate the phase noise in the implemented setup. In this scheme, a pilot-tone-assisted PNC method is used to compensate for the fast-drift phase noise of the MC quantum signal which mainly originates from the rapid phase disturbances of two independent lasers and the fiber channel [52]. After the fast-drifting PNC, a TS-aided time domain superimposition equalization method is proposed for further eliminating the slow-drift phase noise with 1/5 percentage of TSs embedded in the MC quantum signal. In the experiment, we optimize the TS ratio to achieve precise phase compensation while minimizing the SKR overhead. It is worth noting that the accuracy of compensating slow-drift phase noise can be significantly improved by superimposing TSs of multiple blocks for a TS with higher SNR. Importantly, this TS-aided PNC method reduces the high linearity requirements of fast data acquisition cards for high SR CV-QKD without depending on TS with high SNR. Note that excessive superposition not only increases computational complexity but also imposes more stringent requirements on the temporal stability of the channel response. Consequently, the number of superposition times should be minimized, subject to satisfying the accuracy requirements of the TS. Furthermore, modulation noise, channel noise, and detection noise originating from the pilot tone with a high signal-to-noise ratio (SNR) can be effectively minimized in the experiment. This is achieved through independent preparation, multiplexing transmission, and separate detection of the weak MC quantum signal and intense pilot tone. In particular, the spontaneous Rayleigh or Brillouin scattering spectra caused by an intense pilot tone can be avoided by placing a 2 GHz frequency spacing between the pilot tone and MC quantum signal. Additionally, the demonstrated LLO CV-QKD scheme maintains equivalent security to conventional LLO CV-QKD while inherently preventing LO side-channel attacks, as the pilot tone serves exclusively as an untrusted phase reference between Alice and Bob.

B. Performance and Secret Key Distillation

Choosing optimal modulation variances for each subcarrier with $f_{\mathrm{sub}} = 2$ GHz, the excess noises of the five subcarriers are experimentally estimated with block size 1.3×10^7 over typical transmission distances of 5, 10, 25, 50, 75, and 100 km, respectively, as shown in Fig. 4. The average asymptotic SKRs for the MC CV-QKD system are evaluated to be 1819.32 Mbps@5 km, 1078.48 Mbps@10 km, 374.19 Mbps@25 km, 112.96 Mbps@50 km, 34.63 Mbps@75 km, and 12.58 Mbps@100 km.

To verify the potential advantage of the OFDM-based MC CV-QKD scheme, we also experimentally implement an SC CV-QKD system with 10 GHz SR under the same conditions (see Supplement 1 for details). The numerical simulation and experimental results of SKRs for MC and SC CV-QKD setups over different transmission distances are compared in Fig. 5(a). Moreover, an SKR gain is defined as the SKR ratio between MC and SC CV-QKD protocols under the same conditions. The corresponding SKR gains at transmission distances of 5, 10, 25, 50, and 75 km reach 1.09, 1.10, 1.13, 1.54, and 5.55, respectively, as demonstrated in Fig. 5(b). Notably, the SKR gain for 100 km cannot be provided because no secure key can be generated for the implemented SC CV-QKD setup over 100 km. These results indicate that the SKR of the proposed MC CV-QKD can be improved compared to that of SC CV-QKD with the same SR without additional hardware costs. Meanwhile, the SKR gains gradually increase with the transmission distance, which verifies that the MC CV-QKD scheme is more prominent for long transmission distances. Furthermore, the experimentally measured SKR gain is slightly lower than the theoretical estimation value over 75 km as in Fig. 5(b), as the proposed PNC scheme only partially compensates the SC dispersion phase. The compensation effect of the SC dispersion phase will gradually become worse as the transmission distance increases. In contrast, MC CV-QKD systems have a lower PNC requirement due to their natural ability to mitigate inherent chromatic dispersion noise. Notably, the performance of the demonstrated OFDM-based CV-QKD system suffers from hardware characteristics, with broader laser linewidths significantly reducing SKR gains. This degradation primarily originates from OFDM-induced ICI noise, which exhibits strong sensitivity to laser linewidth, as demonstrated by Eq. (S30) in Supplement 1.

Subsequently, we evaluate the SKR performance of the MC CV-QKD system under a composable security framework in a finite-size regime, which is of particular interest in practical cryptographic applications. To distill positive SKR over a long transmission distance, a large block size is required for excess noise estimation and composable finite-size SKR evaluation. In the experiment, we make an average estimator of 10 block sizes for achieving the composable finite-size SKR with a total block size of

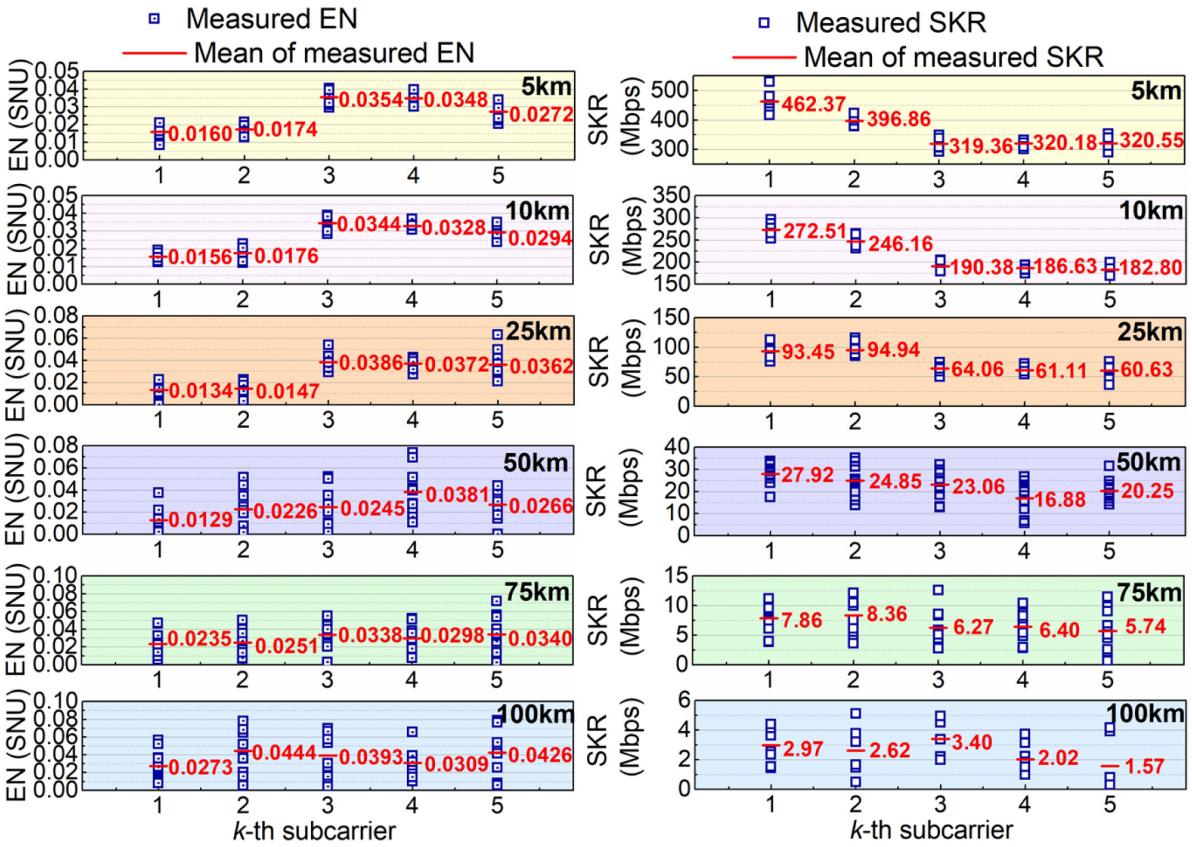

Fig. 4. Experimentally estimated excess noises and asymptotic SKRs for five independent subcarriers over typical transmission distances of 5, 10, 25, 50, 75, and 100 km. EN, excess noise; SKR, secret key rate.

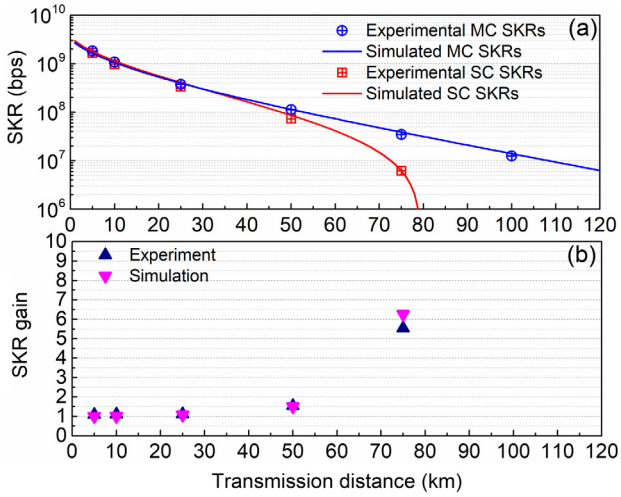

Fig. 5. Measured SKR comparison between MC and SC CV-QKD over different transmission distances in asymptotic regime. MC, multi-carrier; SC, single-carrier; and SKR, secret key rate.

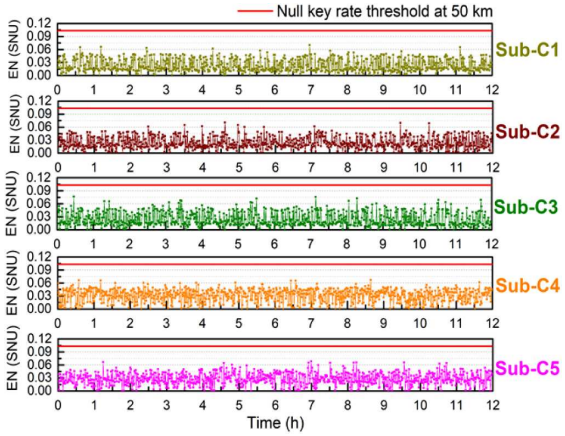

Fig. 6. Experimental excess noises measured for five independent subcarriers over 12 h under the transmission distance of 50 km. EN, excess noise; Sub-C, subcarrier.

10^{10}, where each block size is obtained by accumulating 80 frames of data in continuous time. Note that the precise accumulation of the 80 frames of data requires the excellent stability of the MC CV-QKD system. Figure 6 shows the experimentally estimated excess noise over continuous 12 h over 50 km transmission distance, verifying the continuous operation stability of our system. Under the block size of 10^{10}, the worst-case excess noise and composable finite-size SKR are estimated over typical distances of 5, 10, 25, 50, 75, and 100 km, as summarized in Table 2. The MC excess noise and SKR in Table 2 represent the average excess noise and the sum of SKRs for the five subcarriers, respectively.

4. DISCUSSION

In this work, we have experimentally demonstrated a high-rate MC CV-QKD based on the novelly proposed OFDM protocol. By modeling MC excess noise, an optimal subcarrier number $N = 5$ is chosen to achieve the maximal SKR. Thus, the MC CV-QKD

Table 2. Estimated Worst-Case Excess Noises and Composable Finite-Size SKRs with Block Size of 1×10^{10} over Different Transmission Distances[a]

Composable Security	Sub-C1	Sub-C2	Sub-C3	Sub-C4	Sub-C5	MC	Distance
Excess noise (SNU)	0.0145	0.0253	0.0339	0.0311	0.0265	0.0263	5 km
SKR (Mbps)	454.04	370.06	356.78	280.70	317.87	1779.45	
Excess noise (SNU)	0.0158	0.0288	0.0346	0.0328	0.0274	0.0279	10 km
SKR (Mbps)	258.95	209.30	206.70	162.55	187.99	1025.49	
Excess noise (SNU)	0.0154	0.0157	0.0386	0.0362	0.0413	0.0294	25 km
SKR (Mbps)	87.61	104.13	66.50	57.37	54.89	370.50	
Excess noise (SNU)	0.0065	0.0064	0.0376	0.0453	0.0412	0.0274	50 km
SKR (Mbps)	27.65	32.31	16.06	11.06	12.85	99.93	
Excess noise (SNU)	0.0164	0.0195	0.0228	0.0356	0.0357	0.0260	75 km
SKR (Mbps)	6.54	7.47	5.92	2.81	2.96	25.70	
Excess noise (SNU)	0.0349	0.0103	0.0632	0.0613	0.0556	0.0451	100 km
SKR (Mbps)	0.03	2.21	8.4e-4	8.1e-4	5.3e-3	2.25	

[a]SKR, secret key rate; SNU, shot noise unit; Sub-C, subcarrier; MC, multi-carrier.

operating at 10 GHz SR is converted into five parallel subcarriers with 2 GHz SR using only one transceiver. In this experiment, the five low-speed subcarriers can be respectively realized with reasonably low excess noise based on the OFDM mechanism and well-designed PNC scheme. Moreover, the modulation variance for each subcarrier is finely optimized under restricted capacity of post-processing with finite β_k and FER_k. Furthermore, a high-performance post-processing module with worst-case error correction throughput up to 1.6 Gbps is efficiently achieved by the innovatively designed shuffled BP decoding scheme on multi-GPUs, enabling the practical real-time extraction of the final secure keys for each subcarrier. Finally, the experimental asymptotic SKRs achieve 1819.32 Mbps@5 km, 1078.48 Mbps@10 km, 374.19 Mbps@25 km, 112.96 Mbps@50 km, 34.63 Mbps@75 km, and 12.58 Mbps@100 km. Interestingly, comparing our MC CV-QKD with SC CV-QKD operating at 10 GHz SR, the SKR gain reaches up to five times without additional hardware costs. Furthermore, the more practical SKRs are reported as 1779.45 Mbps@5 km, 1025.49 Mbps@10 km, 370.50 Mbps@25 km, 99.93 Mbps@50 km, 25.70 Mbps@75 km, and 2.25 Mbps@100 km under finite-size regime with universal composability against collective attacks.

Compared with the state-of-the-art QKD works shown in Table 1, our work performs the first experimental implementation of 10 GHz SR MC CV-QKD based on OFDM protocol, which offers a robust advantage in well mitigating the chromatic dispersion noise. Moreover, our work successfully develops a high-performance post-processing module capable of extracting the secure key of each subcarrier with 2 GHz SR in real time. As a result, our work firstly achieves an MC CV-QKD with finite-size SKR of Gbps within 10 km and Mbps over 100 km under composable security against collective attacks. Furthermore, our work improves the composable finite-size SKR by two orders of magnitude and increases the maximum transmission distance four-fold compared to the most state-of-the-art results [33], verifying the high rate of the proposed MC CV-QKD. Compared to the most recent progress in DV-QKD with 110 Mbps@10 km, this CV-QKD work improves the SKR by an order of magnitude over 10 km metropolitan area [34], indicating readiness for future high-rate practical CV-QKD deployment. The proposed MC CVQKD scheme enables flexible distribution of N independent subcarriers with variable symbol rates and modulation protocols, offering enhanced interoperability, dynamic bandwidth optimization, and improved security through randomized multi-protocol operation.

5. METHODS

A. OFDM-Based MC DSP

In this experiment, the DSP of the OFDM-based MC CV-QKD includes MC generation at Alice's site and MC demodulation at Bob's site. At Alice's site, the DSP routine of the OFDM-based MC generator is shown in Fig. 2(a) and described as follows. (i) A high-rate serial random bit stream is converted into five parallel low-rate random bit streams using serial-to-parallel conversion (S/P). Notably, the random bits are generated from a high-speed quantum random number generator. (ii) The five parallel bit streams are each mapped to Gaussian-modulated subcarriers and then insert 1/5 proportion of TS. After inverse fast Fourier transform (IFFT), the orthogonal Gaussian-modulated subcarriers are converted to the desired OFDM signal through parallel-to-serial conversion (P/S). (iii) The OFDM signal is further shaped by an RRC filter with a roll-off factor of 0.3 and up-sampled to 30 GSa/s. (iv) The OFDM signal is frequency-shifted by $f_s = 8.5$ GHz for the intermediate frequency (IF) detection in our scheme. (v) The real part and imaginary part of the formed OFDM signal are, respectively, converted by a two-channel DAC, and the obtained $I_s(t)$ and $Q_s(t)$ are applied onto two driving electrodes of the I/Q modulator, respectively.

At Bob's site, the DSP routine of the OFDM-based MC demodulator is depicted in Fig. 2(b) and described as follows. (i) The detected MC quantum signal and pilot tone are digitized as y_{sig} and y_{pilot} by a high-speed DSA. (ii) The frequency difference Δf_{AB} of two independent lasers is estimated to be 16 GHz by peaking the frequency spectra of the digitized pilot signal y_{pilot}. Thus, the central frequency $\Delta f_{AB} - f_s$ of the MC quantum signal is calculated to be 7.5 GHz, given the known shifting frequency $f_s = 8.5$ GHz. (iii) The digitized MC quantum signal and pilot signal are bandpass-filtered at the central frequencies $\Delta f_{AB} - f_s$ (7.5 GHz) and Δf_{AB} (16 GHz), respectively. (iv) The bandpass-filtered pilot signal is Hilbert transformed to extract the in-phase and quadrature components of the MC quantum signal. (v) In the proposed high-precision PNC scheme, the fast-drift phase noise is initially compensated using the sharing phase of the pilot tone according to the pilot-tone-assisted phase compensation method.

After the RRC matched filtering and time synchronization, the slow-drift phase noise is further compensated by employing the TS-aided time domain superimposition equalization method based on the least mean square (LMS) algorithm. It is important to note that TSs of M blocks are time-domain superimposed to create a TS with higher SNR, which is then used to compensate for the phase noise of the quantum signal in the M blocks (e.g., the optimal $M = 16$ in the experiment). (vi) The compensated MC quantum signal is serial-to-parallel converted and then fast Fourier transformed into five-parallel quantum raw keys.

B. Parameter Optimization

In the MC CV-QKD system, one can parallelly achieve multichannel key distribution and reduce the chromatic dispersion noise by increasing the subcarrier number N, however, which will induce increased ID noise and ICI noise. Thus, an optimal N should be chosen to achieve maximal SKR for the MC CV-QKD system. The SKR gains at different subcarrier number N and different transmission distances are calculated and shown in Fig. 7, where the SKRs of MC CV-QKD and SC CV-QKD are simulated under the same condition. One can see from Fig. 7 that the optimal choice of N approaches 5 for this experimental setups. Moreover, the SKR gain gradually increases with transmission distances due to the excess noise suppression effect provided by OFDM mechanism.

In a practical experiment, the modulation variance $V_A(k)$ for the kth subcarrier is globally optimized under restricted capacity of post-processing with finite β_k and FER_k [48]. Taking the 50 km transmission distance as an example, the detailed optimization process of $V_A(k)$ for the kth subcarrier is described as follows. (i) The transmittance T, excess noise ε_k, and detection efficiency η_k are experimentally calibrated and updated in real-time for kth subcarrier. (ii) In a suitable modulation variance range (e.g., from 0 to 10 SNU), the corresponding SNRs and the error correction matrix $\mathbf{H}$ are selected to determine the code rate CR_k. The function of $\beta_k - V_A(k)$ is computed as $\mathrm{CR}_k/(0.5\log_2(1+\mathrm{SNR}_k))$. (iii) Based on the experimental data, one can obtain a numerical relationship of $\mathrm{FER}_k - V_A(k)$ through curve fitting under the specific performance of data reconciliation and error correction. (iv) Using $\beta_k - V_A(k)$ and $\mathrm{FER}_k - V_A(k)$, the comprehensive function of asymptotic SKR R_k on $V_A(k)$ is derived, enabling the estimation of the optimal modulation variances for the five subcarriers as follows: $V_A(1) = 3.8$ SNU ($\beta_1 = 0.9296$, $\mathrm{FER}_1 = 0.0209$), $V_A(2) = 3.6$ SNU ($\beta_2 = 0.9299$, $\mathrm{FER}_2 = 0.0234$), $V_A(3) = 3.8$ SNU ($\beta_3 = 0.9301$, $\mathrm{FER}_3 = 0.0252$), $V_A(4) = 4.1$ SNU ($\beta_4 = 0.9311$, $\mathrm{FER}_4 = 0.0362$), and $V_A(5) = 4.1$ SNU ($\beta_5 = 0.9305$, $\mathrm{FER}_5 = 0.0292$). This optimization scheme ensures that the SKR for each subcarrier is optimal over a certain transmission distance.

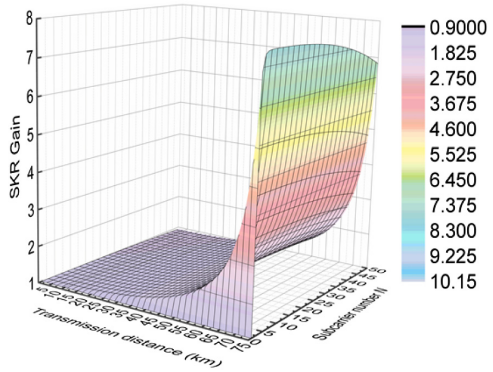

Fig. 7. Simulated SKR gains for different subcarrier number N and different transmission distances.

C. One-Time and Real-Time SNU Calibration

In a realistic scenario, inaccuracies in SNU calibration significantly impact the estimated SKR. In our work, a one-time and real-time SNU calibration scheme is implemented to accurately evaluate the SKR of the CV-QKD setup. On one hand, the one-time SNU calibration method simplifies the calibration process by redefining the SNU as the sum of shot noise and electronic noise variances [53], which eliminates the need to separately measure electronic noise in practical experiment, thereby enhancing SNU calibration accuracy. In the one-time calibration, the electronic noise and detection efficiency of the practical BHD are both modeled as loss. Notably, the loss attributed to the electronic noise is untrusted since the electronic noise remains uncalibrated. On the other hand, a real-time SNU calibration method utilizes a high-speed and high-ER optical switch comprising two AOMs with 50 dB ER. During measurement, the sum of quantum signal and SNU variances is obtained in the front switch-on period, while the SNU variance is solely measured in the latter switch-off period. This allows for real-time calibration of SNU, considering that two SNUs are approximately equal within *ms* period. Importantly, the SNU should be processed with the same DSP procedure as the MC quantum signal in the experiment.

D. Post-Processing

In the MC CV-QKD experiment, we innovatively design a high-performance post-processing module based on heterogeneous computing scheme. In the post-processing, reverse multi-dimensional reconciliation (MR) is performed prior to parameter estimation (PE) in order to extract the secret key bits from the whole raw keys [43,54]. To enable this, Alice recovers Bob's continuous-variable string before MR from the post-error-corrected bit string shared between them, and then carries out PE with her continuous-variable data and the recovered Bob's continuous-variable data. Based on this approach, the detailed processing routine of the designed high-performance post-processing module is outlined as follows. First, the whole raw data of each subcarrier undergoes reverse multi-dimensional reconciliation (MR) without PE. After the reconciliation, the raw keys of Bob are converted into binary sequences, while the raw keys of Alice are converted into binary sequences with noises. Second, EC is performed using all block sizes of each subcarrier based on multi-edge-type low-density parity check (MET-LDPC) method [55,56]. Six EC matrices $\mathbf{H}$ are correspondingly designed and optimized for experiments at the transmission distances of 5, 10, 25, 50, 75, and 100 km, with respective code rates of 0.33, 0.3, 0.18, 0.07, 0.0325, and 0.02. Successful decoding at Alice's site enables PE and finally triggers PA using the Toeplitz matrix [57,58] to extract the final key bits. The PE results in current block are then used to optimize MR and EC for the next block. If Alice's decoding fails, this set of raw data is all disclosed for updating the estimated channel parameters and the optimization of the subsequent EC.

In the designed post-processing module, a shuffled BP decoding scheme is adopted to reduce the number of iterations and markedly increase the throughput of EC [59]. Moreover, a cycle elimination algorithm is designed to improve the girth of the quasi-cycle MET-LDPC matrix, enabling parallel speed-up on the GPU [59].

Furthermore, a multiple code scheme is chosen to decrease the time of I/O operation [39]. Consequently, a single GPU can effectively achieve a worst-case EC throughput of 279.2 Mbps over typical transmission distances of 5, 10, 25, 50, 75, and 100 km. The EC utilizes six parallel GPUs to practically extract the final secure keys for each subcarrier in real time.

Funding. National Cryptologic Science Fund of China (2025NCSF02052, 2025NCSF02053); National Key Research and Development Program of China (2020YFA0309704); National Natural Science Foundation of China (62471446, 62171418, 62201530, U24B20135, 62301517); Natural Science Foundation of Sichuan Province (2024NSFSC0470, 2024NSFSC0454, 2024JDDQ0008, 2023ZYD0131, 2023JDRC0017, 2022ZDZX0009, 2024ZYD0008, 2025ZNSFSC1473).

Acknowledgment. Author contributions: W.H. and X.B.J. proposed the idea and wrote this manuscript. W.H., Y.T., P.Y.D., P.Y., and B.Y.M. carried out the experimental work. S.Y., H.W., L.J.L., Z.Y.C., and S.A. carried out the excess noise modeling. M.L., Y.J., and L.Y. carried out the post-processing work. S.P., Z.Y.C., L.J.H., and W.M.Z. carried out the theoretical analysis of the protocol. All the authors analyzed and discussed the results and contributed to writing the manuscript.

Disclosures. The authors declare no competing interests.

Data availability. All of the data that support the findings of this study are reported in the main text and Supplement 1. Source data are available from the corresponding authors on reasonable request.

Supplemental document. See Supplement 1 for supporting content.

REFERENCES

1. N. Gisin, G. Ribordy, W. Tittel, *et al.*, "Quantum cryptography," Rev. Mod. Phys. **74**, 145 (2002).
2. S. Pirandola, U. L. Andersen, L. Banchi, *et al.*, "Advances in quantum cryptography," Adv. Opt. Photonics **12**, 1012–1236 (2020).
3. F. H. Xu, X. F. Ma, Q. Zhang, *et al.*, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
4. Y. C. Zhang, Y. M. Bian, Z. Y. Li, *et al.*, "Continuous-variable quantum key distribution system: past, present, and future," Appl. Phys. Rev. **11**, 011318 (2024).
5. C. Weedbrook, S. Pirandola, R. García-Patrón, *et al.*, "Gaussian quantum information," Rev. Mod. Phys. **84**, 621–669 (2012).
6. S. L. Braunstein and P. Van Loock, "Quantum information with continuous variables," Rev. Mod. Phys. **77**, 513 (2005).
7. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
8. F. Grosshans, G. V. Assche, J. Wenger, *et al.*, "Quantum key distribution using Gaussian-modulated coherent states," Nature **421**, 238–241 (2003).
9. C. Weedbrook, A. M. Lance, W. P. Bowen, *et al.*, "Quantum cryptography without switching," Phys. Rev. Lett. **93**, 170504 (2004).
10. X. L. Su, W. Z. Wang, Y. Wang, *et al.*, "Continuous variable quantum key distribution based on optical entangled states without signal modulation," Europhys. Lett. **87**, 20005 (2009).
11. F. Furrer, T. Franz, M. Berta, *et al.*, "Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks," Phys. Rev. Lett. **109**, 100502 (2012).
12. A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," Phys. Rev. Lett. **114**, 070501 (2015).
13. A. Leverrier, "Security of Continuous-variable quantum key distribution via a Gaussian de Finetti reduction," Phys. Rev. Lett. **118**, 200501 (2017).
14. T. Matsuura, K. Maeda, T. Sasaki, *et al.*, "Finite-size security of continuous-variable quantum key distribution with digital signal processing," Nat. Commun. **12**, 252 (2021).
15. Z. Y. Chen, X. Y. Wang, S. Yu, *et al.*, "Continuous-mode quantum key distribution with digital signal processing," NPJ Quantum Inform. **9**, 28 (2023).
16. S. Pirandola, "Limits and security of free-space quantum communications," Phys. Rev. Res. **3**, 013279 (2021).
17. S. Pirandola, "Composable security for continuous variable quantum key distribution: trust levels and practical key rates in wired and wireless networks," Phys. Rev. Res. **3**, 043014 (2021).
18. S. Y. Ren, Y. Wang, and X. L. Su, "Hybrid quantum key distribution network," Sci. China Inf. Sci. **65**, 200502 (2022).
19. G. Zhang, J. Y. Haw, H. Cai, *et al.*, "An integrated silicon photonic chip platform for continuous variable quantum key distribution," Nat. Photon. **13**, 839–842 (2019).
20. L. Li, T. Wang, X. H. Li, *et al.*, "Continuous-variable quantum key distribution with on-chip light sources," Photonics Res. **11**, 504–516 (2023).
21. P. Jouguet, S. Kunz-Jacques, A. Leverrier, *et al.*, "Experimental demonstration of long-distance continuous-variable quantum key distribution," Nat. Photonics **7**, 378–381 (2013).
22. Y. C. Zhang, Z. Y. Chen, S. Pirandola, *et al.*, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Phys. Rev. Lett. **125**, 010502 (2020).
23. Y. Pan, H. Wang, Y. Shao, *et al.*, "Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system," Opt. Lett. **47**, 3307–3310 (2022).
24. Y. Tian, P. Wang, J. Q. Liu, *et al.*, "Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber," Optica **9**, 492–500 (2022).
25. Y. C. Zhang, Z. Y. Li, Z. Y. Chen, *et al.*, "Continuous-variable QKD over 50 km commercial fiber," Quantum Sci. Technol. **4**, 035006 (2019).
26. H. Wang, Y. Li, Y. D. Pi, *et al.*, "Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area," Commun. Phys. **5**, 162 (2022).
27. Y. Tian, Y. Zhang, S. S. Liu, *et al.*, "High-performance long-distance discrete-modulation continuous-variable quantum key distribution," Opt. Lett. **48**, 2953–2956 (2023).
28. Y. D. Pi, H. Wang, Y. Pan, *et al.*, "Sub-Mbps key-rate continuous-variable quantum key distribution with local oscillator over 100-km fiber," Opt. Lett. **48**, 1766–1769 (2023).
29. T. Wang, P. Huang, L. Li, *et al.*, "High key rate continuous-variable quantum key distribution using telecom optical components," New J. Phys. **26**, 023002 (2024).
30. F. Roumestan, A. Ghazisaeidi, J. Renaudier, *et al.*, "Shaped constellation continuous variable quantum key distribution: concepts, methods and experimental validation," J. Lightwave Technol. **42**, 5182–5189 (2024).
31. A. Hajomer, C. Bruynsteen, I. Derkach, *et al.*, "Continuous-variable quantum key distribution at 10 GBaud using an integrated photonic-electronic receiver," Optica **11**, 1197–1204 (2024).
32. A. Hajomer, I. Derkach, N. Jain, *et al.*, "Long-distance continuous-variable quantum key distribution over 100-km fiber with local oscillator," Sci. Adv. **10**, eadi9474 (2024).
33. N. Jain, H. M. Chin, H. Mani, *et al.*, "Practical continuous-variable quantum key distribution with composable security," Nat. Commun. **13**, 4740 (2022).
34. W. Li, L. K. Zhang, H. Tan, *et al.*, "High-rate quantum key distribution exceeding 110 Mbs-1," Nat. Photon. **17**, 416–421 (2023).
35. F. Laudenbach, C. Pacher, C. F. Fung, *et al.*, "Continuous-variable quantum key distribution with Gaussian modulation—the theory of practical implementations," Adv. Quantum Technol. **1**, 1800011 (2018).
36. F. Kiselev, E. Samsonov, R. Goncharov, *et al.*, "Analysis of the chromatic dispersion effect on the subcarrier wave QKD system," Opt. Exp. **28**, 28696–28712 (2020).
37. A. Weerasinghe, M. Alhussein, A. Alderton, *et al.*, "Practical, high-speed Gaussian coherent state continuous variable quantum key distribution with real-time parameter monitoring, optimized slicing, and post-processed key distillation," Sci. Rep. **13**, 21543 (2023).
38. Y. Li, X. F. Zhang, Y. Li, *et al.*, "High-throughput GPU layered decoder of multi-edge type low density parity check codes in continuous-variable quantum key distribution systems," Sci. Rep. **10**, 14561 (2020).
39. H. Z. Yang, S. S. Liu, S. S. Yang, *et al.*, "High-efficiency rate-adaptive reconciliation in continuous-variable quantum key distribution," Phys. Rev. A **109**, 012604 (2024).
40. S. S. Yang, Z. G. Lu, and Y. M. Li, "High-speed post-processing in continuous-variable quantum key distribution based on FPGA implementation," J. Lightwave Technol. **38**, 3935–3941 (2020).
41. C. Zhou, Y. Li, L. Ma, *et al.*, "Integrated high-performance error correction for continuous-variable quantum key distribution," arXiv (2024).
42. T. A. Eriksson, R. S. Luís, B. J. Puttnam, *et al.*, "Wavelength division multiplexing of 194 continuous variable quantum key distribution channels," J. Lightwave Technol. **38**, 2214–2218 (2020).

43. X. Y. Wang, Y. C. Zhang, Z. Y. Li, *et al.*, "Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution," Quantum Inf. Comput. **17**, 1123–1134 (2017).
44. S. Pirandola and P. Papanastasiou, "Improved composable key rates for CV-QKD," Phys. Rev. Res. **6**, 023321 (2024).
45. M. Tomamichel, C. Schaffner, A. Smith, *et al.*, "Leftover hashing against quantum side information," IEEE T. Inform. Theory **57**, 5524–5535 (2011).
46. M. Tomamichel, "A framework for non-asymptotic quantum information theory," Ph.D. thesis, Zurich (2005).
47. A. A. E. Hajomer, N. Jain, H. Mani, *et al.*, "Modulation leakage-free continuous-variable quantum key distribution," npj Quantum Inform. **8**, 136 (2022).
48. L. Ma, J. Yang, T. Zhang, *et al.*, "Practical continuous-variable quantum key distribution with feasible optimization parameters," Sci. China Inf. Sci. **66**, 180507 (2023).
49. H. Wang, Y. Pan, Y. Shao, *et al.*, "Performance analysis for OFDM-based multi-carrier continuous-variable quantum key distribution with an arbitrary modulation protocol," Opt. Exp. **31**, 5577–5592 (2023).
50. P. Jouguet, S. Kunz-Jacques, E. Diamanti, *et al.*, "Analysis of imperfections in practical continuous-variable quantum key distribution," Phys. Rev. A **86**, 032309 (2012).
51. S. Wu, P. Liu, and Y. Bar-Ness, "Phase noise estimation and mitigation for OFDM systems," IEEE T. Wirel. Commun. **5**, 3616–3625 (2006).
52. B. Qi, P. Lougovski, R. Pooser, *et al.*, "Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection," Phys. Rev. X **5**, 041009 (2015).
53. Y. C. Zhang, Y. D. Huang, Z. Y. Chen, *et al.*, "One-time shot-noise unit calibration method for continuous-variable quantum key distribution," Phys. Rev. Appl. **13**, 024058 (2020).
54. X. Y. Wang, Y. C. Zhang, S. Yu, *et al.*, "High efficiency postprocessing for continuous-variable quantum key distribution: using all raw keys for parameter estimation and key extraction," Quantum Inf. Process. **18**, 1–14 (2019).
55. T. Member and I. R. Urbanke, *Multi-edge Type LDPC Codes. Presented at Workshop Honoring Prof. Bob McEliece on his 60th Birthday* (California Institute of Technology, 2002), pp. 24–25.
56. T. Richardson and R. Urbanke, *Modern Coding Theory* (Cambridge University Press, 2008), Chap. 7.
57. Y. J. Luo, Y. Li, J. Yang, *et al.*, "High-speed implementation of privacy amplification for continuous-variable quantum key distribution," Proc. SPIE **11558**, 25–33 (2020).
58. X. Y. Wang, Y. C. Zhang, S. Yu, *et al.*, "High-speed implementation of length-compatible privacy amplification in continuous-variable quantum key distribution," Photonics J. **10**, 7600309 (2018).
59. Y. Li, B. J. Xu, L. Ma, *et al.*, "High-throughput error correction for continuous-variable quantum key distribution on shuffled iterative decoding," Proc. SPIE **11558**, 77–82 (2020).