PHOTONICS Research

Experimental demonstration of phase-sensitive multimode continuous variable quantum key distribution with improved secure key rate

Zikang Su,[1,†] Jintao Wang,[1,†] Dajian Cai,[1] Xiaojie Guo,[2,4] Dawei Wang,[1,3,*] and Zhaohui Li[1,3,5]

[1]Guangdong Provincial Key Laboratory of Optoelectronic Information Processing Chips and Systems, School of Electronics and Information Technology, Sun Yat-sen University, Guangzhou 510006, China
[2]Guangdong Provincial Key Laboratory of Optical Fiber Sensing and Communications, Institute of Photonics Technology, Jinan University, Guangzhou 510632, China
[3]Southern Marine Science and Engineering Guangdong Laboratory (Zhuhai), Zhuhai 519000, China
[4]e-mail: xjguo@jnu.edu.cn
[5]e-mail: lzh88@mail.sysu.edu.cn
[†]These authors contributed equally to this paper.
*Corresponding author: wangdw9@mail.sysu.edu.cn

Received 16 January 2023; revised 14 August 2023; accepted 4 September 2023; posted 5 September 2023 (Doc. ID 485654); published 16 October 2023

We develop and experimentally demonstrate a phase-sensitive continuous variable quantum key distribution system with improved secure key rate. This is achieved using multimode coherent states with phase-conjugated subcarrier modulation and phase-sensitive detection. The local oscillator for phase-sensitive detection is regenerated from a polarization-multiplexed carrier wave via optical injection locking. The proposed scheme has a higher classical information capacity at a given number of received photons and exhibits a higher secure key rate when applying the security analysis of the GG02 protocol. Experimental results confirm the higher secret key rate and better excess noise tolerance of the new scheme compared to the typical implementation of GG02.

https://doi.org/10.1364/PRJ.485654

1. INTRODUCTION

Quantum key distribution (QKD), one of the most active areas in quantum information [1], allows remote legitimate parties to share encryption keys in the quantum secure network [2]. QKD is designed based on the laws of quantum mechanics and thus offers prestigious security against quantum code breaking. In contrast to the discrete-variable (DV) QKD with dedicated single-photon detectors [3], the continuous-variable (CV) QKD relies on optical coherent detection to gain information encoded in the electromagnetic field quadratures of coherent states [4]. In other words, single-photon detection can be replaced by more conventional detection methods. Hence, CVQKD demonstrates better compatibility with commercially available telecom components and provides higher key distribution rates in metropolitan areas, which is well suited for large-scale, cost-effective deployment. Its security has been thoroughly studied with consideration of realistic devices [5]. Emerging protocols, such as discrete modulation CVQKD with quadrature phase shift keying [6], keep pushing the CVQKD frontier toward high tolerance to excess noise and long transmission distance. The prominent and well-studied protocol of CVQKD is undoubtedly the GG02 [7], which utilizes Gaussian-modulated coherent states as quantum objects to deliver the raw key. With quantum channel transmission and shot noise-limited coherent detection of the coherent states, the secure key can be subsequently extracted via a series of post-processing procedures.

The GG02 protocol possesses the most developed security proofs, which have established information-theoretic security against collective attacks [8] and coherent attacks [9]. Like the other types of CV protocols, the amount of the distillable secure information depends on the difference between the two legal parties' (Alice and Bob) mutual information and the eavesdropper's (Eve) potential information about Bob (assuming reverse reconciliation). The mutual information of Alice and Bob is usually upper-bounded by the channel capacity of the Shannon limit in the homodyne or heterodyne detection schemes; whereas Eve's potential information is related to the type of eavesdropping attacks and system architecture, including the detection mode, the reconciliation direction, and the finite block sizes [1]. Here, we consider the asymptotic secure key rate (SKR) R with reverse reconciliation in the case of collective attacks, namely,

$$R = \beta I_{AB} - \chi_{EB}, \tag{1}$$

where β is the reconciliation efficiency, I_{AB} is Alice and Bob's mutual information, and χ_{EB} is the Holevo information between Eve and Bob. Typical ways to improve the secure key rate or to reach a longer transmission distance include using an error correction code with high efficiency (i.e., a larger β) [10] and controlling the system excess noise for a lower χ_{EB} [11].

Developing novel CVQKD systems mainly focuses on alternative state preparation and measurement schemes. For example, the subcarrier wave (SCW) CVQKD using a modulated multimode state is proposed in Refs. [12,13]. The quantum state is prepared by modulating the monochromatic light via an electro-optic phase modulator to produce weak sidebands without suppressing the central carrier. The carrier wave acts as the local oscillator (LO) at the receiver side for coherent detection of the sidebands [14]. This scheme provides an alternative GG02 implementation with an LO transmitting through a quantum channel, thus still suffering from LO intensity bottleneck and LO-signal cross talk. Also, the sharp spectral filtering needed to separate the LO at the receiver end may pose a technical challenge. Another implementation uses a carrier-suppressed sideband signal modulation and a discrete frequency component as the pilot tone for synchronizing a local LO [15]. The subcarrier-modulated signal can be down-converted to an intermediate frequency (IF) stage by heterodyne detection with one balanced photodetector (BPD) and be recovered through subsequent signal processing in the digital domain.

This paper proposes a multimode implementation of GG02 CVQKD utilizing the digital phase-conjugated subcarrier (PCS) modulation and phase-sensitive heterodyne detection. The proposed scheme is experimentally demonstrated using only one quadrature for signal modulation and detection. We show that the phase-sensitive detection of PCS exhibits a higher information capacity than ordinary GG02 prepare-and-measure schemes at the cost of lower spectral efficiency. We develop the theoretical information capacity of the proposed scheme and experimentally achieve a higher SKR than the conventional GG02. The PCS uses the same phase-conjugated first-order subcarriers as the SCW scheme [12,13]. However, the PCS ensures maximum modulation efficiency with complete carrier suppression. At the same time, a weak reference signal transmits on an orthogonal polarization for LO regeneration based on optical injection locking (OIL) [16]. Despite the implementation differences between the two schemes, the security analysis developed for SCW also applies to PCS, because they both use symmetric modes carrying the same information without interaction and thus act as two separate GG02 channels. The complete experimental demonstration and detailed information capacity analysis performed in this paper have not been seen in previous studies. Moreover, the phase-sensitive multimode preparation and measurement developed in this work are expected to find applications in scientific areas such as phase-sensitive amplification [17] and phase-sensitive quantum storage [18]. The PCS can also be employed as a multiplexing technique for the multichannel CVQKD system [19,20].

2. OPERATION PRINCIPLE

A semi-classic approach is sufficient to describe the operation principle of PCS and compare it to other schemes. Consider a narrowband, linearly polarized optical signal with randomly distributed complex field amplitude α. Like the GG02, we consider the distribution of α to be zero-mean Gaussian. The variance, $\bar{n} = E\{|\alpha|^2\}$, has the interpretation of the mean photon number of the signal, and it is also called the modulation variance, denoted by V_{mod}. Propagation through a standard additive white Gaussian noise (AWGN) channel is modeled by the transformation $\alpha \to \alpha' = \sqrt{\tau}\alpha + \xi$, where the transmittance τ specifies the change of the optical signal power, and ξ is a complex-valued zero-mean Gaussian random variable that characterizes the excess noise. The mean photon numbers of both the received signal, denoted as $n_s = \tau\bar{n}$, and the excess noise, $n_{\text{ex}} = E\{|\xi|^2\}$, are the same for all schemes discussed below. We also consider the detectors to have ideal quantum efficiencies and operate at the shot noise-limited level. We define the shot noise unit (SNU $\equiv 1/2$) as a zero-mean complex-valued noise with variance corresponding to the vacuum state. Hence, the received signal has a total variance of $V = \tau\bar{n} + 1/2 + n_{\text{ex}} = n_s + 1/2 + n_{\text{ex}}$.

Consider first the scheme where both quadrature components of the optical signal are carrying information and measured simultaneously (denoted as 2Q2D). The so-called "no-switching" protocol is one example [21]. Denote the complex amplitude of the received signal by $\sqrt{\tau}\alpha = x + ip$, and the mean photon number of each quadrature is thus $E\{x^2\} = E\{p^2\} = n_s/2$. As illustrated in Fig. 1(a), using a phase-diversity homodyne receiver with a 3-dB coupler, half of the input power is directed to each of the two homodyne detectors for quadrature measurement. Therefore, the mean photon number of one signal quadrature is $S_{\text{2Q2D}} = n_s/4$. For the same reason, the mean photon number of one noise quadrature is $N_{\text{2Q2D}} = n_{\text{ex}}/4 + 1/4$, where the 1/4 denotes one quadrature of vacuum noise. Thus, we can express the signal-to-noise ratio (SNR) of the 2Q2D scheme as

$$\text{SNR}_{\text{2Q2D}} = \frac{n_s/4}{n_{\text{ex}}/4 + 1/4} = \frac{n_s}{n_{\text{ex}} + 1}. \tag{2}$$

In contrast, the CVQKD protocol that uses two quadratures to carry information but measures only one quadrature at a time by randomly switching the LO phase between 0 and $\pi/2$ is illustrated in Fig. 1(b) (denoted as 2Q1D). With the absence of the input 3 dB loss, the mean photon number of the selected signal quadrature is thus $S_{\text{2Q1D}} = n_s/2$, and the noise quadrature is $N_{\text{2Q1D}} = n_{\text{ex}}/2 + 1/4$. The SNR of 2Q1D is

$$\text{SNR}_{\text{2Q1D}} = \frac{n_s/2}{n_{\text{ex}}/2 + 1/4} = \frac{2n_s}{2n_{\text{ex}} + 1}. \tag{3}$$

Moreover, the unidimensional protocol [22] uses only one quadrature at both the transmitter and the receiver (denoted as 1Q1D), shown as Fig. 1(c). Since all information is encoded in one quadrature, we assign the mean photon number of the received signal as $S_{\text{1Q1D}} = \tau E\{\alpha^2\} = n_s$, where α is real-valued.

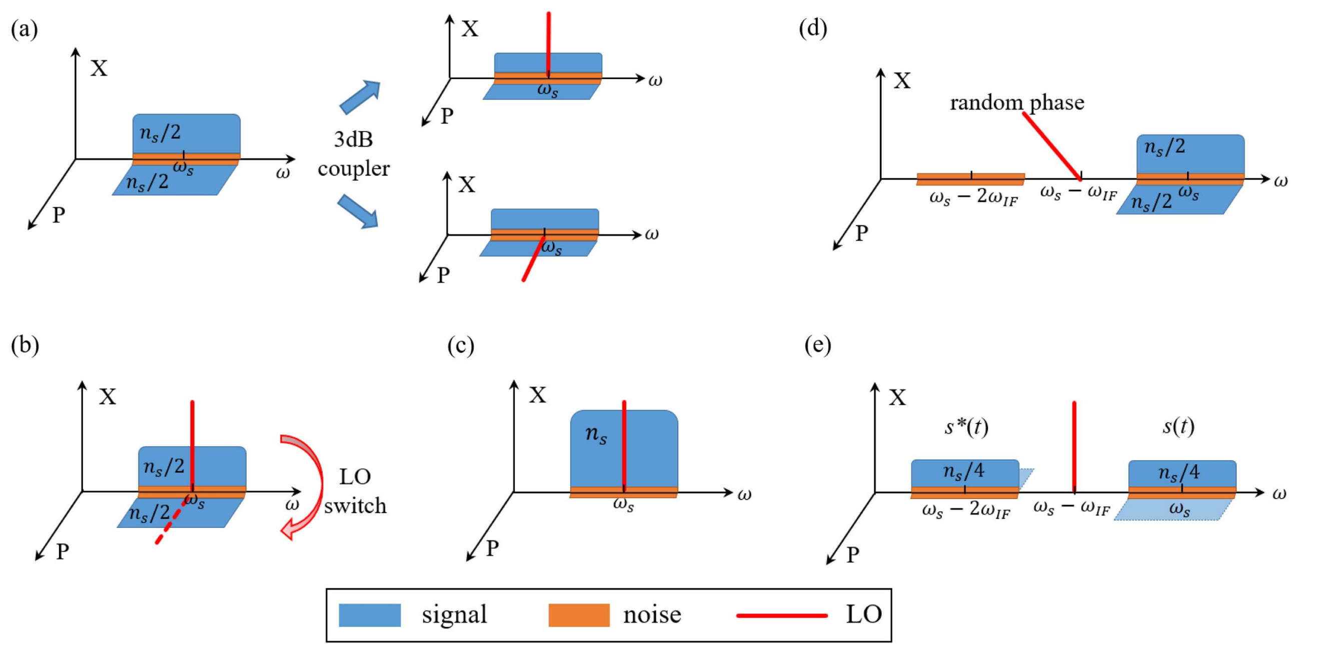

Fig. 1. Optical spectra of different detection schemes with quadrature components representation. (a) Two-quadrature encoding with phase-diversity homodyne detection (2Q2D); (b) two-quadrature encoding with LO phase switching (2Q1D), showing a $\pi/2$ phase difference between the solid LO and the dashed LO; (c) single-quadrature encoding with LO phase-locked to the signal (1Q1D); (d) two-quadrature encoding with heterodyne detection at IF stage (sub-2Q2D); (e) phase-conjugated subcarrier encoding with phase-sensitive heterodyne detection (PCS).

The excess noise is, however, still complex. Hence, the SNR of the 1Q1D scenario is

$$\mathrm{SNR}_{\mathrm{1Q1D}} = \frac{n_s}{n_{\mathrm{ex}}/2 + 1/4} = \frac{4n_s}{2n_{\mathrm{ex}} + 1}. \tag{4}$$

In contrast to the schemes discussed above, the subcarrier CVQKD schemes exhibit intermediate frequencies, ω_{IF}, in the coherently detected signals. They can be implemented via subcarrier modulation at the transmitter and/or heterodyne detection at the receiver with one balanced photodetector. The quantum theory of optical heterodyne detection relies on image band vacuum mode [23–25]. Denote the center frequency of the signal band as ω_s. The LO will be outside the signal band and has the frequency $\omega_{\mathrm{LO}} = \omega_s - \omega_{\mathrm{IF}}$. The scheme is identified as sub-2Q2D and is illustrated in Fig. 1(d). The signal that is optically downconverted to the IF preserves all information of both quadratures and can be recovered via subsequent electrical processing. During the optical downconversion, the signal is superimposed with the image band at $\omega_s - 2\omega_{\mathrm{IF}}$, which doubles the shot noise power. The mean photon number in each quadrature of signal and excess noise detected by the free-running LO will be $n_s/2$ and $n_{\mathrm{ex}}/2$, respectively. The SNR of sub-2Q2D turns out to be the same as the 2Q2D,

$$\mathrm{SNR}_{\text{sub-2Q2D}} = \frac{n_s/2}{n_{\mathrm{ex}}/2 + 1/2} = \frac{n_s}{n_{\mathrm{ex}} + 1}. \tag{5}$$

A traditional heterodyne detector is a phase-insensitive device that suffers a 3 dB noise penalty caused by the extra quantum noise in the image sideband vacuum mode, which contributes nothing to the signal. However, suppose the image sideband vacuum mode is also excited to a coherent state at the same level as the signal mode, but with a conjugated phase. In that case, the 3 dB noise penalty can be eliminated [26,27]. This, however, requires phase-sensitive detection, where the phase of LO should be locked to the combined signal $s(t) + s^*(t)$. As shown in Fig. 1(e), two phase-conjugated signal bands are modulated at the subcarrier frequency $\omega_{\mathrm{LO}} \pm \omega_{\mathrm{IF}}$. After the phase-sensitive detection, the mean photon number of signal and noise will be $S_{\mathrm{PCS}} = n_s$ and $N_{\mathrm{PCS}} = n_{\mathrm{ex}} + 1/2$, respectively. The twofold increase in n_s and n_{ex} relative to the ordinary sub-2Q2D is due to the coherent signal and image band superposition. The SNR of the PCS scheme is therefore

$$\mathrm{SNR}_{\mathrm{PCS}} = \frac{n_s}{n_{\mathrm{ex}} + 1/2} = \frac{2n_s}{2n_{\mathrm{ex}} + 1}. \tag{6}$$

The classical information capacity (Shannon capacity) of an analog communication channel with power constraint is expressed as $C = (\mu/2)\log_2(1 + \mathrm{SNR})$, where $\mu = 1$ or 2 corresponds to using one or two quadratures for information extraction. The expressions of Shannon capacity of the CVQKD schemes discussed above are summarized in Table 1. The Holevo bound for the AWGN channel is also listed [28] with the entropy function,

$$g(v) = (v + 1)\log_2(v + 1) - v\log_2 v. \tag{7}$$

The channel capacities as functions of the received signal photon number n_s are plotted in Fig. 2 for the loss-only case, i.e., $n_{\mathrm{ex}} = 0$. The PCS scheme with phase-sensitive detection offers the highest capacity that is closest to the Holevo bound for all n_s, at the cost of using twice the usable bandwidth. It is easy to verify that increasing the number of modes, i.e., using

Table 1. AWGN Channel Capacities of Various CVQKD Schemes and the Holevo Bound

CVQKD Scheme	AWGN Channel Capacity
1Q1D	$C = \frac{1}{2}\log_2(1 + \frac{4n_s}{2n_{\mathrm{ex}}+1})$
(sub-)2Q2D	$C = \log_2(1 + \frac{n_s}{n_{\mathrm{ex}}+1})$
2Q1D	$C = \frac{1}{2}\log_2(1 + \frac{2n_s}{2n_{\mathrm{ex}}+1})$
PCS	$C = \log_2(1 + \frac{2n_s}{2n_{\mathrm{ex}}+1})$
Holevo	$C = g(n_s + n_{\mathrm{ex}}) - g(n_{\mathrm{ex}})$

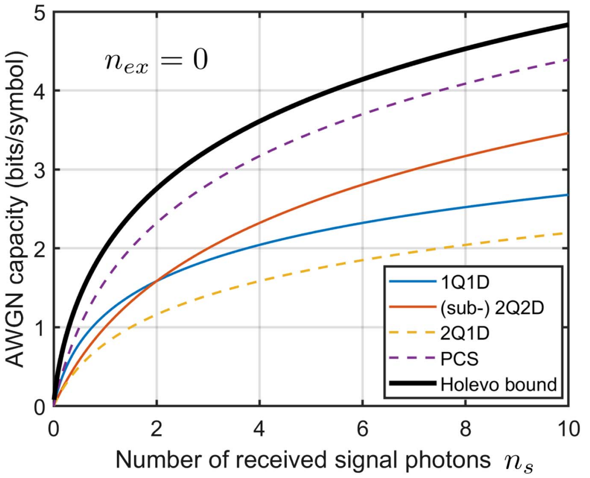

Fig. 2. Loss-only ($n_{\mathrm{ex}} = 0$) AWGN capacities for different CVQKD schemes as functions of received signal photon numbers (n_s). The PCS scheme with phase-sensitive detection offers the highest classic capacity closest to the Holevo bound.

more pairs of phase-conjugates subcarriers, each carrying the same information, does not further increase the capacity.

3. SECURITY ANALYSIS

Note that comprehensive unconditional security proof of the PCS scheme requires dedicated efforts and is outside the scope of this paper. We thus follow the previous study [13] to acknowledge that the state prepared by PCS is the modulator-generated multimode state written as the tensor product over the two symmetric modes around the carrier frequency without mode intersections. Namely, Alice prepares and sends

$$|\Psi\rangle = |\alpha_A e^{-i\omega_{\mathrm{IF}} t}\rangle \otimes |\alpha_A^* e^{i\omega_{\mathrm{IF}} t}\rangle, \tag{8}$$

where $\alpha_A = x_A + ip_A$. Thus, the two sidebands are separate quantum channels carrying the same information. Upon the phase-sensitive detection, Bob retrieves data $\{x_B, p_B\}$ correlated with $\{x_A, p_A\}$ prepared by Alice by using superposition of sidebands. Then, Bob constructs a single covariance matrix,

$$\gamma_{AB} = \begin{bmatrix} V_A I_2 & \sqrt{\tau} V_A I_2 \\ \sqrt{\tau} V_A I_2 & (\tau V_A + V_{\mathrm{ex}} + 1) I_2 \end{bmatrix}, \tag{9}$$

to estimate the mutual information with Alice, where I_2 is a 2×2 identity matrix and $V_A = 2V_{\mathrm{mod}}$ and $V_{\mathrm{ex}} = 2n_{\mathrm{ex}}$ are the SNU (≡1/2) normalized variances. It follows that the correlation coefficient between x_A and x_B can be obtained from γ_{AB} as

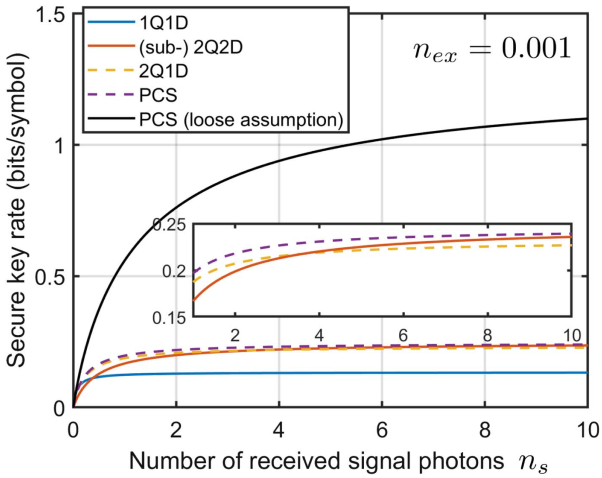

Fig. 3. Simulated secure key rate of the PCS scheme, with and without the loose assumption, and other typical GG02 schemes as functions of received signal photon numbers (n_s). We consider transmittance $\tau = 0.3$, $n_{\mathrm{ex}} = 0.001$, $\beta = 1$, and perfect detectors. We use $V_A = n_s$ and $V_{\mathrm{ex}} = n_{\mathrm{ex}}$ for the loose assumption and $V_A = 2n_s$ and $V_{\mathrm{ex}} = 2n_{\mathrm{ex}}$ otherwise.

$$\rho = \frac{\sqrt{\tau} V_A}{\sqrt{V_A}\sqrt{\tau V_A + V_{\mathrm{ex}} + 1}}, \tag{10}$$

and the mutual information is given by

$$I_{AB} = -\log_2(1 - \rho^2). \tag{11}$$

Using the same procedure of GG02, Bob estimates the Holevo information χ_{EB} based on calculating symplectic eigenvalues $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ of Eve's covariance matrices [29],

$$\chi_{EB} = g\left(\frac{\lambda_1 - 1}{2}\right) + g\left(\frac{\lambda_2 - 1}{2}\right) - g\left(\frac{\lambda_3 - 1}{2}\right) - g\left(\frac{\lambda_4 - 1}{2}\right). \tag{12}$$

We distinguish two scenarios where in one case, Bob makes a crude assumption that Eve cannot perform the perfect phase-sensitive detection without the seed light (PCS with loose assumption). Hence, the values $V_A = n_s$ and $V_{\mathrm{ex}} = n_{\mathrm{ex}}$ are used for Holevo information calculation. Without this assumption, those values are $V_A = 2n_s$ and $V_{\mathrm{ex}} = 2n_{\mathrm{ex}}$. The secure key rate simulation results are shown in Fig. 3 with transmittance $\tau = 0.3$, $n_{\mathrm{ex}} = 0.001$, $\beta = 1$, and perfect detectors. The PCS scheme achieves a slightly higher key rate than the standard 2Q2D implementation of GG02. The improvement is more significant if we apply the loose assumption.

A potential way to enhance the PCS scheme and eliminate the loose assumption is to prepare and transmit two pairs of phase-conjugated subcarriers on the primary carrier's two quadratures with independent data encoded. Bob decides randomly to measure one of the data with phase-sensitive detection. This will require an additional sifting stage in the key distillation process and increase implementation complexity, but it will further reduce the eavesdropper's information, while leaving I_{AB} unchanged.

4. EXPERIMENTAL IMPLEMENTATION

We generate the phase-conjugated signal bands with subcarrier modulation by the arbitrary waveform generator (AWG) to implement the PCS quantum state encoding. The resulting signal in the equivalent baseband form is expressed as

$$q(t) = s(t)e^{-i\omega_{\mathrm{IF}}t} + s^*(t)e^{i\omega_{\mathrm{IF}}t}, \tag{13}$$

where $s(t)$ is the complex-valued Gaussian-modulated baseband signal as described in standard GG02 protocol, $s^*(t)$ is the conjugate version of $s(t)$, and ω_{IF} is the intermediate frequency. Then the signal is upconverted to the optical frequency via an optical modulator. The primary experimental setup used for system implementation and performance verification of the PCS protocol is depicted in Fig. 4. Alice adopts a software-defined transmitter for signal modulation with a polarization multiplexed carrier wave. Two branches of the polarized light are generated from the output of a 1550 nm continuous wave (CW) commercial fiber laser (NKT BasiK X15) with a linewidth of 100 Hz divided by a 50/50 polarization-maintaining beam splitter (BS). One branch of polarized light is fed to a single-polarization IQ modulator (iXblue MXIQER-LN-30) to carry the electrical modulation signal generated by a 12-bit 12 GS/s AWG (Keysight M8190A). The electrical modulation signal is fully synthesized in the digital domain by digital signal processing (DSP) and digital-to-analog converters (DACs). An IQ modulator comprises two Mach-Zehnder modulators (MZMs) with a relative phase shift 90° corresponding to the in-phase and quadrature components. One of the MZMs, taken for concreteness to be the in-phase one, is used to generate the digital PCS signal, which contains the frequency-multiplexed Gaussian-modulated quantum signal and pilot-tone centered at frequency $f_{\mathrm{QU}} = 50$ MHz and $f_{\mathrm{PT}} = 100$ MHz, respectively (denoted as the quantum-signal polarization). The pilot is for the phase correction at Bob's site. However, it should be noted that the pilot is optional, since Bob owns a phase-locked LO due to OIL [16]. The Gaussian-modulated signal has a bandwidth of 20 MHz, and the power of the pilot-tone is 10 dB higher than the average power of the quantum signal. The other MZM (the quadrature one) is modulated by a sinusoidal signal with frequency $f_{\mathrm{PID}} =$ 125 kHz, which serves as the reference signal for the proportional-integral-differential (PID) phase locking at the detection stage. The other branch of the CW laser serves as the carrier wave for the OIL process at Bob's site (denoted as the carrier-wave polarization). The optical power of carrier-wave polarization is set to −50 dBm by the variable optical attenuators VOA1 and VOA2. The power of quantum-signal polarization is adjusted and stabilized by a power controller with the monitoring function at a relatively higher power level. Then the two branches are polarization multiplexed via a polarization beam combiner (PBC) before the VOA2 is set to a fixed 30 dB attenuation. Then, the combined signal is launched to the quantum channel of a 20 km standard single-mode fiber (SSMF) with a loss coefficient of 0.2 dB/km.

The phase-sensitive heterodyne detection is implemented at Bob's site with the help of the close phase relation between the quantum-signal polarization and carrier-wave polarization in polarization multiplexing transmission. The output of the fiber link is demultiplexed by a polarization beam splitter (PBS) placed after a polarization controller (PC) that is used to maximize the power of the carrier-wave polarization. The OIL module takes the isolated carrier wave as the seed light to regenerate an LO with 2.7 dBm optical power. The detailed setup of the OIL module with an electrical phase-locked loop (PLL) is shown in Fig. 4(b), the operating principle of which is described in Ref. [16]. After polarization demultiplexing, the quantum signal is mixed with the LO via a 50/50 coupler before being received by a commercially available BPD. The adopted BPD is engineered particularly to separate the lower frequency components (DC-400 kHz) with a monitor port. The reference signal at 125 kHz is detected from the monitor port, which is connected to a high-speed servo controller consisting of a lock-in amplifier and a PID controller. The servo controller drives the piezoelectric fiber stretchers (PZFSs) placed on the LO path for compensating the slow phase changing between the signal path and the LO path. The PLL is designed to lock the amplitude of the reference signal to the minimum point so that the quantum signal retains the maximum because of the orthogonal relation. Note that the reference signal can be combined with PCS modulation using only one MZM to simplify the setup, provided the PLL can be modified to lock the maximum instead. Afterward, the phase-sensitive detected signal output from the BPD is digitized by a 10-bit digital storage oscilloscope (DSO, Keysight DSOS404A) with a sampling rate of 1 GS/s, followed by

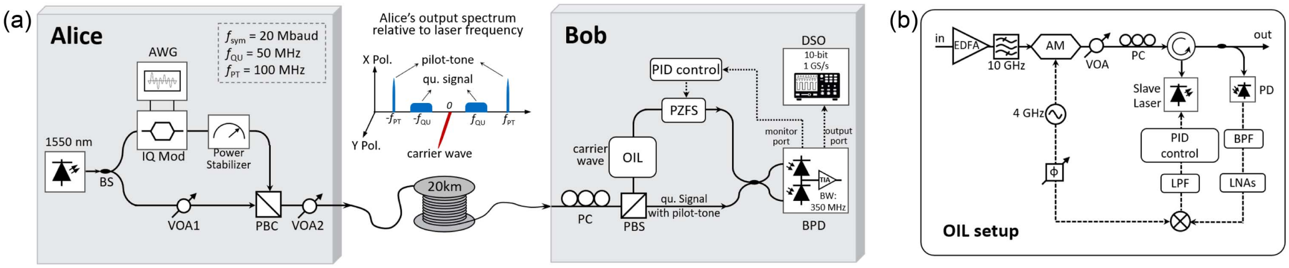

Fig. 4. Experimental setups. (a) Block diagram of the CVQKD system with phase-conjugated subcarrier modulation and the phase-sensitive heterodyne detector; (b) OIL setup with an electrical phase-locked loop (PLL). AM, amplitude modulator; BPF, bandpass filter; BS, beam splitter; EDFA, erbium-doped fiber amplifier; LNA, low-noise amplifier; LPF, lowpass filter; PD, photodetector; PBC, polarization beam combiner; PBS, polarization beam splitter; PC, polarization controller; PID, proportional-integral-differential; PZFS, piezoelectric fiber stretcher.

the offline DSP to prepare the data for raw key rate calculation. The DSP consists of downconverting the quantum signal to the baseband, matched filtering, phase correction, and downsampling. An electrical connection between the AWG and the DSO is used for clock synchronization to avoid additional penalties from the otherwise required digital clock recovery algorithm.

To experimentally evaluate the information capacity of the proposed PCS scheme, a series of received signals with different numbers of received photons are collected by setting different modulation variance V_{mod} by the power stabilizer at the transmitter. With the equivalence between the 2Q2D and the sub-2Q2D, we compare the proposed PCS scheme against the sub-2Q2D, which is relatively easy to implement in our current setup. The mutual information is calculated from the correlation coefficient between the received signals and the original transmitted signal, cf. Eq. (11). We calculate based on SNR defined by correlation coefficient instead of the pessimistic estimate method in typical postprocessing to determine the number of the received signal photons and excess noise photons. The received SNR can be written as

$$\mathrm{SNR} = \frac{\rho^2}{1-\rho^2} = \frac{n_s}{n_{\mathrm{sn}} + n_{\mathrm{el}} + n_{\mathrm{ex}}}, \tag{14}$$

where n_s is the photon number of the received signal, n_{sn} is the photon number of SNU, n_{el} is the photon number of the detector's electric noise, and n_{ex} is the photon number of excess noise, all of which constitute the total photon number of the received signal, namely,

$$n_s + n_{\mathrm{sn}} + n_{\mathrm{el}} + n_{\mathrm{ex}} = n_{\mathrm{tol}}. \tag{15}$$

By calculating the SNR with correlation coefficient and calibrating the SNU and the detector's electric noise, we can determine the photons number of the received signal and excess noise through Eqs. (14) and (15). Considering a realistic detector with electric noise and limited quantum efficiency, the information capacity formula should be modified to

$$C = \log_2\left(1 + \frac{2\eta n_s}{2\eta n_{\mathrm{ex}} + n_{\mathrm{el}} + 1}\right) \ (\mathrm{PCS}), \tag{16}$$

$$C = \log_2\left(1 + \frac{\eta n_s}{\eta n_{\mathrm{ex}} + n_{\mathrm{el}} + 1}\right) \ (\mathrm{sub-2Q2D}), \tag{17}$$

where η is the detector quantum efficiency and n_{el} is the photon number corresponding to the electric noise variance. The experimental results are shown in Fig. 5(a), which match well with the theoretical curves calculated with zero excess noise at the small number of received signal photons (<2 photons). And the proposed PCS scheme shows higher mutual information than the sub-2Q2D scheme. Experimental points with more received photons deviated from the theoretical curve because of the ascending excess noise measured in our experimental system, as shown in Fig. 5(b), which we attribute to the modulator excess noise.

Within the framework of the GG02 protocol and the security proof against collective attacks, we evaluate the achievable raw key rate in the asymptotic regime based on Eq. (1). In the calculation of each part of the formula, I_{AB} is obtained from the estimated correlation coefficient of received signals, and χ_{BE} is calculated as a function of the excess noise and the other calibrated system parameters. The secure key rate of the proposed phase-sensitive scheme and the single sideband heterodyne scheme are shown in Fig. 6(a). The corresponding estimated values of excess noise are shown in Fig. 6(b). By comparison, the proposed phase-sensitive scheme (with the loose assumption) provides a higher secure key rate than the single sideband heterodyne scheme with higher tolerance to excess noise observed in our experiments. However, the PCS performs more like GG02 when applying more strict assumptions. As mentioned above, this calls for solutions such as the dual quadrature PCS with phase-switched measurement to enhance the current scheme.

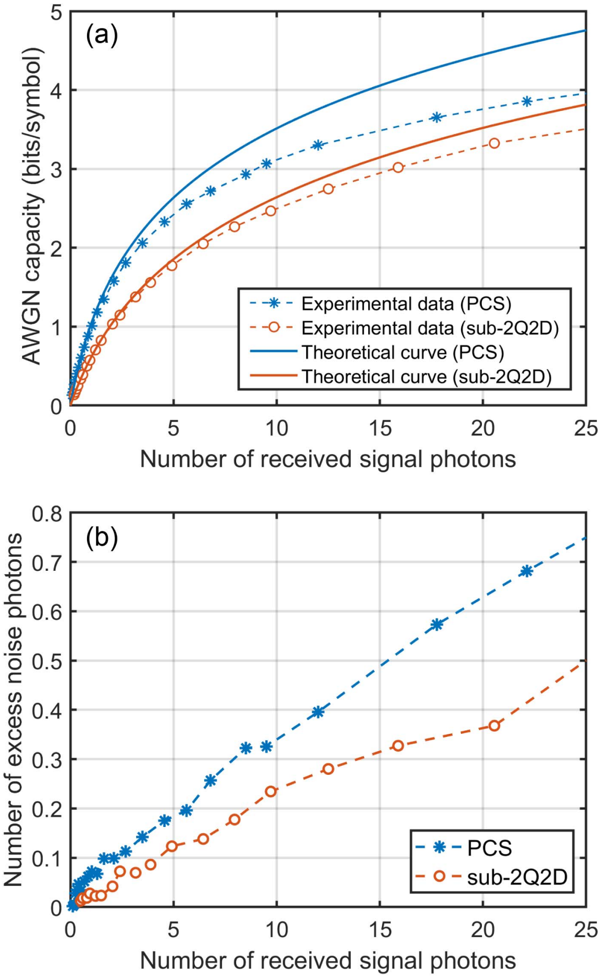

Fig. 5. (a) Experimental results of AWGN capacity of the proposed scheme and the sub-2Q2D scheme, and the theoretical curve plotted with zero excess noise; (b) the corresponding excess noise photons of the experimental points.

To evaluate the system's long-term performance, we collected 120 sets of signal samples from the stably operating system in 2 h to evaluate the excess noise and the raw key rate in the asymptotic regime. In the calibration stage, the detector electrical noise and the SNU are calibrated based on 7 × 10^6 symbols each time the parameters are estimated. Bob's detector, which is assumed to be inaccessible to Eve, is characterized by an electric noise of 0.1473 SNU referring to the channel

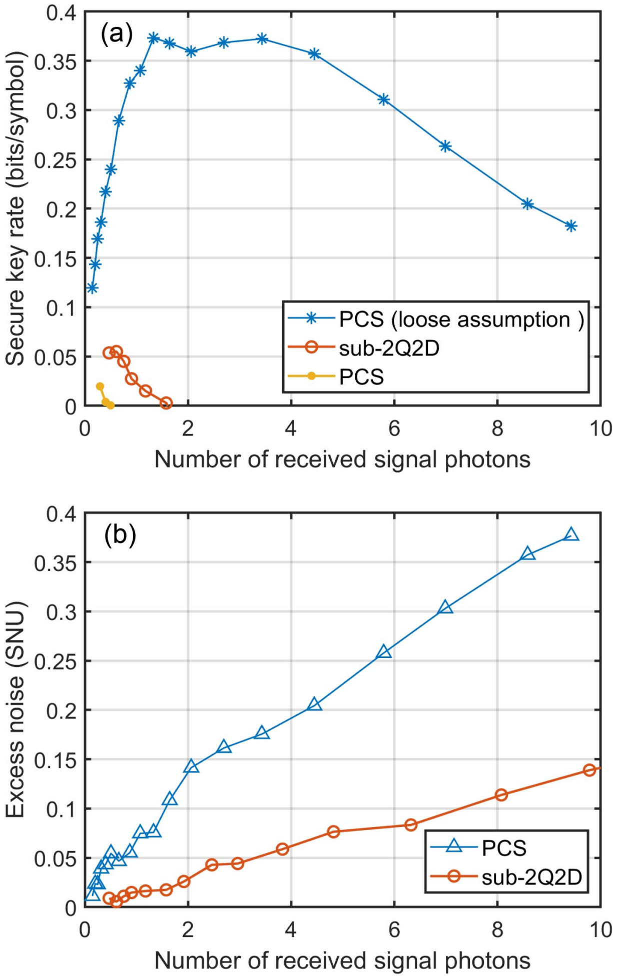

Fig. 6. (a) Experimental results of secure key rate of the proposed scheme and the sub-2Q2D scheme; (b) corresponding excess noise of photons of the experimental points.

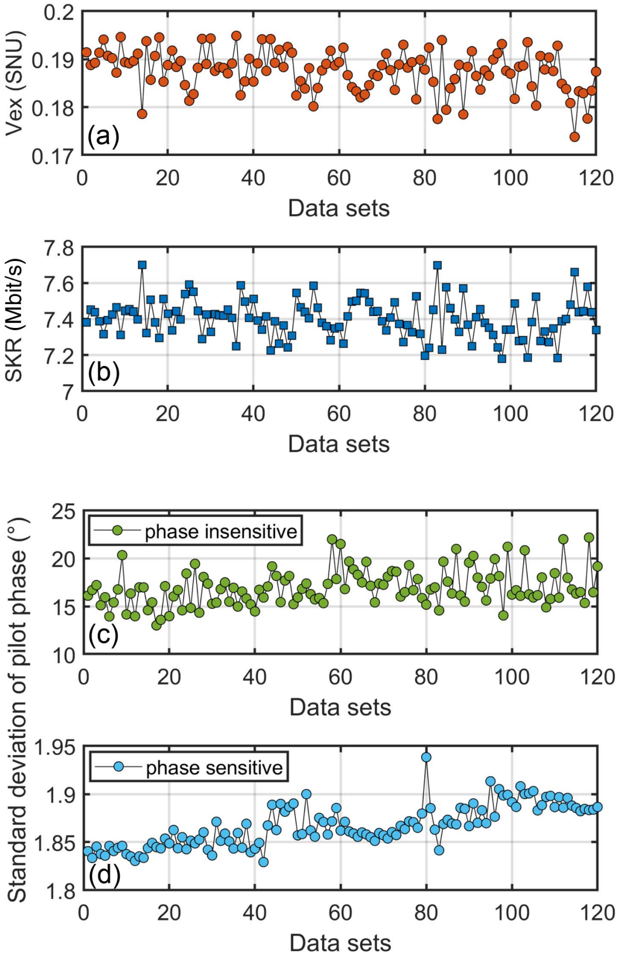

Fig. 7. (a) Estimated excess noise; (b) SKR in the asymptotic regime. The standard deviation of the pilot phase is compared for (c) the sub-2Q2D and (d) the PCS scheme with phase-sensitive detection.

input and a detection efficiency of 0.6. The excess noise and achievable key rate are estimated per 7×10^6 symbols. The results obtained from each set of signal samples are shown in Fig. 7(a). The estimated excess noise is 0.19 SNU on average. The obtained parameters are compatible with a raw key rate in the asymptotic regime between 7.2 and 7.7 Mbit/s with $\beta = 0.95$, an averaged value of 7.4 Mbit/s over a 20-km fiber transmission. The variation of raw key rate is attributed to factors such as the modulator bias drift and the polarization-dependent loss at the receiver. To compare the signal phase fluctuation in the phase-sensitive and phase-insensitive schemes, we calculate the phase standard deviation of the pilot-tone frequency downconverted to the baseband followed by narrow lowpass filtering (a 1-MHz rectangular filter). The results are shown in Fig. 7(b). The standard deviation of the pilot phase keeps around the value of 1.9° with a small range of 1.85°–1.95° in the phase-sensitive scheme. In comparison, the phase-insensitive scheme exhibits a more significant fluctuation of the pilot phase without the phase locking.

To further verify the LO phase is locked to the state that ensures the maximum amplitude of quantum signal (i.e., the maximum SNR), the power of pilot-tone at 100 MHz is measured with an electronic spectrum analyzer (ESA) in zero-span mode when the LO phase is either locking or scanning. The resolution bandwidth and video bandwidth of the ESA are both 1.8 MHz. The results are shown in Fig. 8. The magnitude at the frequency of pilot-tone fluctuates regularly when the LO phase is scanned with PZFS driven by a ramp voltage, whereas in the phase-locked case, the magnitude of pilot tone remains steady at the maximum level in the phase-scanning case.

The improvement of classical information capacity in the proposed scheme is at the cost of spectral efficiency, which is at most half of the single-sideband modulation. From a telecommunication point of view, the proposed scheme possesses several additional advantages. First of all, the use of one balanced detector and possibly one MZM simplifies the system implementation. Second, the detected signal is at an intermediate frequency and hence is free from the $1/f$ noise of the detector and the laser dithering signal at lower frequencies. The PCS scheme can be easily multiplexed with many subcarriers and combined with the wavelength division multiplexing

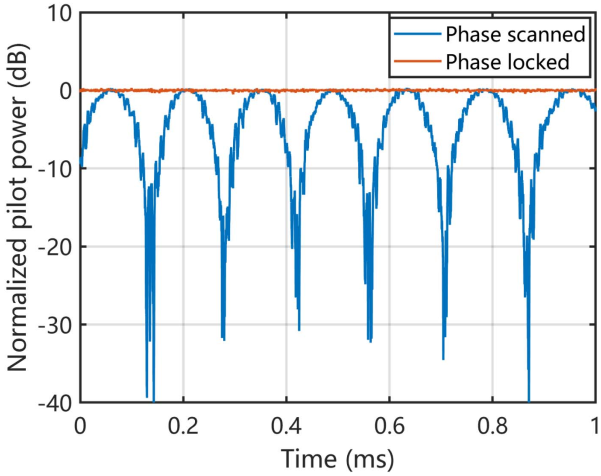

Fig. 8. Normalized power at the pilot frequency in the LO phase-scanned and phase-locked cases.

(WDM) technique to construct a CVQKD network. It is also important to note that the PCS-modulated multimode signal can replace the optical copier for the idler component generation in phase-sensitive amplification (PSA) [30]. Therefore, the proposed scheme is fully compatible with the PSA application, which is a project we are currently working on.

5. CONCLUSION

We develop a phase-sensitive multimode CVQKD scheme exploiting phase-conjugated subcarrier modulation and phase-sensitive homodyne detection. The proposed scheme transmits two phase-conjugated subbands carrying a Gaussian-modulated signal. It is advantageous among the conventional CVQKD schemes, with continuous modulation in the classical information capacity when phase-sensitive detection is applied at the receiver. The experimental implementation of the novel scheme is performed with a simple transmitter. The phase-sensitive detection is realized via OIL and active feedback control. The experimental results confirm the information capacity improvement. Within the GG02 security analysis framework, the proposed scheme offers a higher secure key rate and better excess noise tolerance with a loose assumption. The developed scheme also has great potential for a phase-sensitive optical amplification enhanced CVQKD.

Funding. National Key Research and Development Program of China (2018YFB1801804); National Natural Science Foundation of China (61935011, 62227819, U2001601); Key-Area Research and Development Program of Guangdong Province (2020B0303040001).

Disclosures. The authors declare no conflicts of interest.

Data Availability. Data underlying the results presented in this paper are not publicly available at this time but may be obtained from the authors upon reasonable request.

REFERENCES

1. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden, "Advances in quantum cryptography," Adv. Opt. Photon. **12**, 1012–1236 (2020).
2. H. Yin, Y. Fu, C. Li, C. Weng, B. Li, J. Gu, Y. Lu, S. Huang, and Z. Chen, "Experimental quantum secure network with digital signatures and encryption," Natl. Sci. Rev. **10**, nwac228 (2023).
3. H. Yin, T. Chen, Z. Yu, H. Liu, L. You, Y. Zhou, S. Chen, Y. Mao, M. Huang, W. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, "Measurement-device-independent quantum key distribution over a 404 km optical fiber," Phys. Rev. Lett. **117**, 190501 (2016).
4. Y. Zhang, Z. Chen, S. Pirandola, X. Wang, C. Zhou, B. Chu, Y. Zhao, B. Xu, S. Yu, and H. Guo, "Long-distance continuous-variable quantum key distribution over 202.81 km of fiber," Phys. Rev. Lett. **125**, 010502 (2020).
5. F. Xu, X. Ma, Q. Zhang, H. Lo, and J. Pan, "Secure quantum key distribution with realistic devices," Rev. Mod. Phys. **92**, 025002 (2020).
6. W. Liu, C. Li, Y. Xie, C. Weng, J. Gu, X. Cao, Y. Lu, B. Li, H. Yin, and Z. Chen, "Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance," PRX Quantum **2**, 040334 (2021).
7. F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," Phys. Rev. Lett. **88**, 057902 (2002).
8. M. Navascués, F. Grosshans, and A. Acin, "Optimality of Gaussian attacks in continuous-variable quantum cryptography," Phys. Rev. Lett. **97**, 190502 (2006).
9. F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, "Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks," Phys. Rev. Lett. **109**, 100502 (2012).
10. 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).
11. D. Huang, P. Huang, D. Lin, and G. Zeng, "Long-distance continuous-variable quantum key distribution by controlling excess noise," Sci. Rep. **6**, 19201 (2016).
12. E. Samsonov, R. Goncharov, A. Gaidash, A. Kozubov, V. Egorov, and A. Gleim, "Subcarrier wave continuous variable quantum key distribution with discrete modulation: mathematical model and finite-key analysis," Sci. Rep. **10**, 10034 (2020).
13. R. Goncharov, E. Samsonov, and A. Kiselev, "Subcarrier wave quantum key distribution system with Gaussian modulation," J. Phys. Conf. Series **2103**, 012169 (2021).
14. E. Samsonov, R. Goncharov, M. Fadeev, A. Zinoviev, D. Kirichenko, B. Nasedkin, A. Kiselev, and V. Egorov, "Coherent detection schemes for subcarrier wave continuous variable quantum key distribution," J. Opt. Soc. Am. B **38**, 2215–2222 (2021).
15. H. H. Brunner, L. C. Comandar, F. Karinou, S. Bettelli, D. Hillerkuss, F. Fung, D. Wang, S. Mikroulis, Q. Yi, M. Kuschnerov, A. Poppe, C. Xie, and M. Peev, "A low-complexity heterodyne CV-QKD architecture," in *19th International Conference on Transparent Optical Networks (ICTON)* (IEEE, 2017), pp. 1–4.
16. Z. Su, D. Cai, H. Jiang, J. Wang, D. Wang, X. Guo, and Z. Li, "Optical injection locking based local oscillator regeneration for continuous variable quantum key distribution," Opt. Lett. **47**, 1287–1290 (2022).
17. L. Huang, Y. Zhang, Y. Huang, T. Jiang, and S. Yu, "Improvement of unidimensional continuous-variable quantum key distribution systems by using a phase-sensitive amplifier," J. Phys. B **52**, 225502 (2019).
18. Y. Hashimoto, T. Toyama, J.-I. Yoshikawa, K. Makino, F. Okamoto, R. Sakakibara, S. Takeda, P. van Loock, and A. Furusawa, "All-optical storage of phase-sensitive quantum states of light," Phys. Rev. Lett. **123**, 113603 (2019).
19. J. Mora, A. Ruiz-Alba, W. Amaya, A. Martnez, V. Garca-Muñoz, D. Calvo, and J. Capmany, "Experimental demonstration of subcarrier multiplexed quantum key distribution system," Opt. Lett. **37**, 2031–2033 (2012).

20. J. Fang, P. Huang, and G. Zeng, "Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation," Phys. Rev. A **89**, 022315 (2014).
21. C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," Phys. Rev. Lett. **93**, 170504 (2004).
22. V. C. Usenko and F. Grosshans, "Unidimensional continuous-variable quantum key distribution," Phys. Rev. A **92**, 062337 (2015).
23. S. D. Personick, "BSTJ brief: an image band interpretation of optical heterodyne noise," Bell Syst. Tech. J. **50**, 213–216 (1971).
24. H. P. Yuen and V. W. Chan, "Noise in homodyne and heterodyne detection," Opt. Lett. **8**, 177–179 (1983).
25. Y. Yamamoto and H. Haus, "Preparation, measurement and information capacity of optical quantum states," Rev. Mod. Phys. **58**, 1001–1020 (1986).
26. M. Collett, R. Loudon, and C. Gardiner, "Quantum theory of optical homodyne and heterodyne detection," J. Mod. Opt. **34**, 881–902 (1987).
27. C. M. Caves, "Quantum limits on noise in linear amplifiers," Phys. Rev. D **26**, 1817–1839 (1982).
28. V. Giovannetti, R. Garcia-Patron, N. J. Cerf, and A. S. Holevo, "Ultimate classical communication rates of quantum optical channels," Nat. Photonics **8**, 796–800 (2014).
29. J. Lodewyck, M. Bloch, R. Garca-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, "Quantum key distribution over 25 km with an all-fiber continuous-variable system," Phys. Rev. A **76**, 042305 (2007).
30. R. Kakarla, J. Schröder, and P. A. Andrekson, "One photon-per-bit receiver using near-noiseless phase-sensitive amplification," Light Sci. Appl. **9**, 153 (2020).