Long-distance continuous-variable quantum key distribution over 202.81 km fiber

Yichen Zhang¹, Ziyang Chen², Stefano Pirandola¹, Xiangyu Wang¹, Chao Zhou¹, Binjie Chu¹, Yijia Zhao¹, Bingjie Xu¹, Song Yu¹, and Hong Guo²†

¹State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China
²State Key Laboratory of Advanced Optical Communication Systems and Networks, Department of Electronics, and Center for Quantum Information Technology, Peking University, Beijing 100871, China
³Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, United Kingdom and
⁴Science and Technology on Security Communication Laboratory, Institute of Southwestern Communication, Chengdu 610041, China

(Dated: January 9, 2020)

Quantum key distribution (QKD) [1-3] provides secure keys resistant to code-breaking quantum computers. The continuous-variable version of QKD [1,4-6] offers the advantages of higher secret key rates in metropolitan areas, as well as the use of standard telecom components that can operate at room temperature [7-10]. However, the transmission distance of these systems (compared with discrete-variable systems) are currently limited and considered unsuitable for long-distance distribution [11]. Herein, we report the experimental results of long distance continuous-variable QKD over 202.81 km of ultralow-loss optical fiber by suitably controlling the excess noise and employing highly-efficient reconciliation procedures. This record-breaking implementation of the continuous-variable QKD doubles the previous distance record and shows the road for long-distance and large-scale secure QKD using room-temperature standard telecom components.

The BB84 protocol [2] started the era of quantum key distribution (QKD), providing a way to securely generate secret keys between two remote users by exploiting the laws of quantum mechanics. Combining this method with one-time pad provides ultimate physical-layer protection to the transmission of confidential messages. In general, for cost-effective implementations, QKD protocols are formulated in a prepare-and-measure fashion, where classical information is encoded in non-orthogonal quantum states: these are randomly prepared by Alice (the sender) and then transmitted to Bob (the receiver) through an insecure quantum channel. At the output of the channel, the states will be measured by Bob, so as to retrieve the encoded classical information. Depending on the setting, this measurement may consist of single-photon detections or coherent measurements, such as homodyne or heterodyne detections. The latter are certainly more attractive for commercial deployment, due to their room-temperature operation and compatibility with the current telecommunication infrastructure [7,10]. Protocols that exploit such coherent measurements and encode classical information by modulating states of an optical mode are today very popular and known as continuous-variable QKD (CV-QKD) protocols [1,4-6].

The most known CV-QKD protocol is the seminal GG02 protocol: this is based on the Gaussian modulation of the amplitudes of coherent states and homodyne detection of the channel output which is randomly switched between the two quadratures [12,13]. This protocol later evolved into various other Gaussian protocols [14-16] and it has been the subject of increasingly-refined security proofs [17,20]. Many experimental demonstrations of GG02 [11,21] and other CV-QKD protocols have been achieved so far (e.g., see [1 Sec. VIII] for an overview). The longest distance achieved in CV-QKD is currently 100 km in fiber, with a secure key rate of the order of 50 bps [21]. Compared to the performance of discrete-variable (DV) QKD protocols, this is a limited transmission distance with a relatively low key rate.

Here, we report the longest-distance experimental demonstration of CV-QKD, so as to be finally comparable with the performances currently achieved in DV-QKD. In fact, our experiment realizes CV-QKD over the record-breaking distance of about 200 km of fiber channel, doubling the previous record [21]. More precisely, we achieve the secret key rate of 6.214 bps at a distance of 202.81 km of ultralow-loss optical fiber. We obtain this result thanks to a fully automatic control system and high-precision phase compensation, so that the excess noise can be kept down to reasonably low values. In our experiment, we also use different reconciliation strategies at the various experimental distances considered, with an efficiency of 98% for the longest point at 202.81 km.

Our experimental setup is shown in Fig. 4. At Alice’s side, continuous-wave coherent light is generated by a 1550 nm commercial laser diode with a narrow linewidth of 100 Hz (NKT BasicE15). Two cascaded amplitude modulators (AM₁ and AM₂), each with high optical extinction of 45 dB, generate coherent light pulses at a repetition rate of 5 MHz. A very unbalanced 1/99 beamsplitter divides the pulses into strong local oscillator (LO) pulses and weak signal pulses. The latter are modulated by an amplitude modulator (AM₃) and a phase modulator (PM) with centered Gaussian distributions. For security reasons, the signal pulses are then attenuated to a several-photon level by using another amplitude modulator (AM₄). Finally, the signal pulses are recombined with the LO pulses in a polarizing beamsplitter and sent to Bob, each with a duration period of 38 ns.

At the output of the fiber link, signal and LO pulses are demultiplexed by another polarizing beamsplitter which is placed after an active dynamic polarization controller whose aim is optimize the outputs. On the LO path, we adopt an Erbium doped fiber amplifier. This is employed for amplifying the co-propagated and decreased-power LO to a magnitude
FIG. 1. **Optical layout of our long-distance CV-QKD system.** Alice sends an ensemble of 38 ns weak Gaussian-modulated coherent states to Bob multiplexed with a strong local oscillator (LO) in time and polarization by using a delay line and a polarization beam-combiner, respectively. Then the two optical paths are demultiplexed at Bob’s side by a polarizing beamsplitter placed after an active dynamic polarization controller. We perform phase modulation on the LO path to select the signal quadrature randomly. Finally, the quantum signal interferes with the LO on a shot-noise-limited balanced pulsed homodyne detector. Laser: continuous-wave laser; AM: amplitude modulator; PM: phase modulator; BS: beamsplitter; VATT: variable attenuator; PBS: polarizing beamsplitter; DPC: dynamic polarization controller; EDF A: Erbium doped fiber amplifier; PD: photodetector.

that is large enough to amplify the weak quantum signal. A second delay line realizes the time superposition of signal and LO pulses, and a phase modulator on the LO path selects the signal quadrature components randomly. The signal pulses interfere with the LO pulses on a shot-noise-limited balanced pulsed homodyne detector whose output is proportional to the signal and LO intensity. In this way, the quantum signal with ultra-low signal-to-noise ratio is amplified.

For the fiber link, we have used an ultralow-loss ITU-T G.652 standard compliant fiber (Corning SMF-28® ultralow-loss fibre) [22]. The average fiber attenuation (without splices) is 0.16 dB/km at 1550 nm. Our 202.81 km link has a total loss 32.45 dB. This is equivalent to 162.25 km of standard fibre with attenuation of 0.2 dB/km. Besides the longest distance of 202.81 km fiber link, the experiments with 27.27 km, 49.3 km, 69.53 km, 99.31 km, 140.52 km fiber link have also been done to show the performance of the CV-QKD system at different distances.

To overcome the channel perturbations due to the long-distance fiber, we employ several automatic feedback systems to calibrate time, polarization, and phase of the quantum states transmitted (see Methods for more details). To reduce the excess noise, we use an Erbium doped fiber amplifier. As previously mentioned, this amplifies the LO to the optimal working point of the homodyne detector (see Supplementary Section I for more details). The main contribution to the excess noise comes from residual phase noise due to the mismatch between the actual phase noise accumulated in the fiber and its estimation during our process of compensation (see Supplementary Section II for more details).

To reduce this residual phase noise we switch the key signals (i.e., those used for key generation) with higher-intensity ‘reference signals’ that are specifically dedicated to phase noise estimation. In our setup, the variance $V_A$ of the Gaussian modulation of the key signals as well as the signal-to-noise ratio (SNR) of the reference signals are controlled by modulators AM$_1$ and AM$_4$, which are in turn controlled by a 10-bit digital-analog-converter (DAC). The SNR of the reference signals is 34 dB higher than the SNR of the key signals. With this value, the residual phase noise is low enough to support the system over 202.81 km fiber.

Once Bob has measured the states sent from Alice, the two parties postprocess their data to generate a secret key [8]. In a CV-QKD system, postprocessing can be divided in four parts: basis sifting, parameter estimation, information reconciliation (or error correction), and privacy amplification. In our system, parameter estimation is performed after error correction (apart from a preliminary estimation of the SNR). From the

FIG. 2. **Covariance matrix.** We depict the covariance matrix of Alice’s and Bob’s variables in our CV-QKD system after 202.81 km of fiber link transmission. This follows the ordering \{(\(x_A, p_A, x_B, p_B\) \} and its components are expressed in shot noise units.
TABLE I. Overview of experimental parameters and performance for different fiber lengths. SNR: signal-to-noise ratio; $\beta$: reconciliation efficiency; $\alpha$: system overhead; FER: frame error rate of the reconciliation; $\nu_{el}$: modulation variance; $\xi$: excess noise; $\nu_{el}$: electronic noise; $\eta$: efficiency of the homodyne detector; $K_{\text{finite}}$: final secret key rate in the finite-size regime. SNU: shot-noise unit.

| Attenuation (dB) | 4.363 | 8.289 | 11.68 | 15.89 | 23.46 | 32.45 |
|------------------|-------|-------|-------|-------|-------|-------|
| Length (km)      | 27.27 | 49.30 | 69.53 | 99.31 | 140.52 | 202.81 |
| SNR              | 2.8035 | 1.0715 | 0.4619 | 0.1806 | 0.0308 | 0.0023 |
| $\beta$ (%)      | 95.00 | 95.00 | 96.00 | 96.00 | 96.00 | 98.00 |
| $\alpha$ (%)     | 10 | 10 | 10 | 10 | 10 | 10 |
| FER (%)          | 50 | 50 | 10 | 10 | 10 | 90 |
| $\nu_{el}$ (SNU) | 14.37 | 14.14 | 14.12 | 14.53 | 14.23 | 7.65 |
| $\xi$ (SNU)      | 0.1216 | 0.1881 | 0.049 | 0.0063 | 0.0086 | 0.0081 |
| $\eta$ (%)       | 61.34 | 61.34 | 61.34 | 61.34 | 61.34 | 61.34 |
| $K_{\text{finite}}$ (bps) | $2.78 \times 10^5$ | $0.62 \times 10^5$ | $4.28 \times 10^4$ | $1.18 \times 10^4$ | $318.85$ | $6.214$ |

For correlated data, we compute the covariance matrix illustrated in Fig. 5 from which we can derive the asymptotic key rate of our system. Then taking finite-size effects into account, the reverse reconciliation secret key rate is given by the general formula [1, 23]

$$K_{\text{finite}} = f (1 - \alpha) (1 - \text{FER}) \left[ \beta I(A : B) - \chi(B : E) - \Delta(n) \right],$$

where $f$ is the repetition rate (5 MHz in our experiment), $\alpha$ is the system overhead quantifying the ratio between reference and key signals, FER is the frame error rate of the reconciliation, $\beta$ is the reconciliation efficiency, $I(A : B)$ is the classical mutual information between Alice and Bob, $\chi(B : E)$ bounds Eve’s Holevo information on Bob’s variable in the finite-size regime, and $\Delta(n)$ is an offset term which accounts for privacy amplification in the finite-size regime. Here the number of points contributing to the final key is $n = (1 - \alpha) (1 - \text{FER}) N$ where $N$ is the number of total points. The same number of points $n$ is also used for parameter estimation, so that we build corresponding maximum-likelihood estimators for the channel parameters, compute their confidence intervals, and bound their values adopting 6.5 standard deviations. This worst-case scenario is then used to evaluate Eve’s Holevo bound.

Highly efficient postprocessing is needed to achieve long transmission distances at sufficiently high secret key rates. We use different information reconciliation schemes for different transmission distances (see Supplementary Section III for more details). Polar codes and multi-edge type LDPC codes are used to obtain high reconciliation efficiencies at the intermediate distances. For extremely low SNRs (lower than -23 dB), error correction is very difficult and it becomes challenging to construct suitable fixed-rate error correcting codes. For this reason, for our longest distance, we resort to a Raptor code. This is a type of rateless code able to reach high reconciliation efficiency at any SNR by sending check information until error correction is successful (see Methods for details). Privacy amplification is implemented by a hash function (Toeplitz matrices in our scheme). A graphic processing unit and multi-threading technology are used to accelerate the postprocessing procedure to generate secure keys.

The overview of experimental parameters and performance for different fiber lengths is shown in TABLE I. The secret key rate is 278 kbps at 27.27 km (4.363 dB losses), 62 kbps at 49.3 km (8.289 dB losses), 42.8 kbps at 69.53 km (11.68 dB losses), 11.8 kbps at 99.31 km (15.89 dB losses) and 318.85 bps at 140.52 km (23.46 dB losses). For the longest transmission distance of 202.81 km (32.45 dB) in our experiment, there is a SNR of 0.0023, the modulation variance $\nu_{el}$ is 7.65 SNU, and the excess noise is 0.0081 SNU, where SNU represents shot-noise units. Bob’s detector is assumed to be inaccessible to Eve and it is characterized by an electric noise of 0.1523 SNU and an efficiency of 0.6134. The final calculated secret key rate is 6.214 bps with a reconciliation efficiency of 98%.

The secret key rates of numerical simulations and experi-

FIG. 3. Experimental key rates and numerical simulations. The six five-pointed stars correspond to the experimental results at different fiber lengths of 27.27 km, 49.3 km, 69.53 km, 99.31 km, 140.52 km, and 202.81 km. The blue solid curve is a numerical simulation of the key rate which is computed starting from the experimental parameters at 140.52 km. The red solid curve is the corresponding numerical simulation computed from the parameters at 202.81 km. For comparison, we also show previous state-of-the-art experimental results [11, 23] and we compare the values and the scaling of our rates with the PLOB bound [24], i.e., the fundamental limit of repeaterless quantum communications.
mental results are shown in Fig. 3. The five-pointed stars correspond to our experimental results at different fiber lengths. The blue ones are for 27.27 km and 49.3 km with a reconciliation efficiency of 95%, and for 69.53 km, 99.31 km, and 140.52 km with a reconciliation efficiency of 96%. The red one is instead for 202.81 km with 98% reconciliation efficiency. The blue and red solid curves are the numerical simulations calculated from experimental parameters at 140.52 km and 202.81 km, respectively. We compare our points with the previous state-of-the-art experimental results and we also show their behaviour with respect to the PLOB bound [24], i.e., the secret key capacity of the bosonic lossy channel and fundamental limit of repeaterless quantum communications.

In conclusion, our long distance experiment has extended the security range of a CV-QKD system to the record fiber-distance of 202.81 km, a distance that is fully comparable with the performance of current QKD protocols with discrete variable systems. In addition, thanks to optimization procedures at the optical layer (phase compensation) and highly-efficient postprocessing techniques, the secret key rates are higher than previous results in CV-QKD at almost all distances. It is worth to remark that these key rates have been achieved with a repetition rate of only 5 MHz, therefore much slower than the clocks used in discrete-variable experiments (of the order of 1 GHz). Our results pave the way for an implementation of CV-QKD in more practical settings and show that large-scale secure QKD networks are within reach of room-temperature standard telecom components.

METHODS

Automatic feedback control systems. The overall feedback control systems consist of a synchronization module and a polarization calibration module. Clock synchronization and data synchronization are implemented by splitting a part of the LO pulses, after their de-multiplexing at Bob’s side, and detecting them by using a photodiode. The detection results are fed into a clock chip to generate the high-frequency clock signals as the time baseline for the overall system. Data synchronization is necessary for recognizing the consistent data pulses between the transmitted and received data. Combined with the inserted specific training sequences before the data frame for the modulation on AM1, data synchronization is thus realized using this detection output of the photodiode by distinguishing the training sequences. The polarization calibration module aims to compensate the polarization drift during the transmission through the quantum channel, including the aforementioned polarization beamsplitter and photodiode, and another key component, i.e., a dynamic polarization controller. The output of the photodiode is a feedback signal which is used for adjusting the dynamic polarization controller so as to let the LO power larger than that of the signal up to 30 dB.

High precision phase compensate. In our system we adopt a high-precision phase compensation scheme in order to (i) eliminate the phase shift induced from the unbalanced MZI structure and (ii) decrease the phase noise as much as possible. In this way, we can achieve long-distance transmission where even a slight increase of the excess noise may have non-trivial degradation effects on the value of the secret key rate. In our phase compensation scheme, a series of specific phase reference frames modulate the AM1 to generate 100 reference pulses every 1000 data pulses. With the help of another amplitude modulator AM4, the final SNR of the reference pulses is 34 dB higher than that of the signal pulses. This is sufficient to decrease the residual phase noise to a suitable low level. The results of the homodyne detection are used for calculating the relative phase difference between transmitted and received data, and the phase modulator on the LO path at Bob’s side modulates Bob’s data according to the calculated phase estimation results.

High efficient information reconciliation at approximately 26 dB SNR. In order to extract secret key at low SNR (lower than 26dB), we use the reconciliation scheme that combine multidimensional reconciliation and Raptor codes. Alice and Bob divide their data into vectors of size 8 and normalized them. A binary random sequence c is generated by a quantum random number generator. The sequence c is then encoded into another sequence c′ through Raptor encoding. Bob uses U and his own Gaussian variable Y′ to calculate the mapping function M(Y′, U). After Alice received enough side information, she starts to recover U by Raptor decoding and, therefore, Bob’s random binary sequence c. The rate of Raptor codes is uncertain before information transmission. In this work, we set the expected reconciliation efficiency to 98% and the length of encoded sequence is 1.81 × 10^6.

Acknowledgements This work was supported in part by the Key Program of National Natural Science Foundation of China under Grants 61531003, the National Natural Science Foundation under Grants 61427813 and the Fund of State Key Laboratory of Information Photonics and Optical Communications. S.P. has been sponsored by the EPSRC via the UK quantum communications hub (Grants No. EP/T001011/1).

Author Contributions H.G. and S.Y. conceived the research. H.G., S.Y. and Y.Z. designed the experiments. Y.Z., X.W., C.Z., B.C. and Y.Z. performed the experiments. S.P., Z.C and B.X. assisted with the theory. All authors contributed to the discussion of experimental results. H.G. and S.Y. supervised and coordinatized all the work. Y.Z., S.P., S.Y. and H.G. wrote the manuscript with contributions from all co-authors.

Competing interests and Correspondence The authors declare no competing financial interests. Correspondence and requests for materials should be addressed to S. Yu (yusong@bupt.edu.cn) and H. Guo (hongguo@pku.edu.cn).

[1] S. Pirandola, et al., Advances in Quantum Cryptography, arXiv preprint arXiv:1906.01645 (2019).
[2] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in Proc. IEEE Int. Conf.
on Computers, Systems and Signal Processing 175–179 (IEEE Press, 1984).

[3] A. K. Ekert, Quantum cryptography based on Bell’s theorem, Phys. Rev. Lett. 67, 661–663 (1991).

[4] C. Weedbrook, S. Pirandola, R. García-Patrón et al., Gaussian quantum information, Rev. Mod. Phys. 84, 621 (2012).

[5] P. K. Lam and T. C. Ralph, Quantum cryptography: Continuous improvement, Nature Photon., 7, 350–352 (2013).

[6] V. C. Usenko and R. Filip, Trusted Noise in Continuous-Variable Quantum Key Distribution: A Threat and a Defense, Entropy 18, 20 (2016).

[7] G. Zhang, et al., An integrated silicon photonic chip platform for continuous-variable quantum key distribution, Nature Photon., 13, 839–842 (2019).

[8] Y. Zhang, et al., Continuous-variable QKD over 50 km commercial fiber. Quantum Sci. Technol. 4(3), p.035006 (2019).

[9] F. Karinou, et al., Toward the integration of cv quantum key distribution in deployed optical networks, IEEE Photonics Technology Letters 30(7), 650-653 (2018).

[10] T. A. Eriksson, et al., Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tb/s data channels, Communications Physics 2(1), 9 (2019).

[11] P. Jouguet, S. Kunz-Jacques, A. Leverrier, et al., Experimental demonstration of long-distance continuous-variable quantum key distribution, Nature Photon., 7, 378–381 (2013).

[12] F. Grosshans and P. Grangier, Continuous Variable Quantum Cryptography Using Coherent States, Phys. Rev. Lett. 88, 057902 (2002).

[13] F. Grosshans, G. Van Assche, J. Wenger, et al., Quantum key distribution using gaussian-modulated coherent states, Nature 421, 238 (2003).

[14] C. Weedbrook, A. M. Lance, W. P. Bowen, et al., Quantum Cryptography Without Switching, Phys. Rev. Lett. 93, 170504 (2004).

[15] R. García-Patrón and N. J. Cerf, Continuous-variable quantum key distribution protocols over noisy channels, Phys. Rev. Lett. 102, 130501 (2009).

[16] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, Continuous-variable quantum cryptography using two-way quantum communication, Nature Phys., 4, 726–730 (2008).

[17] M. Navascués, F. Grosshans, and A. Acín, Optimality of Gaussian attacks in continuous-variable quantum cryptography, Phys. Rev. Lett. 97, 190502 (2006).

[18] R. García-Patrón and N. J. Cerf, Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution, Phys. Rev. Lett. 97, 190503 (2006).

[19] F. Furrer, T. Franz, M. Berta, et al., Continuous variable quantum key distribution: finite-key analysis of composable security against coherent attacks, Phys. Rev. Lett. 109, 100502 (2012).

[20] A. Leverrier, Composable security proof for continuous-variable quantum key distribution with coherent states, Phys. Rev. Lett. 114, 070501 (2015).

[21] 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).

[22] http://www.corning.com

[23] A. Leverrier, F. Grosshans, and P. Grangier, Finite-size analysis of continuous-variable quantum key distribution, Phys. Rev. A 81, 062343 (2010).

[24] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nature communications 8, 15043 (2017).

SUPPLEMENTARY INFORMATION

I. SHOT-NOISE-LIMITED HIGH-GAIN HOMODYNE DETECTOR

Here we show the experimental results for the quantum to classical noise ratio and the bandwidth of the shot-noise-limited high-gain homodyne detector. A 1550-nm fiber-coupled laser (NKT BasicE15, linewidth 100 Hz) offers continuous wave at its output, which is followed by a variable optical attenuator in order to adjust the beam power to an appropriate value. In the experiment, one of the input ports of beam splitter is left unconnected to provide the vacuum state. The LO and the vacuum state will interfere at the beam splitter with splitting ratio of 50:50. After that, there are a variable optical attenuator and a variable optical delay to balance the output arms of the fiber coupler, so that a homodyne detector will only amplify the differential signal. At the output of the homodyne detector, we then use a spectrum analyzer (Rigol DSA815), an oscilloscope (Keysight Technology MSOS804A) and a FPGA with ADC (ADS5400, sampling rate: 1GHz, sampling accuracy: 12bits) to analyze the output signal in both frequency and time domains. This experimental system needs to be properly adjusted to test the parameters of the homodyne detector.

In the frequency domain, the background noise spectrum of the spectrum analyzer, the electronic noise spectrum of the homodyne detector, and the output noise spectrum of the homodyne detector under different values of the LO power is shown in Fig. 4. By increasing the LO power, the output noise power of the homodyne detector will rise from kHz to 10 MHz. In the low-frequency region, the lower cut-off frequency is determined by the DC blocking capacitor. However, in this region, the superimposed 1/f noise and the instrument noise are so strong that the output noise spectrum of the homodyne detector is overwhelmed. As illustrated in Fig. 4, the quantum to classical noise ratio is about 24 dB at an LO power of 0.652 mW.
Here we explain the problem and management of the residual phase noise in our long distance CV-QKD experiment. In the experiment, Alice draws two sets of Gaussian random variables \((x_A, p_A) \sim N(0, V_A)\) and prepares a set of coherent states centered on the point \((x_A, p_A)\). These signal coherent states are transmitted through a fiber, at the end of which Bob performs homodyne detection in order to measure the quadratures of the received signal states (in a switching fashion). Phase noise is a common problem to all coherent detection schemes including those exploited in CV-QKD systems. This is mainly introduced by the unbalanced path of the Mach-Zehnder interferometer (MZI) and the use of different lasers for LO and signal.

To estimate the phase noise, \(n\) reference signals \((x_A', p_A')\) are also prepared by Alice and added to the Gaussian-modulated signals or 'key signals' for a total compensation period of \(m\) signals as shown in Fig. 5. The ratio \(\alpha \equiv n/m\) quantifies the percentage of exchanged signals which are not used for key generation. During a compensation period, the phase noise drift of all measurement results should be small enough to ignore its influence on the secret key rate. The compensation period is dependent on the drift rate of the phase noise and the repetition frequency of system. The phase noise estimation method is the same regardless of whether the drift rate is faster or slower than the repetition frequency.

The measurement results corresponding to the reference signals can be expressed by the formulas

\[
\begin{align*}
    x_B' &= \eta \sqrt{T} (x_A' \cos \phi + p_A' \sin \phi) + x_N \\
    p_B' &= \eta \sqrt{T} (-x_A' \sin \phi + p_A' \cos \phi) + p_N,
\end{align*}
\]

where \(\eta\) is the efficiency of the homodyne detector, \(\phi\) is the phase drift, \(T\) is the transmittance of the channel, \(x_N\) and \(p_N\) are quadratures describing a mode \(N\) with mean value and additive-noise variance \(V_N\). Here the variance \(V_N\) is a global parameter that includes shot noise, excess noise, and the electronic noise of the homodyne detector.

In the phase noise estimation stage, the measurement results \((x_B'\) or \(p_B')\) of the reference signals are transmitted to Alice. Since \(x_A', p_A', x_N\) and \(p_N\) are independent of each other, the correlations \(E_{XP} = \langle x_A' p_A' \rangle, E_{XN} = \langle x_A' x_N \rangle, E_{PP} = \langle p_A' p_A' \rangle, E_{PN} = \langle p_A' x_N \rangle\) are ideally equal to 0 and \(E_{XX} = \langle x_A' x_A' \rangle\) is equal to \(E_{PP} = \langle p_A' p_A' \rangle\). Ideally, the correlations \(\langle p_A' x_B' \rangle\) and \(\langle x_A' x_B' \rangle\) are given by

\[
\begin{align*}
    \langle x_A' x_B' \rangle &= \eta \sqrt{T} E_{XX} \cos \phi \\
    \langle p_A' x_B' \rangle &= \eta \sqrt{T} E_{PP} \sin \phi,
\end{align*}
\]
FIG. 5. The reference signals are used to estimate the phase noise affecting the key signals. The key signals are the Gaussian-modulated coherent states.

so that the phase drift can be estimated by

$$\tan \varphi = \frac{\langle p'_A x'_B \rangle}{\langle x'_A x'_B \rangle}. \quad (4)$$

Using this value, Alice and Bob can modify their data in order to clean the drift. However, the estimation of this drift is in practice affected by two errors: the first one is due to the fact that other types of correlations may intervene in the system (e.g., $E_{XP}$, $E_{YN}$, and $E_{PN}$ may be non-zero); the second is coming from the fact that the number of reference signals is finite and therefore there is an intrinsic statistical error due to the finite-size regime.

Because of the difference between the estimated phase drift $\varphi$ and the actual one $\varphi'$, there will be some phase noise building up in the system and contributing to the overall excess noise. Let us denote this difference by $\theta = \varphi' - \varphi$ and call it ‘residual phase noise’. This is now a random variable with expected value $\kappa = |\langle E(\cos \theta) \rangle|^2$. It is to show that its contributions to the excess noise is equal to $(1 - \kappa) V_A$ where $V_A$ is the variance of the Gaussian modulation of the input coherent states. Thanks to the compensation system of our experiment, we can keep $(1 - \kappa)$ to low values, which is about $7.6 \times 10^{-5}$.

III. HIGH EFFICIENT INFORMATION RECONCILIATION AT DIFFERENT DISTANCES

Currently, high-performance error reconciliation schemes exists for quantum cryptography [1-3]. In our information reconciliation step, we use slice reconciliation with polar codes at 27.27 km and 49.30 km, multidimensional reconciliation with multi-edge type LDPC (MET-LDPC) codes at 69.53 km, 99.31 km and 140.52 km, and multidimensional reconciliation with Raptor codes at 202.81 km.

Slice reconciliation scheme is an efficient reconciliation method for the scenario with high SNR. It can be divided in two steps: quantification and error correction. In reverse reconciliation, Bob quantifies his data into $n = 5$ slices. Then the real axis is divided in $2^n$ intervals by the interval points which are designed to maximize the quantification efficiency. In particular, we choose equal-width intervals to quantify the Gaussian distribution variables. After the quantification, a multi-level coding (MLC) and multi-stage decoding (MSD) scheme based on polar codes is performed to eliminate the errors. Each level is encoded independently in MLC and decoded successively in MSD with the decoding results used as side information to assist in decoding in the next stage. The optimal code rate of the $i^{th}$ ($1 \leq i \leq n$) slice with a given SNR is calculated by $R'_{i\text{opt}} = 1 - (I_i(\infty) - I_i(SNR))$, where $I_i(SNR)$ is the mutual information of the $i^{th}$ equivalent channel for given SNR [4]. Then polar codes with a length of $2^{20}$ are used to correct all the errors between Alice and Bob. The efficient of the information reconciliation are about 95.00% at 27.27 km and 49.30 km, which is shown in Fig. [5]

Multidimensional reconciliation scheme transforms a channel with Gaussian modulation to a virtual binary modulation channel as a first step. For 8-dimensional reconciliation, Alice and Bob divide their data into vectors $X$ and $Y$ of size 8 and normalize them to $X = \frac{1}{\sqrt{8}}$ and $Y = \frac{1}{\sqrt{8}}$. Then a random binary vector $U$ is generated by quantum random generator. Bob calculates the mapping function $M(Y', U)$ that satisfies $M(Y', U) \cdot Y' = U$. The mapping function is sent to Alice as side information. Alice maps her Gaussian variable $X'$ to $V$ where $V = M(Y', U) \cdot X' \ [5]$. Then Alice starts to recover $U$ by MET-LDPC codes with a code length of $10^6$. We use three different code rate parity check matrices, one is 0.25 for 73 km, the other one is 0.1 for 99.31 km and the last one is 0.02 for 146.62 km. As illustrated in Fig. [6] the efficient of the information reconciliation are about 96.00% at 69.53 km, 99.31 km and 140.52 km.

$\begin{aligned}
\text{Reference Signals} & \quad \text{Key Signals} \quad \text{Reference Signals} \\
\end{aligned}$
FIG. 6. Reconciliation efficiencies for different SNRs. We use slice reconciliation with polar codes at 27.27 km and 49.30 km, multidimensional reconciliation with multi-edge type LDPC (MET-LDPC) codes at 69.53 km, 99.31 km and 140.52 km, and multidimensional reconciliation with Raptor codes at 202.81 km.

[1] M. Milicevic, *Low-Density Parity-Check Decoder Architectures for Integrated Circuits and Quantum Cryptography*, Phd Thesis, University of Toronto (2017).
[2] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, *Quasi-cyclic multi-edge LDPC codes for long distance quantum cryptography*, npj Quantum Information 4, 21 (2017).
[3] X. Wang, Y. Zhang, S. Yu, B. Xu, Z. Li, and H. Guo, *Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution*, Quantum Inf. Comput. 17, 1123 (2017).
[4] G. V. Assche, J. Cardinal, N. J. Cerf, *Reconciliation of a quantum-distributed Gaussian key*, IEEE Transactions on Information Theory 50(2), 394-400 (2004).
[5] A. Leverrier, R. Allèame, J. Boutros, G. Zémor, P. Grangier, *Multidimensional reconciliation for a continuous-variable quantum key distribution*, Phys. Rev. A 77(4), 042325 (2008).
[6] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu and H. Guo, *Continuous-Variable Quantum Key Distribution with Rateless Reconciliation Protocol*, Phys. Rev. Appl. 12, 054013 (2019).