Experimental continuous-variable quantum key distribution using a thermal source

Peng Huang1,2,∗, Tao Wang1,2, Rui Chen1, Ping Wang1, Yingming Zhou3 and Guihua Zeng1,2

1 State Key Laboratory of Advanced Optical Communication Systems and Networks, Center for Quantum Sensing and Information Processing, Shanghai Jiao Tong University, Shanghai 200240, People’s Republic of China
2 Shanghai Research Center for Quantum Sciences, Shanghai 201315, People’s Republic of China
3 Shanghai XunTai Quantech Co., Ltd, Shanghai, 200241, People’s Republic of China

∗ Author to whom any correspondence should be addressed.
E-mail: huang.peng@sjtu.edu.cn

Keywords: continuous-variable quantum key distribution, thermal state, passive-state-preparation

Abstract
Gaussian-modulated coherent-state (GMCS) continuous-variable quantum key distribution (CVQKD) protocol can allow authenticated users to share secret key with unconditional security. So far, all previous experimental implementations of GMCS CVQKD schemes are based on active modulations, i.e. amplitude and phase modulators and quantum random number generator (QRNG) are required. However, high-speed modulation with high extinction ratio and stability is challenging, which is extremely remarkable in chip-scale silicon photonic realization. While the passive-state-preparation (PSP) CVQKD scheme, which explores the intrinsic field fluctuations of a thermal source, avoids the uses of active modulations and QRNG. In this paper, we experimentally realize the intact PSP CVQKD through a realistic optical fiber channel using off-the-shelf amplified spontaneous emission source. In particular, specially designed frame synchronization method is used to build the correlation between the data measured from the two legitimate parties, and excess noise are synthetically controlled to generate secure secret keys at the metro-area distances when considering the practical and non-negligible finite-size effects under collective Gaussian attacks. Due to the avoidance of modulators and QRNG, the passive state encoding scheme provides a promising direction of applicable high-speed, chip-based and even sunlight-based CVQKD with less cost and complexity.

1. Introduction

Continuous-variable quantum key distribution (CVQKD) [1–4] provides an efficient way for two remote authenticated users to share secure key through untrusted quantum channels and authenticated classical channels by using coherent source and detection. In particular, the secret keys are always encoded on the quadrature values [2, 5, 6] or the quadrature choices [7] of the quantized electromagnetic field of coherent states, which are measured by the coherent detections, i.e. homodyne or heterodyne detector. Since the intrinsic filtering characteristic of the local oscillator (LO) in coherent detection can extremely suppress the background noise, CVQKD can be a cost-effective solution with already deployed classical optical communication infrastructures and could achieve high secure-key rates especially over relatively short distances. In addition, the ideal implementation of CVQKD can approximately reach the ultimate limit of secret key capacity of repeaterless quantum communication, i.e. the PLOB bound [8].

Nowadays the Gaussian-modulated coherent-state (GMCS) CVQKD protocol [2] has been theoretically proved to be secure against arbitrary collective attacks [9] and coherent attacks [10], when even considering the finite-size effects [11–16]. Moreover, this protocol has been experimentally realized both in laboratory [3, 17–20] and field tests [21–24], which has been demonstrated its superior applicability in metropolitan area quantum networks. In these implementations, the encoded quantum states are usually
prepared actively using amplitude and phase modulations, i.e. Alice first generates Gaussian-distributed random numbers $x_A$ and $p_A$, and then performs amplitude and phase modulations on the source state with these random numbers in order to prepare the coherent states $|x_A + ip_A\rangle$. However, high-speed modulation with high extinction ratio and stability in realistic condition is challenging, which is even serious in chip-scale silicon photonic implementation. Moreover, the high-speed on-chip modulators in the active CVQKD scheme induce significant cost, manufacturing time, implementation complexity and contribute natural loss in most integrated photonic circuits [25].

In order to overcome these shortcomings, one efficient way is adopting the passive-state-preparation (PSP) CVQKD scheme [26], where the amplitude and phase modulators and quantum random number generator (QRNG) used for encoding are removed and replaced by a thermal source, beam splitters, optical attenuators, and homodyne detectors. It is shown in reference [26] that the PSP CVQKD scheme explores the intrinsic quadrature fluctuations of a thermal state, which is equivalent to the GMCS CVQKD when the transmitter in Alice’s station is trusted. So the well-established security proofs for GMCS CVQKD can be directly applied to the PSP scheme. Recently, a noise model for the PSP CVQKD scheme is developed, and it is further verified experimentally by using an off-the-shelf amplified spontaneous emission source (ASE) [25], which suggests the feasibility of secure key generation over metro-area distances. However, the full demonstration of secure key distribution over the realistic fiber channel has not been realized yet, even without considering the practical and non-negligible finite-size effects. The main obstacles lie in robust frame synchronization without special-frame-based methods, and the suppression of excess noise arising from the polarization and phase drifts when passive-preparation quantum states are transmitting over realistic fiber channel. Meanwhile, the limited interference stability for thermal states also restricts the length of the raw key data block, which will lead to intense finite-size effects [11] and thus quite increase the excess noise.

In this paper, we experimentally realize the intact PSP CVQKD for the first time over a 5.005 km standard single-mode-fibre spool with a loss of 0.2 dB km$^{-1}$ with an off-the-shelf ASE source. In particular, frame phase compensation and specially designed frame synchronization method are used to suppress the excess noise and thus build the correlation between the two legitimate parties. Finally, with the consideration of finite-size effects under collective Gaussian attacks, the secure secret keys are generated with 9.3 Mbps at Alice and Bob’s sides by applying a high-efficiency reconciliation method based on slice-type polar codes. Since the required amplitude and phase modulators and QRNG are replaced with simple and cheap devices, the passive state encoding scheme provides a promising direction of applicable high-speed and chip-based CVQKD with less complexity and cost. It is anticipated that even the natural and perfect thermal light, i.e. the sunlight, may be directly explored to realize the quantum cryptography communication.

2. Experimental results and discussion

2.1. Protocol and setup

PSP CVQKD protocol [26] can be simply implemented using the intrinsic field fluctuations of a thermal source, which can be schematically depicted in figure 1. Firstly, Alice splits the output of a thermal source into two spatial modes. One is attenuated with Att$_1$ and then sent to Bob, while the other will be locally measured by Alice using heterodyne detection (here Att$_2$ denotes the local loss in Alice’s signal channel). Secondly, Bob performs heterodyne detection on the incoming quantum states transmitted from Alice, and obtains the values of quadratures $X$ and $P$. Thirdly, after frame synchronization and excess noise
suppressing operations, Alice and Bob further perform parameter estimation through the authenticated classical channel to upper bound the secret key information that the potential eavesdropper could gain. Finally, Alice and Bob perform reconciliation and privacy amplification to extract a string of secure secret key.

Actually, we can see except the first step where the Alice’s key information is obtained by heterodyne detection, the other steps are same with the conventional GMCS CVQKD protocol. In the PSP CVQKD scheme, Alice can scale down her measurement results by a factor thus to optimize the estimation of the quadrature values of the outgoing mode. Since the quadrature values in Alice’s side is obtained by an imperfect heterodyne detection in PSP scheme rather than the fixed value directly generated by QRNG, Alice’s minimum uncertainty on the quadrature of the outgoing mode will be larger than one [25]. This leads to extra excess noise in quantum state preparation step (see appendix A for more details), which is always classified as the untrusted noise as

\[ \varepsilon_s = \frac{2V_A \eta_A (\nu_\text{el} + 1)}{V_A \eta_B (\nu_\text{el} + 1)} \]

where \( V_A = n_0 \eta_A \) is the modulation variance with \( n_0 \) the average photon number of the prepared thermal source.

Therefore, Alice can adjust the source intensity and transmittance \( \eta_A \) of Att1 to set a desired quadrature variance \( V_A \) of the outgoing mode. So from the viewpoint of an eavesdropper, she cannot distinguish the quantum state sent in PSP CVQKD from the one in active GMCS CVQKD (preparation-and-measurement scheme or entanglement-based scheme), and the theoretical securities of these CVQKD schemes are equivalent, i.e. the unconditional security of the PSP CVQKD can be guaranteed. Here the coherent detections provide the mode-selective capability to distill the intrinsic randomness of a thermal key. It is shown in references [27–29] that the extra noise introduced by the mismatched modes of thermal light can be negligible due to the suppressing effect of strong LO.

The secret key rate can therefore be calculated as [11]

\[ R = f \frac{n(1-\alpha)}{N} (1-\text{FER})[\beta I_{\text{AB}} - \chi_{\text{BE}} - \Delta(n)] \]

where \( f \) is the repetition rate, \( I_{\text{AB}} \) is the classical mutual information between Alice and Bob, \( \chi_{\text{BE}} \) is the Holevo bound on the information leaked to Eve in the finite-size regime, \( \beta \) is the reconciliation efficiency, FER is the frame error rate of the reconciliation, \( \Delta(n) \) is an offset term due to privacy amplification in the finite-size regime, \( \alpha \) is the overhead for phase drift reference and frame synchronization, \( n \) and \( N \) denotes the block length for final key distillation and the whole sampling length, respectively.

The experimental setup is shown in figure 2. In order to generate a high-intensity broadband thermal source, a fiber amplifier work in continuous-wave (CW) mode with a commercial ASE source (Golight) input is employed. A nominal 0.4 nm optical band-pass filter centred at 1549.72 nm with polarization-maintaining (PM) fiber is applied to reduce the power of unused light and select out a single polarization mode after the fiber amplifier. The property of the filtered thermal source is tested, and the polarization-maintaining (PM) fiber is applied to reduce the power of unused light and select out a single input is employed. A nominal 0.4 nm optical band-pass filter centred at 1549.72 nm with 100 Hz line width

The modulation variance is set accurately through VOA in the experiment. In theory, the optimal modulation variance is directly related to the transmittance of the optical attenuator \( \eta_A \) and the average photon number of the thermal source \( n_0 \) with equation \( V_A = \eta_A n_0 \). When \( n_0 \) is fixed for a specific thermal source, decreasing \( \eta_A \) will lead to smaller extra excess noise \( \varepsilon_s \) in Alice’s quantum state preparation step. But meanwhile it will also lead to smaller modulation variance and thus decrease the secret key rate. So here according to the intensity of the used thermal source, we set \( V_A = 4 \) for optimal consideration.

After adjusted by the polarization controllers, the filtered thermal signals are measured by Alice and Bob with heterodyne detections, respectively. Here the heterodyne detection is implemented by a 90° optical
hybrid (Optoplex) and two balanced homodyne detectors (Thorlabs), and Bob’s LO is directly split from Alice’s LO source for simplicity. While for practical applications, it is preferable to generate Bob’s LO locally [30–32], especially for long-distance transmissions. The outputs of the four balanced homodyne detectors are sampled by a real time oscilloscope. To simply achieve cursory frame synchronization of the simultaneously sampled data with one oscilloscope, a same 5.005 km SMF spool with ±100 m of length deviation is added here in Alice’s thermal light transmission channel. It should be mentioned that this extra spool is not necessary when Alice and Bob use independent data sampling modules and calibrate the transmission delay.

2.2. Synchronization and excess noise suppression

In our experiment, to optimize the interference of the filtered thermal light and LO, an AM is used to cut the filtered thermal light into pulses so as to adjust and verify the interference (while there exist coherent peaks in pulses). Specifically, in the preparation stage, the filtered thermal light is transformed into a 5 MHz clock square pulse train by an AM in pulse modulation. Then in the key generation stage, Alice and Bob execute the PSP CVQKD protocol, where both the broadband thermal source in Alice’s and Bob’s side and the LO are operated in CW mode (disable the AM), and a 13 GHz bandwidth real-time oscilloscope is employed to sample the outputs of Alice’s and Bob’s balanced homodyne detectors at 5 GS s\(^{-1}\) rate. Here four homodyne detectors are selected with the same quantum efficiencies \( \eta_a(b) = 0.6 \) and electronic noises \( \nu_{el} = 0.25 \) in shot noise units (SNU). The quantum efficiencies and electronic noises are calibrated before the key distribution experiment. Quantum efficiencies \( \eta_D^{(a(b)} = 0.6 \) are contributed by the PC with a 0.4 dB insert loss, the 90° optical hybrid with 0.8 dB, and the balanced homodyne detector with 1 dB. Electronic noises are calibrated through the sampled data with the disconnected LO. Moreover, the SNU is calibrated in real time by randomly switching off the signal path to prevent the possible side-attacks on transmitting LO [33, 34]. It should be mentioned here that by using the interference operation in CW mode, we can extract as much raw key data as possible during the finite stable period to perform parameter estimation and key generation, thus relieving the finite-size effects. However, limited by the finite bandwidth of the homodyne detectors, the raw key data should be down-sampled with the rate not higher than the bandwidth of homodyne detectors, which to some extent restricts the block length. Fortunately, the development of high-bandwidth homodyne detectors [35] can resolve this problem.

Precise frame synchronization is necessary for Alice and Bob to generate final key. However, the conventional frame synchronization schemes for CVQKD require active modulation devices to construct special frames, which is technically impossible for PSP CVQKD schemes. So precise frame synchronization for PSP scheme is a very challenging problem. Here a novel robust synchronization algorithm is specially designed and is applied without using specially modulated frames, but just with some of the shared measurement results of heterodyne detections, i.e. the random values of quadratures \( X \) and \( P \), even when intense phase drifts exist or at a low signal-to-noise (SNR) ratio [36]. Especially, a new feature based on labelling is designed to tolerate phase shifts and synchronize in a strong noise environment. See appendix C for more details about the frame synchronization scheme. After the frame synchronization process, the sampled raw data in Alice and Bob’s sides are then directly correlated. Figure 3 shows the relationship of raw data of Alice’s and Bob’s x-quadrature measurement results with and without channel losses of two 5.005 km SMF spools. It can be seen from the raw data that the correlation between Alice’s and Bob’s data is barely visible for the low loss channel.

By changing the output power of ASE, pump power of the fiber amplifier, and the attenuation of VOA, we can adjust the average photon number of the filtered thermal light \( \bar{n}_0 \), and then control the excess noise due to the passive state preparation to \( \varepsilon_s = 0.0349 \) SNU based on the evaluation of equation (A5). In order
Figure 3. The raw data of Alice’s and Bob’s x-quadrature measurement results (a) without (and no optical attenuation is applied, i.e. $\eta_A = 1, \eta_s = 1$) and (b) with channel losses (and optical attenuation is applied, i.e. $\eta_A = 0.0067, \eta_s = 0.7925$).

Figure 4. Experimental excess noise measured with a SNR of 1.488 on Bob’s side. The lower blue circle points are measured at 5.005 km with $1 \times 10^5$ finite-size blocks. The effective excess noise under worst-case estimator (orange square point) is employed to compute the final secret key rate. The red solid line defines the tolerable maximal value of excess noise at 5.005 km. The dashed and dotted lines are the average experimental excess noise and the worst-case excess noise estimator at the channel input, respectively.

to further control the excess noise due to mode mismatching through the lossy and noisy channel, frame phase compensation is performed to improve the data correlation. In particular, approximate 40% random points are announced to estimate the phase drift for phase compensation. See appendix D for more details about the frame phase compensation. In theory, the residual phase excess noise can be completely eliminated by the frame phase compensation for relatively slow phase drift. However, in practical situations, phase compensation in one frame may be not so precise due to other reasons, such as the resident depolarization drift and source-intensity fluctuation and so on. So this frame phase compensation does not exclude all of the phase noise, but the actual residual phase noise can be low enough to meet the requirement of key extraction in the experiment.

The experimental excess noises measured with 40 raw data blocks of length $1 \times 10^5$ for a distance of 5.005 km are shown in figure 4. After confirming the average excess noise due to passive state preparation, we perform maximum-likelihood estimations just for the channel parameters when considering the finite-size effects. The corresponding confidence intervals are calculated to bound their values with 6.5 standard deviations. For each data point, a worst-case estimator of the excess noise compatible with the experimental data is also indicated. Moreover, the average experimental excess noise and the worst-case excess noise estimator at the channel input are obtained as 0.0664 and 0.1056 in SNU, respectively.

2.3. Secret-key distillation

Here highly efficient post-processing is needed to distill secure secret key, especially for high excess noise. Fortunately, for the low-loss quantum channel, we can control the SNR ratio to be larger than 1 by using relatively high modulation variance. So here we can use slice reconciliation algorithm, which is very suitable for efficient reconciliation under high SNR [37]. The polar codes with a relatively short length of $10^5$ at each level are sufficient to achieve reconciliation efficiencies above 90% over a wide range of SNR. It can be
Table 1. Key experimental parameters of PSP CVQKD scheme. $\epsilon$, average measured excess noise at the channel input in SNU; $P_{LO}$, output power of LO in CW-mode.

| $V_s$ | $\epsilon$ | $\epsilon_s$ | $\eta^{(b)}$ | $\eta_d$ | SNR | $\alpha$ | $\beta$ | FER | $n$ | $N$ | $P_{LO}$ | $f$ |
|-------|-------------|-------------|-------------|----------|------|---------|-------|-----|-----|-----|---------|-----|
| 4     | 0.0664      | 0.0349      | 0.6         | 0.25     | 1.488| 0.4     | 0.94  | 0.30| $4 \times 10^5$| $5 \times 10^5$| 14.8 dBm | 350 MHz |

Figure 5. Experimental key rates and numerical simulations. The square point corresponds to the experimental result at transmission distance of 5.005 km. The blue solid curve show the simulated secret key rates calculated from the estimated parameters in experiment. The dashed, dotted and dash-dotted curves shows the theoretical secret key rates when considering finite-size effects with different data blocks, respectively.

found from figure 4 that the finite-size effects quite affect the estimated excess noise and thus the performance. Moreover, the fluctuations of the excess noises for different data blocks illustrate the limited stability of the setup, such as the remained relative phase fluctuation due to the uncertainty of passive state preparation, the variations of the intensity of thermal source and the polarization drifts through fiber channel.

It should be mentioned that we just adopt frame phase compensation and passive manual polarization control to suppress the excess noise here, since we mainly focus on the demonstration of the intact implementation of PSP CVQKD. Actually, several data blocks reveal very low excess noises, which illustrates the huge potential improvements of secret key rate and secure transmission distance. Here we use the worst-case scenario to evaluate Eve’s Holevo bound and the secret key rate. The overview of key experimental parameters is shown in table 1.

The simulated secret key rate based on equation (2) and the experimental secret key generation results are shown in figure 5 (see appendix E for more details about the security analysis and secret-key-rate calculation). Limited by the 350 MHz bandwidth of the homodyne detectors, we perform down-sampling of the raw data with 350 MHz rate, and the equivalent repetition rate for the CW-mode communication in our experiment is then also 350 MHz. The secret key rate is 9.3 Mbps over 5.005 km SMF, and the secure transmission distance is 10.2 km. To further increase the secret key rate, one straightforward method is to improve the data sampling rate and use homodyne detectors with a larger bandwidth. For instance, the secret key rate can be roughly evaluated more than 230 Mbps when using 9 GHz homodyne detectors [35] for 10 GHz sampling rate. Nevertheless, a detector with higher bandwidth tends to have higher electrical noise which may slightly reduce the secret key rate in practice. In addition, removing the attenuation of Alice’s local 5.005 km SMF spool will decrease the excess noise due to the passive state preparation. Moreover, larger data block will reduce the finite-size effects and enable higher reconciliation efficiency, thus further improve the secret key rate.

3. Conclusion

We have demonstrated the first intact PSP CVQKD experiment through a realistic optical fiber channel by applying specially designed frame synchronization algorithm to build direct correlation between the two sets of Alice’s and Bob’s measurement results and controlling the excess noise. In particular, we use a high-intensity thermal source, employ a narrow-band optical filter, and perform frame phase compensation.
and passive polarization control to synthetically suppress the excess noise induced in the whole communication including the passive state preparation stage. The secret key rate is 9.3 Mbps with the worst-case estimator over 5.005 km standard optical fiber when finite-size effects are taken into account.

Since the raw key data for Alice and Bob are all obtained from the heterodyne detections of the thermal states. The instability of the setup can be all basically attributed to the interference instability in Alice’s and Bob’s stations. It is anticipated that improvement of stability with active polarization and phase compensations, and optimization of thermal source and modulation variance, will enhance the correlations between Alice and Bob, thus further decreasing the measured excess noise. In particular, since the equivalent repetition rate here is limited to 350 MHz, the stable duration for generating a raw data block of length $5 \times 10^5$ is just approximately millisecond level. So improving the interference stability of the PSP CVQKD setup or bandwidth of homodyne detection will all lead to linear increase of the length of raw data blocks for key generation, and thus decrease the excess noise due to finite-size effects. Actually, the existence of low excess noises in the data blocks reveals the realistic probability of further suppression of excess noise, which enables the PSP CVQKD with higher secret key rate and longer secure transmission distance.

It should be mentioned that one may concern the randomness from the thermal source, since it is common to apply a QRNG in the active CVQKD. The illustrations in references [25, 38] show that true randomness can be trusted as long as the eavesdropper Eve cannot access (or control) the thermal source. This can be fully guaranteed because it is a common and reasonable assumption in security proof of CVQKD. Our experiment verifies the practical ability of secure key generation for PSP CVQKD over metro-area distances, which provides an appealing way to implement high-speed, chip-based and even sunlight-based CVQKD with less cost and complexity.

**Acknowledgments**

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

**Data availability statement**

The data generated and/or analysed during the current study are not publicly available for legal/ethical reasons but are available from the corresponding author on reasonable request.

**Author contribution**

PH and TW contributed equally to this work.

**Appendix A. Excess noise analysis in passive-state-preparation scheme**

The noise model of the experimental PSP CVQKD scheme is based on the one proposed in references [25, 26], which could be constructed as follows.

For simplicity, only the quadrature $X$ is considered below. The quadrature $P$ can be considered in the same model. From the depicted model shown in figure 6, we can get the mode sent by Alice after passing through the attenuator will be

$$x_1 = \sqrt{\frac{\eta_A}{2}} x_s - \sqrt{\frac{\eta_A}{2}} x_{v1} - \sqrt{1 - \eta_A} x_{v3}, \quad (A1)$$

where $x_s$ is the $X$-quadrature of the output mode of the thermal source, $\eta_A$ is the transmittance of the optical attenuator, $x_{v1}$ and $x_{v3}$ are the vacuum noise introduced by BS$_1$ and the attenuator. For the vacuum noise, $\langle x^2_{v1} \rangle = \langle x^2_{v3} \rangle = 1$. We assume the average photon number of the thermal source is $n_0$, then the average photon number sent to Bob is $\eta_A n_0 / 2$. Thus the modulation variance $V_A$ which is equivalent to the one in GMCS CVQKD scheme can be calculated as

$$V_A = \eta_A n_0, \quad (A2)$$
Figure 6. The excess noise model for passive state preparation. BS_{1(2)}, 50:50 beam splitter; Att_{1}, optical attenuator; Att_{2}, the equivalent optical attenuator of the used 5.005 km optical fiber in Alice’s signal channel; Hom, homodyne detector.

Similarly, the X-quadrature measured by Alice can be expressed as

\[
x_{A} = \sqrt{\frac{\eta_{s}}{2}} x_{s} + \sqrt{\frac{\eta_{a} \eta_{D}}{2}} x_{v1} - \sqrt{(1 - \eta_{s}) \eta_{a} \eta_{D}} x_{v4} - \sqrt{\eta_{a} \eta_{D}} x_{v2} - \sqrt{1 - \eta_{s}} x_{vd} + x_{De},
\]

where \( \eta_{s} \) is the transmittance of the equivalent optical attenuator Att_{2} before homodyne detections in Alice’s other signal path, \( \eta_{a} \eta_{D} \) is the efficiency of Alice’s homodyne detector, \( x_{v2} \) denotes the vacuum noise introduced by BS_{2}, \( x_{v4} \) denotes the vacuum noise introduced by the equivalent optical attenuator Att_{2}, \( x_{vd} \) represents the vacuum noise introduced by Alice’s detector, and \( x_{De} \) represents the electrical noise of Alice’s detector. Also \( \langle x_{v2}^2 \rangle = \langle x_{v4}^2 \rangle = 1 \). According to the agreement, Alice multiplies the measurement results by the correction factor \( \alpha_{A} \) to estimate the quadratures sent to Bob. Here \( \alpha_{A} = \langle x_{A} x_{1} \rangle / \langle x_{A}^2 \rangle \), which can be deduced as

\[
\alpha_{A} = \frac{\nu_{el} \sqrt{2 \eta_{A} \eta_{s} \eta_{D}}}{\nu_{el} \eta_{s} \eta_{D} + 2 \nu_{el} + 2},
\]

where \( \nu_{el} = \langle x_{De}^2 \rangle \) represents the variance of electrical noise of Alice’s homodyne detector. Therefore, the excess noise \( \varepsilon_{s} \) due to passive state preparation can be calculated as

\[
\varepsilon_{s} = \langle (x_{1} - \alpha_{A} x_{A})^2 \rangle - 1 = \frac{2 V_{A} \eta_{A} (\nu_{el} + 1)}{V_{A} \eta_{s} \eta_{D} + 2 \eta_{h} (\nu_{el} + 1)}.
\]

It can be found that we can increase \( \eta_{s} \), decrease \( \eta_{A} \) and optimize the modulation variance to reduce the excess noise due to passive state preparation. In practice, the measured modes by Alice and Bob may not be perfectly overlapped, which are determined by the modes of Alice’s and Bob’s LOs after the transmission of the thermal state. So the mode mismatch will induce untrusted excess noise. Moreover, the noisy and lossy quantum channel will also introduce additional excess noise.

Here we can use the known parameter estimation procedure to evaluate the total excess noise for each communication cases based on the shared raw key data. And also the excess noise due to passive state preparation can be calculated with equation (A5). Once the excess noise in the source is obtained, we can set it as a fixed value of untrusted excess noise. Then we can attribute the other excess noise as the untrusted one like the channel excess noise, whereby the worst-case estimator of the excess noise can be evaluated, which is further applied to calculate the secret key rate.

Appendix B. Thermal source characterization

In our experiment, the centre wavelength of LO laser is carefully turned close to the centre wavelength of optical band-pass filter by adjusting the bias current. It should be noted that the wavelength of LO laser can never drift out 0.4 nm range under normal operation, which is centred at 1549.72 nm, and the line width of the used LO laser is 100 Hz.
Before distributing quantum secret key, we firstly test the characteristics of the filtered thermal source. In particular, we here use the sampled data of Alice’s measurement outcomes to perform the analysis. Figure 7 shows the distributions of the measurement results with thermal input and vacuum input, where the efficiencies and electronic noise of Alice’s two homodyne detectors are both 0.6 and 0.25, respectively. By normalizing the quadrature variances of the thermal state to the Alice’s vacuum noise, the average photon number (per mode) of the filtered thermal state can be evaluated as 597, where the attenuation efficiency is $\eta_A = 0.0067$. Since we apply CW-mode signal and high-bandwidth sampling in our experiment, the average photon number per mode here can be seen as averaging based on the response time of used homodyne detectors with limited bandwidth.

The two-dimensional histogram of Alice’s measured data is shown in figure 8 when inputting the thermal source. The small deviation from a perfect two-dimensional Gaussian distribution is most likely due to the nonuniform bin size of the analog-to-digital converter of the oscilloscope. The single-time second-order correlation function $g^{(2)}(0) = \frac{\langle Z^2 \rangle - 4 \langle Z \rangle^2 + 2}{\langle Z \rangle^2}$ for $Z = X^2 + P^2$ is calculated to be 2.0179, which indicates that the thermal source is very close to the value of 2 for a perfect thermal source.
Appendix C. Robust frame synchronization

The synchronization algorithm should work well at low SNR situations and tolerate phase shifts. After the heterodyne detection (the conjugate homodyne detection), the sender Alice and receiver Bob share some values of the quadratures $X$ and $P$. Here we use a specially designed frame synchronization algorithm [36], where parts of the output of detection are directly regarded as synchronization frames. Then a transformation is performed on these quadratures and every value of the output strings is assigned a label.

This labelling process will output a random number sequence $X$ which can be expressed as $(x_1, x_2, \ldots)$ into a binary sequence $Y(y_1, y_2, \ldots)$ by the rules: step 1, sum the next $L$ numbers of the current position, such as $x_{i+3}, x_{i+4}$ for current position $x_{i+2}$ and $L = 2$. Then subtract the sum of the former $L$ numbers, the output is used as a descriptor. And we call the $2L + 1$ interval an transformation unit. Step 2, we first set a threshold $V_0$, which is usually the modulation variance. If $\sum_{i=0}^{L} x_i - \sum_{j=0}^{L-1} x_j > V_0$, we mark this position with symbol ’1’ ($y_1 = 1$). If $\sum_{i=0}^{L} x_i - \sum_{j=0}^{L-1} x_j < V_0$, we mark this position with symbol ’0’ ($y_1 = 0$). After marking all the received signals, the synchronization process begins. Every successive $N$ bits of conversion sequence $Y$ are seen as a feature, and we can calculate the hamming distance of the two signal sequences to measure their similarity. It should be mentioned that noise with zero expectation will be suppressed and their impact on synchronization is weaken. We can see this transformation method is simple and efficient.

In order to compete with phase drifts, the sender Alice can prepare four transformation sequences of her synchronization frames, which contain binary sequences $TX_A$ and $TP_A$ and their complements. Firstly, Alice generates the binary sequences $TX_A$ and $TP_A$ by using the rules listed in steps 1 and 2 with the sequences of quadratures $x_A$ and $p_A$, respectively. Then their complements $\overline{TX_A}$ and $\overline{TP_A}$, can be directly obtained by using a not operator. For example, if $TX_A$ is ’0101’, then $\overline{TX_A}$ is ’1010’, the rules are same for $TP_A$ and $\overline{TP_A}$.

Bob also transforms the sequences with the received quadratures $x_b$ (or $p_b$) with the same rules. After the sequence transformations, the similarity can be measured by calculating the hamming distance between the transformed sequences of Alice’s synchronization symbols and every segments of Bob’s received signal. We should make the cost function reach its peak value when synchronization succeed, the cost can be rewritten $D(TX_A, TX_B) = n - H(TX_A, TX_B)$, where $H(X_1, X_2)$ means similarity of sequences $X_1$ and $X_2$, and $H(X_1, X_2)$ means hamming distance of $X_1$ and $X_2$. Here we define a new function,

$$ F(A, B) = \max \left[ D(TX_A, TX_B), D(\overline{TX_A}, TX_B), D(TP_A, TX_B), D(\overline{TP_A}, TX_B) \right]. \quad (C1) $$

The location of synchronization is just where the function $F(A, B)$ reaches its peak value.

The following synchronization scheme can then be performed based on this feature; step 1, Alice (the sender) selects parts of the random strings as the synchronization frame; step 2, Alice transforms the selected sequences into 0–1 sequences by the incremental label algorithm proposed above. Both $x$ and $p$ components must be transformed. Then we get two 0–1 sequences $TX_A$ and $TP_A$; step 3, Alice publishes the two 0–1 sequences $TX_A$ and $TP_A$ through classical channel; step 4, Bob transforms $x_b$ (or $p_b$) into 0–1 sequences by the incremental label algorithm, and matches them to the received two 0–1 sequences $TX_A$ and $TP_A$ bits by bits. Then he calculates the function $F(A, B)$; step 5, Alice and Bob synchronize at the position where the function $F(A, B)$ reaches its peak value.

Appendix D. Frame phase compensation

The purpose of phase compensation is to align the phase reference coordinate of Alice and Bob. In the practical fiber link, due to the fluctuation of the transmission path length, the optical waveform that reaches the detector of Alice and Bob changes with time, which in turn causes the phase reference coordinate at both ends inconsistent, hindering the extraction of secret key. Considering that the optical path changes relatively slowly during transmission, the relative phase drift in a frame with a relatively high-repetition rate can be assumed constant. Therefore, a random part of the data is disclosed in one frame and estimate the relative phase drift value through cross-correlation calculation with Alice, and then use this value to compensate Alice’s data. The specific operation includes the following steps: step 1, disclose a part of Alice’s data $(x_A, p_A)$ and the corresponding Bob’s data $(x_B, p_B)$. Set the phase drift estimator $\theta_0$ and calculate the cross-correlation value of the Alice and Bob components based on the above data, namely,

$$ K = \sum_{i=0}^{n} x_{ABi} \times x_{Bi}, \text{ where } x_{ABi} = \exp([x_A + jp_A] \times \exp(j\theta_0))] $$

is the preset phase rotation of Alice’s data; step 2, traverse $\theta_0$ from 0 to $2\pi$ to get the relationship between $K$ and $\theta_0$; step 3, find the maximum value of $K$ and the corresponding $\theta_0$, which is the optimal phase drift estimator. Use this value to compensate for Alice’s undisclosed data, namely $x_{AC} + jp_{AC} = (x_A + jp_A) \times \exp(j\theta_0)$. The compensated data $(x_{AC}, p_{AC})$ are then used for final key distillation.

10
Appendix E. Security analysis and secret-key-rate calculation

Here in this paper, the security of the PSP CVQKD scheme basically follows from the references [25, 26], which show that the PSP CVQKD scheme is equivalent to the GMCS CVQKD protocol, but just with some additional excess noise in passive state preparation. As well known, the security of the GMCS CVQKD protocol has been theoretically proved to be secure against arbitrary collective attacks [9] and coherent additional excess noise in passive state preparation. As well known, the security of the GMCS CVQKD scheme from the one in active GMCS CVQKD (or even the entanglement-based CVQKD), so all three protocols are equivalent in terms of security [25, 26].

Actually, in the active GMCS CVQKD scheme, the raw key data $x_A$ and $p_A$ in Alice’s side are generated by a trusted QRNG, which are utilized to prepared the state $|x_A + ip_A⟩$. While in the PSP CVQKD scheme, the raw key data $x_A$ and $p_A$ are obtained by Alice’s local measurements on a split thermal source with the conjugate homodyne detection, where the intrinsic field fluctuations of a thermal source are applied [38].

Alice can then scale down the measurement results numerically with a factor $\alpha_A$ to estimate the quadrature values of the outgoing mode. So from Eve’s point of view, she cannot distinguish the quantum state sent in the PSP CVQKD scheme from the one in active GMCS CVQKD (or even the entanglement-based CVQKD), so all three protocols are equivalent in terms of security [25, 26].

To estimate $I_{AB}$ and $\chi_{BE}$, here we also adopt the realistic noise model under Gaussian and collective attacks as in references [25, 26], i.e. Eve cannot control the imperfections of Bob’s station, which is widely used in CVQKD experiments [17–20, 24]. When considering the asymptotic case, under this noise model, the mutual information between Alice and Bob $I_{AB}$ can be calculated as

$$I_{AB} = \log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}},$$

(E1)

where $V = V_A + 1$, and $\chi_{tot}$ representing the total noise referred to the channel input can be expressed as $\chi_{tot} = \chi_{line} + \chi_{het}/T$, in which $\chi_{line} = 1/T - 1 + \varepsilon$, and $\chi_{het} = [1 + (1 - \eta_B^2) + 2\nu_d]/\eta$. Here $T$ denotes the channel transmittance, $\eta_B^2$ and $\nu_d$ are the quantum efficiency and the electronic noise of Bob’s two homodyne detectors, respectively. Here the total untrusted excess noise $\varepsilon$, which refers to the average measured excess noise at the channel input in the experiment, is separated into terms $\varepsilon = \varepsilon_s + \varepsilon_c$, $\varepsilon_c$ represents the other sources of untrusted excess noise. And $\chi_{BE}$ is given by [17]

$$\chi_{BE} = \sum_{i=1}^{2} G \left( \frac{\lambda_i - 1}{2} \right) - \sum_{i=3}^{5} G \left( \frac{\lambda_i - 1}{2} \right),$$

(E2)

where $G(x) = (x + 1)\log_2(x + 1) - x \log_2 x$. $\lambda_i$ can be expressed as

$$\lambda_{1,2} = \frac{1}{2} \left( A \pm \sqrt{A^2 - 4B} \right),$$

$$\lambda_{3,4} = \frac{1}{2} \left( C \pm \sqrt{C^2 - 4D} \right),$$

$$\lambda_5 = 1,$$

(E3)

where

$$A = V^2(1 - 2T) + 2T + T^2(V + \chi_{line})^2,$$

$$B = T^2(V\chi_{line} + 1)^2,$$

$$C = \frac{1}{(T(V + \chi_{tot}))^2} \left[ A\chi_{het}^2 + B + 1 + 2\chi_{het}(V\sqrt{B} + T(V + \chi_{line})) + 2T(V^2 - 1) \right],$$

$$D = \left( \frac{V + \sqrt{B}\chi_{het}}{T(V + \chi_{tot})} \right)^2.$$ 

(E4)
When considering finite-size effects, the transmission efficiency $T$ and the excess noise $\varepsilon_c = \varepsilon - \varepsilon_s$ in equations (E1) and (E2) should be renewed as [11]

$$T' = \left(\sqrt{T} - z_{PE/2}/2\right)^2 \left(1 + T\varepsilon_c\right) \sqrt{(N - n)V_A}$$ \hspace{1cm} (E5)

$$\varepsilon'_c = \frac{\varepsilon_c + z_{PE/2} + (1 + T\varepsilon_c)}{\sqrt{N - n}} / T'$$

where $z_{PE/2}$ is such that $1 - \text{erf}(z_{PE/2}/\sqrt{2})/2 = \varepsilon_{PE/2}$, with erf the error function $\text{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x e^{-t^2} dt$, $\varepsilon_{PE}$ quantifies the failure probability of the parameter estimation. Moreover, $\Delta(n)$ is given by

$$\Delta(n) = 7\sqrt{\log_2(2/\bar{\varepsilon})} + 2n \log_2(1/\epsilon_{PA}),$$ \hspace{1cm} (E6)

where $\bar{\varepsilon}$ is a smoothing parameter, and $\epsilon_{PA}$ is the failure probability of the privacy amplification procedure. Here we set $z_{PE/2} = 6.5$, $\varepsilon_{PE} = \bar{\varepsilon} = \epsilon_{PA} = 10^{-10}$ as in reference [11] for typical values.

**ORCID iDs**

Peng Huang [https://orcid.org/0000-0003-1449-1499](https://orcid.org/0000-0003-1449-1499)

**References**

[1] Ralph T C 1999 Continuous variable quantum cryptography Phys. Rev. A 61 010303(R)
[2] Grosshans F and Grangier P 2002 Continuous variable quantum cryptography using coherent states Phys. Rev. Lett. 88 057902
[3] Grosshans F, Asche G V, Wenger J, Brosi U, Cerf N J and Grangier P 2003 Quantum key distribution using Gaussian-modulated coherent states Nature 421 238
[4] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 Gaussian quantum information Rev. Mod. Phys. 84 621
[5] Pirandola S, Mancini S, Lloyd S and Braunstein S L 2008 Continuous-variable quantum cryptography using two-way quantum communication Nat. Phys. 4 726–30
[6] Leverrier A and Grangier P 2009 Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation Phys. Rev. Lett. 102 180504
[7] Huang P, Huang J, Zhang Z and Zeng G 2018 Quantum key distribution using basis encoding of Gaussian-modulated coherent states Phys. Rev. A 97 042313
[8] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 Fundamental limits of repeaterless quantum communications Nat. Commun. 8 15043
[9] Navascués M, Grosshans F and Acín A 2006 Optimality of Gaussian attacks in continuous-variable quantum cryptography Phys. Rev. Lett. 97 190502
[10] Renner R and Cirac J I 2009 de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography Phys. Rev. Lett. 102 110504
[11] Leverrier A, Grosshans F and Grangier P 2010 Finite-size analysis of a continuous-variable quantum key distribution Phys. Rev. A 81 062343
[12] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks Phys. Rev. Lett. 109 100502
[13] Leverrier A, García-Patrón R, Renner R and Cerf N J 2013 Security of continuous-variable quantum key distribution against general attacks Phys. Rev. Lett. 110 030502
[14] Leverrier A 2017 Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction Phys. Rev. Lett. 118 200501
[15] Leverrier A 2015 Composable security proof for continuous-variable quantum key distribution with coherent states Phys. Rev. Lett. 114 070501
[16] Lupo C, Ottaviani C, Papanastasiou P and Pirandola S 2018 Continuous-variable measurement-device-independent quantum key distribution: composable security against coherent attacks Phys. Rev. A 97 052327
[17] Lodewyck J et al 2007 Quantum key distribution over 25 km with an all-fiber continuous-variable system Phys. Rev. A 76 042305
[18] Jouguet P, Kunz-Jacques S, Leverrier A, Grangier P and Diamanti E 2013 Experimental demonstration of long-distance continuous-variable quantum key distribution Nat. Photon. 7 378–81
[19] Huang D, Huang P, Lin D and Zeng G 2016 Long-distance continuous-variable quantum key distribution by controlling excess noise Sci. Rep. 6 19201
[20] Zhang Y, Chen Z, Pirandola S, Wang X, Zhou C, Chu B and Guo H 2020 Long-distance continuous-variable quantum key distribution over 202.81 km of fiber Phys. Rev. Lett. 125 010502
[21] Jouguet P et al 2012 Field test of classical symmetric encryption with continuous variables quantum key distribution Opt. Express 20 14030
[22] Huang D, Huang P, Li H, Wang T, Zhou Y and Zeng G 2016 Field demonstration of a continuous-variable quantum key distribution network Opt. Lett. 41 3511–4
[23] Karinou F et al 2018 Toward the integration of CV quantum key distribution in deployed optical networks IEEE Photon. Technol. Lett. 30 650
[24] Zhang Y et al 2019 Continuous-variable QKD over 50 km commercial fiber Quantum Sci. Technol. 4 035006

12
[25] Qi B, Gunther H, Evans P G, Williams B P, Camacho R M and Peters N A 2020 Experimental passive-state preparation for continuous-variable quantum communications Phys. Rev. Appl. 13 054065
[26] Qi B, Evans P G and Grice W P 2018 Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution Phys. Rev. A 97 012317
[27] Raymer M G, Cooper J, Carmichael H J, Beck M and Smithey D T 1995 Ultrafast measurement of optical-field statistics by dc-balanced homodyne detection J. Opt. Soc. Am. B 12 1801–12
[28] Semenov A A, Turchin A V and Gomomay H V 2008 Detection of quantum light in the presence of noise Phys. Rev. A 78 055803
[29] Wang S, Huang P, Wang T and Zeng G 2019 Feasibility of all-day quantum communication with coherent detection Phys. Rev. Appl. 12 024041
[30] Huang D, Huang P, Lin D, Wang C and Zeng G 2015 High-speed continuous-variable quantum key distribution without sending a local oscillator Opt. Lett. 40 3695–8
[31] Qi B, Lougovski P, Pooser R, Grice W and Bobrek M 2015 Generating the local oscillator ‘locally’ in continuous-variable quantum key distribution based on coherent detection Phys. Rev. X 5 041009
[32] Soh D B S, Brif C, Coles P J, Lütkenhaus N, Camacho R M, Urayama J and Sarovar M 2015 Self-referenced continuous-variable quantum key distribution protocol Phys. Rev. X 5 041010
[33] Ma X C, Sun S H, Jiang M S and Liang L M 2013 Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems Phys. Rev. A 88 022339
[34] Jouguet P, Kunz-Jacques S and Diamanti E 2013 Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution Phys. Rev. A 87 062313
[35] Tasker J F, Frazer J, Ferranti G, Allen E J, Brunel I F, Tanziilli S, D’Auria V and Matthews J C F 2020 Silicon photonics interfaced with integrated electronics for 9 GHz measurement of squeezed light Nat. Photon. 15 11–5
[36] Chen R, Huang P, Li D, Zhu Y and Zeng G 2019 Robust frame synchronization scheme for continuous-variable quantum key distribution with simple process Entropy 21 1146
[37] Van Assche G, Cardinal J and Cerf N J 2004 Reconciliation of a quantum-distributed Gaussian key IEEE Trans. Inform. Theory 50 394–400
[38] Qi B 2017 True randomness from an incoherent source Rev. Sci. Instrum. 88 113101