Boosting higher secret key rate in quantum key distribution over mature telecom components

Tao Wang (tonystar@sjtu.edu.cn)  
Shanghai Jiao Tong University

Peng Huang  
Shanghai Jiaotong University

Lang Li  
Shanghai Jiaotong University

Yingming Zhou  
Shanghai XunTai Quantech Co., Ltd

Guihua Zeng  
Shanghai Jiao Tong University

Article

Keywords: secret key rate, quantum key distribution, mature telecom components

Posted Date: November 11th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-951048/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License. Read Full License
Boosting higher secret key rate in quantum key distribution over mature telecom components

Tao Wang\textsuperscript{1,2,3}, Peng Huang\textsuperscript{1,2,3}, Lang Li\textsuperscript{1}, Yingming Zhou\textsuperscript{4}, and Guihua Zeng\textsuperscript{1,2,3,†}

\textsuperscript{1}State Key Laboratory of Advanced Optical Communication Systems and Networks, Center for Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, China
\textsuperscript{2}Shanghai Research Center for Quantum Sciences, Shanghai 201315, China
\textsuperscript{3}Hefei National Laboratory, CAS Center for Excellence in Quantum Information and Quantum Physics, Hefei, Anhui 230026, China
\textsuperscript{4}Shanghai XunTai Quantech Co., Ltd, Shanghai 200241, China
\textsuperscript{†}ghzeng@sjtu.edu.cn

\textbf{ABSTRACT}

Secret key rate is a core performance indicator in implementing quantum key distribution, which directly determines the transmission rate of enciphered data. Here we demonstrate a high-key-rate quantum key distribution system over mature telecom components. The entire framework of quantum key distribution over these components is constructed. The high-rate low-noise Gaussian modulation of coherent states is realized by a classical electro-optic IQ modulator. High-baud low-intensity quantum signals are received by a commercial integrated coherent receiver under the shot-noise limit. A series of digital signal processing algorithms are proposed to achieve accurate signal recovery and key distillation. The system has yield a secret key rate of 10.37 Mbps, 1.61 Mbps, 337.82 kbps, and 58.06 kbps under the standard telecom fiber of 20 km, 50 km, 70 km, and 100 km, respectively. Our results represent the achieved highest secret key generation rate for quantum key distribution using continuous variables at a standard telecom wavelength. Moreover, it breaks the isolation between quantum communication and classical optical communication in terms of components, and opens the way to a high-speed and cost-effective formation of metropolitan quantum secure communication networks.

\textbf{Introduction}

Quantum key distribution (QKD), one quantum information technology, can provide secure keys for legal parties through an untrusted quantum channel, whose theoretical security is guaranteed by quantum mechanics’ basic principles. Gaussian-modulated coherent-state (GMCS) continuous-variable QKD (CV-QKD) protocol\textsuperscript{1-2} is one well-known QKD protocol, in which the initial key information is encoded on the quadrature components of the quantized electromagnetic field and is detected by coherent detection technology. In theory, GMCS CV-QKD has been theoretically proved to be secure against arbitrary collective attacks\textsuperscript{3-6} and coherent attacks\textsuperscript{7}, even considering the finite-size effects\textsuperscript{8-12}. In actual implementation, CV-QKD has made great breakthroughs in secure transmission distance, secret key rate, integration, and field test\textsuperscript{13-17}, demonstrating its good application prospects in the construction of metropolitan quantum networks.

Nevertheless, before QKD is widely adopted, it still faces some crucial challenges, such as secret key rate, distance, size, cost, and practical security.\textsuperscript{18} Secret key rate (SKR), one core performance indicator of QKD in actual implementation, determines the transmission rate of enciphered data. Specifically, in quantum private communication, information-theoretically secure can only be achieved by combining one-time-pad (OTP) encryption protocol at a time with QKD. OTP protocol requires the key used only once and be as long as the message, which means that SKR needs to be consistent with the classical data rate. As the communication techniques improve, classical optical communications that provide 100 Gbit/s per wavelength channel are deployed\textsuperscript{19}. A field trial featuring an aggregate data rate of 54.2 Tbit/s has been carried out\textsuperscript{20}. Some alternative protocols, such as quantum stream cipher\textsuperscript{21} and physical-layer secret key generation and distribution (SKGD)\textsuperscript{22}, can offer a higher rate, but their security has not been proven entirely yet. Therefore, it is clear that if we want to encrypt high volumes of classical network traffic using OTP in the longer term, significant developments on the SKR generated by QKD are required.\textsuperscript{18}

In terms of improving the SKR, much work has been done for discrete-variable quantum key distribution (DV-QKD), such as improving the repetition rate to gigahertz\textsuperscript{23}, developing high-speed post-processing modules\textsuperscript{24}, exploiting high-dimensional quantum states\textsuperscript{25}, and using heterogeneous multicore fiber\textsuperscript{26}. The latest SKR performance has reached 10 Mbps@10km. For CV-QKD, by controlling the excess noise of the system and increasing the post-processing performance, the SKR has also been significantly improved\textsuperscript{27-29}. Moreover, due to the encoding scheme, the theoretical SKR generated by CV-QKD in the theoretical asymptotic regime can be close to the ideal SKR performance curve without relay, which scales as 1/2 of the PLOB bound\textsuperscript{30}.

At present, the SKR of CV-QKD is mainly limited by the system repetition rate. The classical coherent optical communication, which has a similar optical system structure, can reach the repetition rate of even 100 GBAud\textsuperscript{31}, whereas Gaussian-modulated CV-QKD has been below 100 MBaud.
for a long time. The restriction of repetition rate mainly comes from three aspects:

1. Signal modulation rate. Gaussian modulation is different from the conventional modulation format, requiring higher modulation accuracy, and otherwise, unacceptable modulation noise will be introduced. In standard Gaussian modulation, the quantum state is usually modulated by an amplitude and a phase modulator. This scheme is susceptible to the nonlinear response of the modulator and gain-bandwidth product of the amplifier when the modulation rate is high.

2. Signal reception rate. The signal reception in CV-QKD is required to reach the shot-noise limit; otherwise, the noise introduced by eavesdropping will not be easily detected. The coherent detection circuit limits the shot-noise clearance achievable at high frequencies and therefore restricts the detection bandwidth.

3. Data processing scheme. Since the quantum signal’s signal-to-noise ratio (SNR) under the shot-noise limit detection is relatively low, compensating for channel impairment and imperfections in classical components at a high repetition rate has not been realized yet. The excess noise due to the incomplete compensation will significantly deteriorate the final SKR.

It is a straightforward idea to use high-speed classical devices with well-designed algorithms to solve the above problems. However, most quantum information technologies rely on dedicated quantum devices, and the mature classical components have advantages in performance and cost but do not work in the quantum regime. Therefore, using classical components to exhibit quantum effects and further implement quantum information technology is highly challenging, but once it works, its performance can be significantly improved.

In this paper, we report a complete CV-QKD system composed of mature telecom components that achieves a record-high SKR. The high-rate low-noise Gaussian modulation of coherent states is realized by a classical electro-optic IQ modulator. High-baud low-intensity quantum signals are received by a commercial integrated coherent receiver under the shot-noise limit. A series of digital signal processing algorithms are proposed to achieve accurate signal recovery and key distillation. The system has finally achieved 10.37 Mbps, 1.61 Mbps, 337.82 kbps, and 58.06 kbps SKR within standard telecom single-mode fiber of 20 km, 50 km, 70 km, and 100 km. This achieved SKR is higher than state-of-the-art GMCS CV-QKD experiments. Besides, the isolation between quantum communication and classical optical communication in terms of components has been broken, which opens the way to establish a high-speed and cost-effective QKD network using mature telecom components directly.

Results

Protocol and secret key rate

CV-QKD with Gaussian modulation can be implemented according to the preparation-and-measurement model, which is schematically depicted in Fig. 1. In this protocol, Alice uses the laser source to prepare the original coherent states. Then these states are modulated following the Gaussian distribution. That is, Alice first prepare Gaussian random number vector \( \{x_A, p_A\} \), and then load it on the origin coherent state to generate the coherent state \( |x_A + ip_A\rangle \). Moreover, she needs to adjust the attenuation to set the desired quadrature component variance value \( V_A \) of the output coherent states. After being transmitted through the quantum channel, the quantum signal is detected by a homodyne detector or a heterodyne detector. In this work, the heterodyne detector is adopted to achieve phase recovery easily. Specifically, The quantum signal is first divided equally by a 50 : 50 BS and then detected by two homodyne detectors to obtain the quadrature component value of \( x_B \) and \( p_B \), respectively. The theoretical security of GMCS CV-QKD is proved through the entanglement-based model, and the achievable SKR at a specific distance is estimated according to the information theory.

![Figure 1. The schematic diagram of CV-QKD with Gaussian modulation. CS source: coherent state source; Mod.: modulation; Att.: attenuation. Shot noise is the uncertainty of the quadrature component of a coherent state, and \( V_A \) is the variance of data modulated on the quadrature component.](image)

In the asymptotic conditions, the achievable SKR generated by CV-QKD can be calculated as

\[
R = f_e \times (1 - a)(1 - FER)(1 - \nu)[\beta I_{AB} - \chi_{BE}],
\]  

where \( f_e \) is the effective symbol rate, \( I_{AB} \) is the classical mutual information between Alice and Bob, \( \chi_{BE} \) is the Holevo bound on the information leaked to Eve, \( \beta \) is the reconciliation efficiency, FER is the frame error rate of the reconciliation, \( a \) is the overhead for frame synchronization, \( \nu \) is the key fraction disclosed for parameter estimation. The detailed derivation of SKR is given in Supplemental Material.

In an actual system, the fraction disclosed for parameter estimation \( \nu \) has an optimal value and can be calculated. The overhead \( a \) is determined according to the actual channel condition. The frame error rate and reconciliation efficiency are related to the selected decoder—the selected decoder should
trade off these two parameters. The amount of mutual information $I_{AB}$ and $I_{BE}$ are both related to the modulation variance $V_A$, so $V_A$ has an optimal value to maximize the difference between the two. $X_{BE}$ is also related to the critical parameter excess noise $\varepsilon$. The larger $\varepsilon$ is, the greater the amount of information leaked to Eve, and even make SKR drop to 0. Therefore, controlling the excess noise is essential. According to the formula, it can intuitively be seen that by increasing the repetition rate, SKR will increase proportionally. However, it is also necessary to ensure the accurate modulation and reception of the quantum signal and the high-precision signal recovery after increasing the repetition frequency, guaranteeing excess noise suppression and high SKR performance.

**Experimental set-up**

The entire optical layer set-up is based on the local local oscillator (LLO) scheme architecture \(^{34-39}\), shown in Fig. 2. At Alice, a narrow-linewidth continuous-wave (CW) laser with 100 Hz linewidth (NKT Khoeras BASIK X15) generates the optical carrier, followed by an optical isolator and a variable optical attenuator to control its power. Then, the optical carrier is sent into the high-speed lithium niobate IQ modulator (IQM) to realize the Gaussian modulation. Specifically, an Arbitrary Wave Generator (AWG, Tekronix, AWG5200) is loaded in Gaussian random number data (which is generated by a quantum random number generator (QRNG)) and then outputs two Gaussian distributed electrical analog signals with 500 MHz symbol rate, which are then amplified by a two-channel microwave amplifier (MA) to meet the requirement of the IQ modulator. The AWG can achieve a sampling rate of 5 GSample/s and has a sampling depth of 16 bit. The pilot data is interposed between Gaussian data. Its value is relatively large and alternates between positive and negative. The generated pilot signals are reference symbols with agreed information and location, helping the data processing but not form part of the secret key generation. The six bias of IQ modulator is automatically controlled to a suitable configuration by a bias controller (BC), which adopts automatic feedback control to ensure constellation modulation’s stability. In order to reduce the crosstalk between signal pulses, an intensity modulator with a high extinction ratio (EOSPACE) is employed to cut continuous-wave light into pulsed light. The pulsed electrical signal is also generated by the AWG, and the duty cycle is set to 20%. Then it is amplified by another microwave amplifier and then loaded on the intensity modulator. The bias point of the modulator is controlled by a DC stabilized power supply to ensure stable optical pulse generation. A manual VOA is deployed to control the output power. A deployed 90:10 BS monitors the output power in real-time, followed by several single-mode fiber (SMF) spools for long-distance transmission.

After the signal arrives at the receiver, it is adjusted by the polarization controllers and then interferes with the locally generated LO. The LO is CW mode and comes from another narrow linewidth laser (NKT Khoeras BASIK X15), the center wavelength of which can be controlled by software to align with the signal laser. Both the LO and signal are injected into a commercial integrated coherent detector (ICR, FUJITSU). ICR is a standard component in classical communication that can be integrated into the coherent optical module. The ICR parameter relevant with CV-QKD is tested, where the detectors in ICR have the same quantum efficiencies $\eta = 0.42$ and electronic noises $\nu_{el} = 0.18$ in shot noise units (SNU) (see Supplemental Material for more details). The shot noise is calibrated in real-time. After the LO and signal enter the ICR, they are interfered with, detected, and amplified, and finally, four detection outputs are provided. Two of the detection ports are used to collect signals, and the other two ports are used to observe real-time changes in polarization. These detected signals are sampled and quantized by a real-time high-speed oscilloscope (Lecroy, Wavemaster 8132i-B) (received signal is shown in Fig. 3), finishing the quantum communication procedure.

**Gaussian modulation characterization**

Gaussian modulation is a crucial criterion in the theoretical CV-QKD protocol, making it convenient to use Gaussian optimality to realize unconditional security proof. Therefore, to be consistent with the theoretical protocol, the transmitter must also perform the Gaussian modulation format. Specifically, the amplitude of the modulated electrical signal at the transmitter is restricted to the linear interval of the response function of the IQ modulator to ensure the Gaussian property of the modulated optical field, and the coherent detection at the receiver is also within the linear operating interval. In Fig. 4, the distribution of the modulation data at Alice and the received data at Bob (after digital signal processing) are shown in (a) and (b), respectively. The Gaussian performance is tested by Shapiro and Wilk’s W-test \(^{40}\). Results show that at the significance level of $\alpha = 0.05$, both the modulation and received data obey the Gaussian distribution (W-test statistic $W = 0.995, 0.997$, P-value=$0.182, 0.799$), proving the Gaussian performance. Moreover, Fig. 4(c) shows the linearity of the transmitted data and the received data. The SNR of the quantum signal is 2.58 dB, and the statistical sample size is $10^4$. The slope of the fitting curve is $k = 0.996$, expressing the consistency of data sent and received. Fig. 4(d) is the raw collected data at the receiver, including quantum signal and pilot. The SNR of the pilot is set as 12.53 dB. Due to the phase derivation, the pilot data forms a ring in the phase space, and the signal data maintains a two-dimensional Gaussian distribution.

**Phase noise elimination**

In the experiment, equally spaced pilot signals are inserted between the quantum signals to compensate for the frequency offset and phase drift caused by the independent LO laser. Specifically, we use the same IQ modulator to generate an interleaved pilot signal when preparing a quantum signal. The intensity of the generated pilot signal is entirely proportional to the amplitude of the modulated electrical signal, so it is
Figure 2. (a) Experimental setup of the GMCS CV-QKD scheme using high-speed mature telecom components; (b) Quantum signal modulation module; (c) Quantum signal integrated coherent receiver module; (d) Quantum random number generator module. The blue and red lines denote the single-mode and polarization-maintaining fibers, respectively. Iso: isolator; BS: beam splitter; VOA: variable optical attenuator; IQM: IQ modulator; PC: polarization controller; MA: microwave amplifier; DC: DC stabilized power supply; ICR: integrated coherent receiver; BHD: balanced homodyne detector.

Figure 3. Afterglow of the collected signal. The yellow afterglow represents the $X$ component electronic signal, and the red afterglow represents the $P$ component electronic signal. The higher pulse represents the pilot signal, and the lower pulse between the two pilot signals represents the quantum signal.

convenient to set different power intensities. At the receiver, the phase compensation method is based on the pilot around the quantum signal. A new approach is proposed for different phase drift rates. We set up pilot signals of different powers and then statistics on the remaining phase noise after phase compensation, shown in Fig. 5 (a). One can see that as the pilot power increases, the residual phase noise gradually decreases. When the SNR is higher than 15 dB, the phase noise can be less than 0.01 $rad^2$, and when the SNR is greater than 25 dB, the phase noise can be less than 0.001 $rad^2$. This result determines the set of pilot signal power in the key distribution procedure.

In addition, we also analyzed the frequency offset (FO) of the two lasers through the pilot, which is shown in Fig. 5 (b). The red color represents the FO of the two NKT narrow-linewidth lasers at different times. Due to the high stability of the laser wavelength ($\pm 0.04$ pm within 60 min), the FO changes very slightly. The FO of the two commercial Integrable Tunable Laser Assembly (ITLA) lasers represented in blue is used for comparison. Since its stability is only $\pm 1$ pm within 15 min, it will jitter at MHz level in a short period and finally exceed the detector bandwidth after a while. Therefore, for ITLA lasers, the center wavelength will be controlled through real-time feedback algorithms to ensure long-time system operation in the next step.

Excess noise measurement

In the actual key distribution procedure, a data frame is composed of the frame header, pilot, and raw key data. The length of one frame is $5 \times 10^3$, where the frame header occupies $1 \times 10^3$, data occupies $2.49 \times 10^3$, and the interleaved pilot is $2.5 \times 10^3$. After receiving, the signal will be processed through a series of digital signal processing algorithms (introduced in Methods), and finally, recover the original key.
Figure 4. Gaussian modulation characterization. (a) and (b) show the modulation data and received data, which exhibit Gaussian distribution characteristics. (c) shows the correlation between modulation data and received data, corresponding to an SNR of 2.58 dB. (d) illustrates both the quantum signal and pilot. The SNR of the pilot is set as 12.53 dB, which is 9.95 dB higher than the quantum signal.

Figure 5. Measured phase noise & Frequency offset. (a) The residual phase noise under different SNR of the pilot has been tested. The phase noise in each SNR was tested by 10 times, and both the SNR and the phase noise deviation are displayed. (b) the frequency offset between two lasers has been tested. The FO between the two NKT ultra narrow-linewidth lasers is represented in red. The blue represents the change of the FO of the commercial ITLA lasers for comparison.

Secret key rate analysis
According to the measured excess noise and the key experimental parameters (shown in Table 1), the SKR that can be achieved in the experiment is shown in Table 2. The length of the telecom fiber spools used for test is 20 km, 50 km, 70 km, and 100 km, respectively, and the corresponding attenuation is 3.68 dB, 9.26 dB, 12.94 dB, and 18.96 dB. In order to ensure accurate phase compensation without affecting the quantum signal, the SNR of the pilot is controlled around 16 dB. The modulation variance $V_A$ changes slightly with the distance, and the purpose is to achieve the high SKR performance at different distances. The rate-adaptive LDPC is employed to decode, and FER with $\beta = 95\%$ is obtained through statistics from a large number of samples, which are 15.30%, 18.60%, 19.10%, and 17.40% respectively. Finally, the average SKR achieved in the experiment is 10.37 Mbps, 1.61 Mbps, 337.82 kbps, and 58.06 kbps, respectively.

The SKR that can be achieved at different distances in the

and therefore need to be estimated accurately. The traditional parameter estimation scheme is adopted\textsuperscript{41}. Fig. 6 shows the excess noise measured by the system under a 20 km standard telecommunication fiber. By testing 20 data frame, the average value of the excess noise is 0.062, which can be below the 10 Mbps threshold bound and therefore has 10 Mbps SKR capability. In the experiment, the remaining excess noise of the system mainly comes from the limited phase compensation accuracy, while the excess noise fluctuation comes from the device’s instability. For example, the jitter of the laser intensity will cause the signal modulation variance and pilot power changes.
Table 1. Practical parameter in CV-QKD experiment

| No.  | Parameter                        | Value       |
|------|----------------------------------|-------------|
| 1    | System repetition rate $f_s$     | 500 MHz     |
| 2    | Effective symbol rate $f_c$      | 250 MHz     |
| 3    | Duty cycle $D$                   | 20%         |
| 4    | Sample rate $R$                  | 10 GS/s     |
| 5    | Data frame length $N$            | $2.49 \times 10^5$ |
| 6    | Overhead ratio $a$               | 0.4%        |
| 7    | Ratio for parameter estimation $\nu$ | 10%        |
| 8    | Quantum efficiency $\eta$       | 0.42        |
| 9    | Electronic noise $v_{el}$        | 0.18        |
| 10   | Reconciliation efficiency $\beta$ | 95%         |

In conclusion, we have demonstrated the first complete GMCS CV-QKD system using high-speed mature telecom components, which achieves a record-high SKR. In particular, we use a high-speed IQ modulator to realize accurate Gaussian modulation, employ ICR to detect the quantum signal, and propose a series of algorithms to eliminate the impairment in quantum signals. Finally, the excess noise induced in the whole communication has been suppressed, reaching 0.062, 0.050, 0.054, and 0.037 under the standard single-mode fiber of 20 km, 50 km, 70 km, and 100 km. The corresponding SKR achieved with our post-processing scheme is 10.37 Mbps, 1.61 Mbps, 337.82 kbps, and 58.06 kbps, respectively.

It is anticipated that with the improvement of experiment details, including automatic polarization control and laser power stability, the excess noise in the system can be further controlled stable and low. Besides, the finite-size effect is not considered in this work. It can be mitigated by employing high-speed ADCs to acquire a larger block in the next step. Moreover, with the improved hardware capacity, real-time secret key generation can also be implemented. Our work verifies the feasibility of GMCS CV-QKD with high-speed mature telecom components. The achieved SKR is higher than state-of-the-art GMCS CV-QKD experiments. Considering that existing coherent optical modules such as CFP-ACO are also constructed by these mature components, this work provides a high-speed and cost-effective QKD system scheme to build the future quantum communication network.

**Discussion**

In conclusion, we have demonstrated the first complete GMCS CV-QKD system using high-speed mature telecom components, which achieves a record-high SKR. In particular, we use a high-speed IQ modulator to realize accurate Gaussian modulation, employ ICR to detect the quantum signal, and propose a series of algorithms to eliminate the impairment in quantum signals. Finally, the excess noise induced in the whole communication has been suppressed, reaching 0.062, 0.050, 0.054, and 0.037 under the standard single-mode fiber of 20 km, 50 km, 70 km, and 100 km. The corresponding SKR achieved with our post-processing scheme is 10.37 Mbps, 1.61 Mbps, 337.82 kbps, and 58.06 kbps, respectively.

It is anticipated that with the improvement of experiment details, including automatic polarization control and laser power stability, the excess noise in the system can be further controlled stable and low. Besides, the finite-size effect is not considered in this work. It can be mitigated by employing high-speed ADCs to acquire a larger block in the next step. Moreover, with the improved hardware capacity, real-time secret key generation can also be implemented. Our work verifies the feasibility of GMCS CV-QKD with high-speed mature telecom components. The achieved SKR is higher than state-of-the-art GMCS CV-QKD experiments. Considering that existing coherent optical modules such as CFP-ACO are also constructed by these mature components, this work provides a high-speed and cost-effective QKD system scheme to build the future quantum communication network.

**Methods**

**Peak Searching and shot noise calibration**

Since the oscilloscope that collects the data is triggered by the same clock source as the signal generator for synchronous sampling, we only need to find the peak point for each pulse. Considering that the sampling rate is 10 GS/s and the symbol rate is 500 MHz, the first 40 sampling data $x_{Bi}$ and $p_{Bi}$ (covering one quantum signal and one pilot signal) is used to calculate the corresponding power, i.e., $P_i = x_{Bi}^2 + p_{Bi}^2$. Since
the pilot has high power, the index \( i \) corresponding to the maximum power value \( P_i \) is the optimal sampling position.

Considering that the oversampling ratio is 20, we take this sampling position as the origin and extract the data every 20 point, which constitutes the pilot and quantum signal’s component data \( x_{pilot}, p_{\text{pilot}} \) and \( x_{\text{sig}}, p_{\text{sig}} \).

In addition, since the LO is continuous-wave from and the high extinction ratio AM has converted the signal into a pulse form, the sampling points between the pilot pulse and the quantum signal pulse can be used for real-time shot-noise calibration (shown in Fig. 3. Specifically, we use the data at the intermediate index \((i + 10 \mod 20)\) to evaluate the shot noise. Since the noise has been filtered and has the sampling rate same as the signal, it can accurately reflect the shot noise in the signal (the noise calibrated here is the sum of shot noise and electronic noise calibrated in advance because of its stability). Such a method can dramatically eliminate the influence of the laser’s relative intensity noise (RIN).

### Quadrature component balance calibration

After peak searching, due to the inconsistent responsivity of each photodiode in the ICR, the imbalance of component data \( x \) and \( p \) needs calibration. Here the pilot signal is used again to balance the \( x \) and \( p \). Since the pilot signal is set to a fixed value, the variance of pilot component data \( x_{\text{pilot}} \) and \( p_{\text{pilot}} \) obtained by the receiver will be equal theoretically due to the phase drift. However, the unbalanced response make the variance inconsistent. This inconsistent variance is exploited to determine the scaling ratio. The method is as follows: Step 1. Calculate the variance of the component data of the collected pilot signal, i.e var\[\{x_{\text{pilot}}\}\] and var\[\{p_{\text{pilot}}\}\].

Step 2. Get conversion ratio \( r = \sqrt{\text{var}\[\{x_{\text{pilot}}\}\] / \text{var}\[\{p_{\text{pilot}}\}\]} \).

Step 3. All the \( p \) component data \( p_{\text{sig}}; p_{\text{pilot}} \) is scaled by \( p_{\text{pilot}} = p_{\text{pilot}} \times r, p_{\text{sig}} = p_{\text{sig}} \times r \). After scaling, quadrature component data is balanced.

### Frequency offset estimation

After quadrature balance calibration, we need to estimate the frequency offset. The frequency offset comes from the inconsistency of the center wavelength of the two lasers. We perform Fourier transform on the pilot signal to find the maximum value \( f_{\text{off}} \), which corresponds to the frequency offset. However, the direction of frequency offset cannot be judged.

According to the traditional method in classical optical communication\(^{30}\), the pre-compensation of frequency offset is executed on the pilot signal. We can determine the correct direction according to the variance of the data in both cases. If the compensation direction is wrong, the pilot signal will not converge to a fixed point (see Supplemental Material for more details).

### Phase compensation

After the frequency offset is estimated, the phase drift in the quantum signal is compensated. Unlike classical coherent optical communication, the phase deviation due to frequency offset is not compensated in the previous stage but this stage. According to the estimation of frequency offset and the pilot signal, the phase drift is recovered. The phase compensation method is based on\(^{14}\) but has been further improved to adapt.
to phase drift at different rates (see Supplemental Material for more details).

Frame synchronization

After the phase compensation, the correspondence of sending and receiving data needs to be established. Realizing data frame synchronization at different distances is very important in CV-QKD. Here we use the Zadoff-Chu (ZC) sequence as the frame header of the Gaussian modulation data. The ZC sequence has good zero autocorrelation and low cross-correlation. The longer the length of the ZC sequence, the higher the correlation peak and the better the frame synchronization performance. The frame header length $N$ is set as 1000, and its average power is consistent with the pilot power. Simulations show that the frame header with proper power can support frame synchronization within 100 km, ensuring the CV-QKD experiment’s completion (see Supplemental Material for more details).

Post-processing

In the post-processing stage, the traditional estimations of channel parameters $T$ and $\epsilon$ are performed, by which the achievable SKR can be estimated. Next, the data reconciliation is performed according to the estimated parameters, and the final key is distilled through privacy amplification. In this process, the most crucial part is the decoding scheme, which directly determines the two key parameters in Eq. 1: reconciliation efficiency $\beta$ and frame error rate FER. In the actual implementation of CV-QKD, the SNR of the received signal is much lower than that of the classic communication. Therefore, it is challenging to guarantee the $\beta$ and FER at different distances under such circumstances. Here, the rate-adaptive LDPC using puncturing and shortening with multidimensional reconciliation is adopted to achieve low-SNR decoding at different distances to meet the decoding requirements of CV-QKD within the 100 km transmission distance. Four codes with different code rates ($R = 0.5, 0.1, 0.02, 0.01$) are combined to realize rate-adaptive LDPC, guaranteeing high-performance decoding under different transmission distances (see Supplemental Material for more details).

High-speed quantum random number generator

The quantum random number generator (QRNG) used for raw key data is manufactured by Shanghai XunTai Quanotech Co., Ltd. The entropy source of the QRNG is the fluctuation of vacuum state and is detected by balanced homodyne detection. The detected signal is sampled by high-speed ADC, then processed by FPGA, and converted into a quantum random number sequence. Owing to the ADC and FPGA processing speed, the output rate of the QRNG can reach 1 Gbps, and its randomness has passed the NIST randomness test. We use the random number generated by this QRNG to generate Gaussian modulation data, ensuring the true randomness of the raw key information.

Data availability

The data that support the plots within this paper are available from the corresponding authors on reasonable request.

Code availability

Computer codes to calculate the secret key rate are available from the corresponding authors on reasonable request.

References

1. F. Grosshans and P. Grangier. Continuous variable quantum cryptography using coherent states. Physical Review Letters, 88, 057902 (2002).
2. F. Grosshans, G. Van Assche, J. Wenger, R. Brouni, N. J. Cerf, and P. Grangier. Quantum key distribution using gaussian-modulated coherent states. Nature, 421, 238 (2003).
3. R. Garcia-Patron and N. J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. Physical Review Letters, 97, 190503 (2006).
4. M. Navascues, F. Grosshans, and A. Acin. Optimality of gaussian attacks in continuous-variable quantum cryptography. Physical Review Letters, 97, 190502 (2006).
5. S. Pirandola, S. L. Braunstein, and S. Lloyd. Characterization of collective gaussian attacks and security of coherent-state quantum cryptography. Physical Review Letters, 101, 200504 (2008).
6. A. Leverrier and P. Grangier. Simple proof that gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a gaussian modulation. Physical Review A, 81, 062314 (2010).
7. R. Renner and J. I. Cirac. de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. Physical Review Letters, 102, 110504 (2009).
8. A. Leverrier, F. Grosshans, and P. Grangier. Finite-size analysis of a continuous-variable quantum key distribution. Physical Review A, 81, 062343 (2010).
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. Physical Review Letters, 109, 100502 (2012).
10. A. Leverrier, R. Garcia-Patron, R. Renner, and N. J. Cerf. Security of continuous-variable quantum key distribution against general attacks. Physical Review Letters, 110, 030502 (2013).
11. A. Leverrier. Composable security proof for continuous-variable quantum key distribution with coherent states. Physical Review Letters, 114, 070501 (2015).
12. A. Leverrier. Security of continuous-variable quantum key distribution via a gaussian de finetti reduction. *Physical Review Letters*, **118**, 200501 (2017).

13. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, **7**, 378 (2013).

14. D. Huang, P. Huang, D. Lin, and G. Zeng. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Scientific Reports*, **6**, 19201 (2016).

15. D. Huang, P. Huang, H. Li, T. Wang, Y. Zhou, and G. Zeng. Field demonstration of a continuous-variable quantum key distribution network. *Optics Letters*, **41**, 3511 (2016).

16. G. Zhang, J. Y. Haw, H. Cai, F. Xu, S. M. Assad, J. F. Fitzsimons, X. Zhou, Y. Zhang, S. Yu, J. Wu, W. Ser, L. C. Kwek, and A. Q. Liu. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. *Nature Photonics*, **13**, 839 (2019).

17. 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. *Physical Review Letters*, **125**, 010502 (2020).

18. E. Diamanti, H. K. Lo, B. Qi, and Z. Yuan. Practical challenges in quantum key distribution. *Npj Quantum Information*, **2**, 1-12 (2016).

19. P. J. Winzer. Scaling optical fiber networks: Challenges and solutions. *Optics and Photonics News*, **26**, 28–35 (2015).

20. M. Huang, A. Tanaka, E. Ip, Y. Huang, D. Qian, Y. Zhang, S. Zhang, P. N. Ji, I. B. Djordjevic, T. Wang, Y. Aono, S. Murakami, T. Tajima, T. J. Xia, and G. A. Wellbrock. Terabit/s nyquist superchannels in high capacity fiber field trials using dp-16qam and dp-8qam modulation formats. *Journal of Lightwave Technology*, **32**, 776–782 (2014).

21. G. A. Barbosa, E. Corndorf, P. Kumar, and H. P. Yuen. Secure communication using mesoscopic coherent states. *Physical Review Letters*, **90**, 227901 (2003).

22. K. Kravtsov, Z. Wang, W. Trappe, and P. R. Prucnal. Physical layer secret key generation for fiber-optical networks. *Optics Express*, **21**, 23756-23771 (2013).

23. M. Lucamarini, K. A. Patel, J. F. Dynes, B. Froehlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Efficient decoy-state quantum key distribution with quantified security. *Optics Express*, **21**, 24550-24565 (2013).

24. Z. Yuan, A. Plews, R. Takahashi, K. Doi, W. Tam, A. W. Sharpe, A. R. Dixon, E. Lavelle, J. F. Dynes, A. Murakami, M. Kujiraoka, M. Lucamarini, Y. Tanizawa, H. Sato, and A. J. Shields. 10-mb/s quantum key distribution. *Journal of Lightwave Technology*, **36**, 3427-3433 (2018).

25. N. T. Islam, C. C. W. Lim, C. Cahall, J. Kim, and D. J. Gauthier. Provably secure and high-rate quantum key distribution with time-bin qudits. *Science Advances*, **3**, e1701491 (2017).

26. B. Da Lio, D. Bacco, D. Cozzolino, F. Da Ros, Guo Xueshi, Ding Yunhong, Y. Sasaki, K. Aikawa, S. Miki, H. Terai, T. Yamashita, J. S. Neergaard-Nielsen, M. Galli, K. Rottwitt, U. L. Andersen, L. K. Oxenløwe, and T. Mørioka. Record-High Secret Key Rate for Joint Classical and Quantum Transmission Over a 37-Core Fiber. In *2018 IEEE Photonics conference (IPC)* (pp. 1-2), IEEE, (2018).

27. D. Huang, D. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. Zeng. Continuous-variable quantum key distribution with 1 mbps secure key rate. *Optics Express*, **23**, 17511–17519 (2015).

28. T. Wang, P. Huang, Y. Zhou, W. Liu, H. Ma, S. Wang, and G. Zeng. High key rate continuous-variable quantum key distribution with a real local oscillator. *Optics Express*, **26**, 2794-2806 (2018).

29. Sebastian Kleis and Christian G. Schaeffer. Improving the secret key rate of coherent quantum key distribution with bayesian inference. *Journal of Lightwave Technology*, **37**, 722-728 (2018).

30. S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Sham-sul Shara, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villloresi, and P. Wallden. Advances in quantum cryptography. *Advances in Optics and Photonics*, **12**, 1012-1236 (2020).

31. M. Ziari, et al. High-performance 100 Gbaud Coherent Photonics Modules. In *Optical Fiber Communication Conference (OFC)* (pp. F2A-3), Optical Society of America, (2021).

32. J. F. Tasker, J. Frazer, G. Ferranti, E. J. Allen, L. F. Brunel, S. Tanzilli, V. D’Auria, and J. C. F. Matthews. Silicon photonics interfaced with integrated electronics for 9 GHz measurement of squeezed light. *Nature Photonics*, **15**, 11 (2021).

33. L. Ruppert, V. C. Usenko, and R. Filip. Long-distance continuous-variable quantum key distribution with efficient channel estimation. *Physical Review A*, **90**(6), 062310 (2014).

34. B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Physical Review X*, **5**, 041009 (2015).

35. D. B. S. Soh, C. Brif, P. J. Coles, N. Luetkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar. Self-referenced continuous-variable quantum key distribution protocol. *Physical Review X*, **5**, 041010 (2015).
36. D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Optics Letters*, **40**, 3695 (2015).

37. A. Marie and R. Alleaume. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Physical Review A*, **95**, 012316 (2017).

38. F. Laudenbach, B. Schrenk, C. Pacher, M. Hentschel, C. H. F. Fung, F. Karinou, A. Poppe, M. Peev, and H. Hubel. Pilot-assisted intradyne reception for high-speed continuous-variable quantum key distribution with true local oscillator. *Quantum*, **3**, 193 (2019).

39. S. Kleis, M. Rueckmann, and C. G. Schaeffer. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Optics Letters*, **42**, 1588 (2017).

40. S. Shapiro, and M. Wilk. An analysis of variance test for normality (complete samples). *Biometrika* **52**, 591-611 (1965).

41. F. Laudenbach, C. Pacher, C. H. F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walthier, and H. Hubel. Continuous-variable quantum key distribution with gaussian modulation—the theory of practical implementations. *Advanced Quantum Technologies*, **1**, 1800011 (2018).

42. J. Lodewyck, M. Bloch, R. García-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. *Physical Review A*, **76**, 042305 (2007).

43. B. Qi, L. L. Huang, L. Qian, and H. K. Lo. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Physical Review A*, **76**, 052323 (2007).

44. Q. D. Xuan, Z. Zhang, and P. L. Voss. A 24 km fiber-based discretely signaled continuous variable quantum key distribution system. *Optics express*, **17**, 24244-24249 (2009).

45. C. Wang, D. Huang, P. Huang, D. Lin, J. Peng, and G. Zeng. 25 MHz clock continuous-variable quantum key distribution system over 50 km fiber channel. *Scientific reports*, **5**, 1-8 (2015).

46. M. Rueckmann, and C. G. Schaeffer. 1 Gboud heterodyne continuous variable quantum key distribution over 26 km fiber. In *Conference on Lasers and Electro-Optics (CLEO)* (pp. 1-2), IEEE, (2019).

47. Y. Zhang, Z. Li, Z. Chen, C. Weedbrook, Y. Zhao, X. Wang, Y. Huang, C. Xu, X. Zhang, Z. Wang, M. Li. Continuous-variable QKD over 50 km commercial fiber. *Quantum Science and Technology*, **4**, 035006 (2019).

48. X. B. Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical Review Letters*, **94**, 230503 (2005).

49. H. K. Lo, X. F. Ma, and K. Chen. Decoy state quantum key distribution. *Physical Review Letters*, **94**, 230504 (2005).

50. Y. Cao, S. Yu, J. Shen, W. Gu, and Y. Ji. Frequency estimation for optical coherent mpsk system without removing modulated data phase. *IEEE Photonics Technology Letters*, **22**, 10 (2010).

51. D. C. Chu. Polyphase codes with good periodic correlation properties. *IEEE Transactions on Information Theory*, **18**, 531-532 (1972).

52. A. Leverrier, R. Alléaume, J. Boutros, G. Zemor, and P. Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Physical Review A*, **77**, 042325 (2008).

53. P. Jouguet, S. Kunz-Jacques, and A. Leverrier. Long-distance continuous-variable quantum key distribution with a gaussian modulation. *Physical Review A*, **84**, 062317 (2011).

54. C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, **4**, 711–715 (2010).

55. X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang. Quantum random number generation. *Npj Quantum Information*, **2**, 1-9 (2016).

Acknowledgements

This work is supported by the National key research and development program (Grant No. 2016YFA0302600), National Natural Science Foundation of China (Grants No. 62101320, 61671287, 61971276), Shanghai Municipal Science and Technology Major Project (Grant No.2019SHZDZX01), and the Key R&D Program of Guangdong province (Grant No. 2020B030304002).

Author contributions

G.Z. conceived the research. T.W. and P.H. contributed equally to this work. T.W. and L.L. carried out the experiment. T.W. and P.H. analyzed the data and wrote the manuscript. Y.Z. provided the technical support for post processing and QRNG. All authors contributed to the data collection, discussed the results and reviewed the manuscript.

Competing interests

The authors declare no competing interests.
**Additional information**

Supplementary Information accompanies this paper at https://doi.org/.

Reprints and permission information is available online at http://npg.nature.com/reprintsandpermissions/

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SupplementaryMaterial.pdf