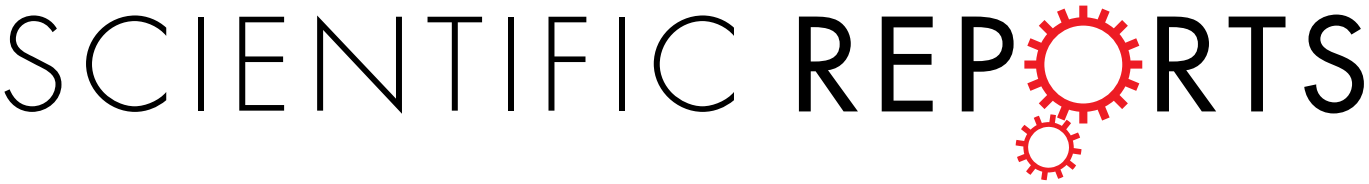

OPEN

Long-distance continuous-variable quantum key distribution by controlling excess noise

Received: 02 April 2015
Accepted: 08 December 2015
Published: 13 January 2016

Duan Huang[1], Peng Huang[1], Dakai Lin[1] & Guihua Zeng[1,2]

Quantum cryptography founded on the laws of physics could revolutionize the way in which communication information is protected. Significant progresses in long-distance quantum key distribution based on discrete variables have led to the secure quantum communication in real-world conditions being available. However, the alternative approach implemented with continuous variables has not yet reached the secure distance beyond 100 km. Here, we overcome the previous range limitation by controlling system excess noise and report such a long distance continuous-variable quantum key distribution experiment. Our result paves the road to the large-scale secure quantum communication with continuous variables and serves as a stepping stone in the quest for quantum network.

Quantum key distribution (QKD) using photons to disseminate encryption codes enables two distant partners to share a secret key[1,2]. Currently, two available approaches referred to as discrete-variable QKD[3,4] and continuous-variable (CV) QKD[5,6] are employed to distribute secret keys. The CV-QKD has been proved, in principle, to be secure against general collective eavesdropping attacks, which are optimal in both the asymptotic case[7,8] and the finite-size regime[9–11]. From a practical point of view, the CV approach has potential advantages[12] because it is compatible with the standard optical telecommunication technologies. It is foreseeable that this approach will become a viable candidate for large-scale secure quantum communication.

However, the practical long-distance environment provides a number of technical challenges for the present CV-QKD experiments. There are two major hurdles that severely limit the secure distance. One is limited reconciliation efficiency[13] and the other is excess noise[14]. Because of the difficulty of reconciliation at low signal-to-noise ratios (SNRs) in previous 25 km experiments[15–19], P. Jouguet *et al.* developed an efficient error-correcting code (ECC)[20] which leads to a remarkable improvement of transmission distance for CV-QKD[21]. However, further extending the secure distance in their experiment is limited, partly because of the incremental technical excess noise. Intuitively, the increase of excess noise is associated with higher fibre loss and lower SNR, which are two key aspects of long-distance implementations. More specifically, the increase of fibre loss requires a stronger Local Oscillator (LO) for shot-noise-limited homodyne detection, and the decrease of SNR is a great challenge for precision phase compensation. Nevertheless, in the long-distance scenarios, control of the excess noise induced by the photons leakage from the strong LO to the weak quantum signal and the inaccuracy of phase compensation has never been studied experimentally. This may be attributed to the fact that beyond 100 km the experimental difficulties of CV-QKD are significantly increased with respect to previous achievements.

In this paper, we report for the first time an experimental demonstration of CV-QKD over 100 km fiber channel. The result is achieved by controlling the excess noise in the following ways. Firstly, the adoption of a high-sensitive homodyne detector with lower requirement of LO power allows us to reach the shot noise limit (SNL) at previously inaccessible parameter regions, and it is the prerequisite of successfully performing a long-distance CV-QKD experiment. Secondly, a secure scheme is proposed to overcome the difficulty of high-precision phase compensation under the low SNR conditions, so that we can get the effective data regardless of the phase drifts of fibre links. Both techniques confine the excess noise within a tolerable limit, and result in a record secure transmission distance. Another practical distance limitation of our experiment is essentially the finite-size effect, and appear to be due mostly to the excess noise induced by finite statistics[9–11]. However, the key

[1]State Key Laboratory of Advanced Optical Communication Systems and Networks, and Center of Quantum Information Sensing and Processing, Shanghai Jiao Tong University, Shanghai 200240, China. [2]College of Information Science and Technology, Northwest University, Xi'an 710127, Shaanxi, China. Correspondence and requests for materials should be addressed to P.H. (email: huang.peng@sjtu.edu.cn) or G.Z. (email: ghzeng@sjtu.edu.cn)

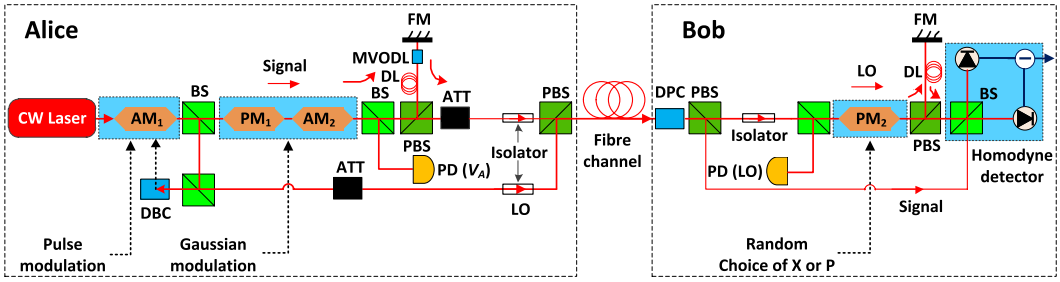

Figure 1. Experimental setup of CV-QKD. CW laser, continuous wave laser; AM, amplitude modulator; DBC, dynamic bias controller; BS, beam splitter; ATT, attenuator; PM, phase modulator; PD, photodetector; PBS, polarizing beamsplitter; DL, delay line; MVODL, manual variable optical delay line; FM, faraday mirror; DPC, dynamic polarization controller.

element for the present experiment is controlling the technical excess noise that is previously overlooked, and we verify the applicability and maturity of such technologies in real-world scenarios.

Results

Experimental setup. We perform the experiment based on the Gaussian-modulated coherent states (GMCS) protocol[12]. The experiment setup is depicted in Fig. 1. It consists of three major steps: pulse modulation, Gaussian modulation and random phase modulation for homodyne detection. At Alice's side, a 1,550 nm continuous-wave (CW) light is transformed into a 2 MHz clock square pulse train by an amplitude modulator (AM) in pulse modulation. An asymmetrical Mach-Zehnder interferometer (AMZI) divides the pulses into a LO path and a signal path. In the signal path, the x and p quadratures of coherent states are modulated in according to a centered Gaussian distribution of variance V_A in the units of shot noise variance N_0, where N_0 appears in the Heisenberg uncertainty relation $\Delta x\Delta p \geq N_0$. By using the polarization-multiplexing and time-multiplexing techniques, the signal together with LO are sent to Bob through a 100 km standard telecom fiber spool with a measured loss of 0.2 dB/km at 1,550 nm. For the polarization-multiplexing, the Faraday mirrors reflects the signal pulses at Alice's side and LO pulses at Bob's side by imposing a 90° rotation on their original polarization states. Besides, two delay lines and a manual variable optical delay line are inserted into the system so as to accurately equilibrate the interferometer. At Bob's side, the demultiplexed LO and signal interfere in a shot-noise-limited homodyne detector. The output intensity is proportional to the modulated quadratures. Bob measures either x or p by randomly generating a $\pi/2$ or zero phase shift on the reference LO light. To enhance the system stability, we developed automatic feedback modules to calibrate the bias of AM at Alice's side and the polarization-demultiplexing at Bob's side (see Methods and Supplementary for more details).

In our experimental setup, we insert several isolators in both sides to prevent the Trojan-horse attacks[22]. Since the shot noise variance is proportional to the LO power, we use a photodiode (PD) to monitor the LO at Bob's side which is transmitted through the insecure quantum channel and it could be manipulated by a potential eavesdropper. In addition, a recent robust shot noise measurement scheme[23] can also be employed in our experiment to prevent some attacks targeting the shot noise, such as LO fluctuation attacks[24] and LO calibration attacks[25,26]. The potential risk of other attacks can also be resisted by additionally inserting optical devices. For example, the wavelength attacks[27] can be prevented with a fiber Bragg grating at Bob's side. In the following, we employ the general assumption that Eve cannot tamper with the devices in both sides. In this case, the detection efficiency η_{hom} and the electronic noise υ_{el} can be considered to be inaccessible to Eve. The other experimental parameters associated with the secure distance, such as V_A, N_0, channel transmission T and excess noise ε, are estimated using a parameter estimation process in real time, where ε and υ_{el} are expressed in shot noise units.

Controlling excess noise by shot-noise-limited homodyne detection with weak LO. In the implementation of the GMCS protocol, homodyne detection of coherent states under the SNL requires sufficient LO power. However, the excess noise increases significantly due to photons leakage from the strong LO to the weak quantum signal. Especially, in an optical system with a finite extinction ratio R_e, it is difficult to completely remove the residual photons between two adjacent LO pulses. Since the leaked LO photons and the signal photons will simultaneously interfere with the LO pulses, the excess noise ε_{LE} and V_A would be of the same order of magnitude. The involved excess noise ε_{LE} is derived in Supplementary S1,

$$\varepsilon_{LE} = \frac{2\langle \hat{N}_{LO}^{Alice} \rangle}{R_e}, \tag{1}$$

where $\langle \hat{N}_{LO}^{Alice} \rangle$ is the LO power at Alice's side. In Fig. 1, we achieved an overall equivalent extinction ratio of 100 dB with customized optics which feature an extinction ratio of 65 dB in pulse modulation and 35 dB in polarization-multiplexing. In the previous experiments[15,16], the typical LO power $\langle \hat{N}_{LO}^{Alice} \rangle$ is 10^8~10^9 photons/pulse. In order to achieve a secure distance of 100~150 km (or equivalently 20~30 dB fiber loss), the tolerable excess noise is around 0.01 under the collective attacks. Therefore, at Bob's side, the shot-noise-limited homodyne detection should be performed with a weak LO $\langle \hat{N}_{LO}^{Bob} \rangle$ of 10^5 photons/pulse. However, to our knowledge, the

reported state-of-art shot-noise-limited homodyne detector is usually operated at a LO power $\langle \hat{N}_{LO}^{Bob} \rangle$ of $10^6 \sim 10^8$ photons/pulse[28], and this quantum detector has been widely used in the shot-noise-limited measurement of quantum state[29–31].

To understand that the insufficient LO power $\langle \hat{N}_{LO}^{Bob} \rangle$ for the shot-noise-limited homodyne detection has become a major constraint in the long-distance CV-QKD, it is useful to start with analysis of shot noise N_0 and electronic noise υ_{el} in terms of the noise ratio

$$S = 10lg\,(N_0/\upsilon_{el}). \tag{2}$$

The basic prerequisite of the shot-noise-limited homodyne detection is $S > 0$ dB. And the shot noise N_0 is associated with the LO power $\langle \hat{N}_{LO}^{Alice} \rangle$ at Alice's side,

$$N_0 = 10^{-0.02L} \eta_{LO} (g\eta_{hom})^2 \langle \hat{N}_{LO}^{Alice} \rangle \langle \Delta X_{vac}^2 \rangle, \tag{3}$$

where L is the fibre length, η_{LO} is the LO transmittance at Bob's side, g is the electronic gain, and $\langle \Delta X_{vac}^2 \rangle$ is the vacuum fluctuation. According to Eqs (2) and (3), it is clear that the homodyne detection in the SNL requires relatively low electronic noise and sufficient LO power at Bob's side, whereas the latter is limited by the maximum tolerable excess noise ε_{LE} in 100 ~ 150 km CV-QKD as discussed above.

To control the excess noise to a level that makes the long-distance experiment possible, we developed an extremely low electronic noise homodyne detector, which allow us to reach the SNL with a weak LO. We replace the conventional operational preamplifier with cooled field-effect transistors (FETs) because that the FETs have been shown superior performance in low-noise applications. The additional cooling increases the transconductance and reduces the leakage current, subsequently reduces the electronic noise. The FETs employed in our detector are fabricated in a multistage thermoelectric cooler with minimum temperature of −510 °C. We note that the FETs with the cryogenic operation have been used in the photon-number-resolving detection[32]. It has great advantage because the noise figure (NF) of first stage completely dominates the NF of the entire detector. In these ways, we designed a nearly noise-free preamplifier circuit. The overall detection efficiency η_{hom} is 0.6, which is limited by the quantum efficiency of PIN photodiodes. The total noise of the detector is measured by a 200 M/s data acquisition card with a 50 ns width pulsed LO at a repetition rate of 2 MHz. In Fig. 2, each noise variance point is obtained from 10^7 sample pulses. One great benefit of handling the electronic noise υ_{el} is that we can achieve a large electronic gain coefficient g in our design so as to get higher noise clearance between shot noise and electronic noise compared with previous detector[28]. The achieved maximum noise ratio S is 30 dB, 19 dB, 8 dB at LO power of 10^7, 10^6, 10^5 photons/pulse, respectively. In this way, with a typical $\langle \hat{N}_{LO}^{Alice} \rangle$ of 10^8 photons/pulse and extinction ratio R_e of 100 dB, we achieved the noise ratio of $S > 8$ dB and effectively controlled the excess noise ε_{LE} in the order of 0.01, which is a tolerable value in our 100 ~ 150 km CV-QKD experiment.

Controlling excess noise by high-precision phase compensation with low SNR. In the GMCS-QKD implementation, the phase difference ϕ between the LO (phase reference) and the quantum signal will drift with time due to the instabilities of AMZIs. Accordingly, a phase compensation scheme is necessary. However, under low SNR situations, the attempt to compensate the phase drift with stronger optical signals compared with the quantum signals, such as brighter labeling pulses, would leave a loophole for Eve. Moreover, the increase of inaccuracy $\delta\theta$ of phase compensation at low SNR will inevitably result in higher level of the excess noise. Here we developed a secure way to control the excess noise, and it is realized with a high-precision phase compensation by means of software based on noisy raw data, which is randomly selected from Gaussian raw keys in the postprocessing process.

We firstly characterize the phase drifts and the corresponding excess noise ε_{phase} in a CV-QKD experiment. The phase difference ϕ in one frame can be described as,

$$\phi = \phi_0 + \Delta\phi, \tag{4}$$

where ϕ_0 is the relative phase difference (or the phase difference when Alice encodes phase 0) which is constant during one frame transmission, and $\Delta\phi = \phi_{max} - \phi_{min}$ is a small variation of the phase drift in one frame. Because the phase difference ϕ is the only estimated value for the phase compensation in the transmission period of one frame, in order to effectively compensate the phase drift, the phase variation $\Delta\phi$ of the phase drift in this frame should be less than the inaccuracy $\delta\theta$, i.e. the precision of the phase compensation. Otherwise, the phase difference between the real phase drift and compensate phase value might be exploited by a potential eavesdropper in this data frame, and the estimated excess noise would be lower than the actual value. Therefore, one has to achieve

$$\Delta\phi \le \delta\theta. \tag{5}$$

To confine the phase excess noise within a tolerable limit, we have derived ε_{phase} due to the inaccuracy of the phase compensation in Supplementary S1,

$$\varepsilon_{phase} = (1 - \kappa)(\varepsilon_c + V_A)/\kappa, \tag{6}$$

where $\kappa = (E[\cos\ \delta\theta])^2$, $E[\cos\ \delta\theta]$ denotes the expectation of the $\cos\delta\theta$, and ε_c is the channel excess noise[33]. According to Eq. (6), to suppress the phase excess noise ε_{phase} to a level of 0.01 or 0.001 with typical values $\varepsilon_c < 0.01$ and $V_A = 4$, the minimum precision requirement of $\delta\theta$ is 2.9° or 0.9° per frame, respectively. In these two cases, according to Eq. (5), the variations of phase drifts $\Delta\phi$ in one frame should be less than 2.9° or 0.9°, respectively.

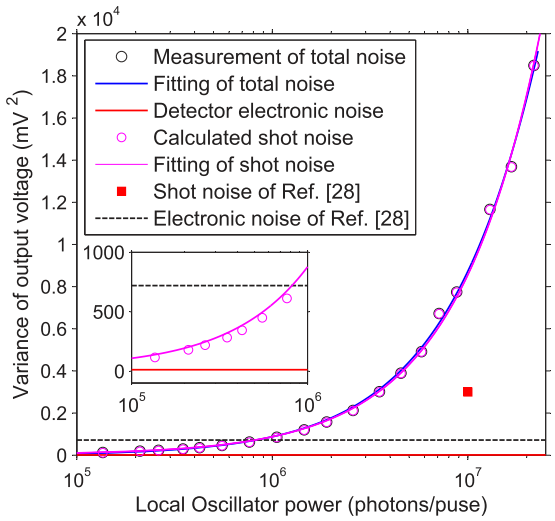

Figure 2. Shot noise characterization of homodyne detector. (**1**) The total noise (black circles) includes: (i) shot noise N_0 (linear LO-dependent), (ii) electronic noise υ_{el} (LO-independent) and (iii) the noise of LO fluctuations ε_{flu} (quadratic LO-dependent). The measurement of total noise is fitted by a quadratic polynomial function with confidence intervals of 0.95 (blue line). The error bars are much smaller than the symbol size. (**2**) The electronic noise $\upsilon_{el} = 12.8\,mV^2$ (red line) is measured without LO. (**3**) The shot noise (magenta circles) is calculated from the measurement total noise. The calculated shot noise is fitted by a linear polynomial function with confidence intervals of 0.95 (magenta line), which can be written as $N_0 = 8.5 \times 10^{-4}$ $\langle \hat{N}_{LO}^{Bob} \rangle \approx 8.5 \times 10^{-4-0.02L} \langle \hat{N}_{LO}^{Alice} \rangle$.

Our phase compensation scheme is described as follows (see Methods). In the reconciliation stage Bob announces a randomly selected subset X_B' of one frame, and then Alice makes a reverse prediction of ϕ by calculating the auto-correlation of her original frame X_A' and Bob's noisy detection results X_B',

$$Cov(X_A', X_B') = 10^{-0.02L}\eta_{hom} g_B V_A N_0 \cos(\phi). \tag{7}$$

where g_B is the overall gain coefficient at Bob's side. It is clear that the auto-correlation results are irrelevant to the Gaussian noise. This way enables us to compensate the phase drift ϕ under a low SNR condition.

The characterization of the phase compensation in our experiment is shown in Fig. 3. We use a secure threshold to estimate the excess noise ε_{phase} due to $\delta\theta$. We firstly compute the phase drifts of measurement results in one data block. The maximum inaccuracy of the phase compensation in the block is used to set an adaptive threshold and bound the excess noise ε_{phase}. In our case, each experiment point of phase drift ϕ is calculated with 4×10^3 pulses which are randomly selected in one frame. The elapsed time of one frame is 5 ms which corresponds to 10^4 pulses. The length of error bar represents the accuracy $\delta\theta$ of the phase compensation. The maximum $\delta\theta$ in one block (40 frames in our case) is used to set as the secure threshold, and the excess noise ε_{phase} is calculated based on the threshold. Under the normal condition, we achieved $\varepsilon_{phase} < 1.2 \times 10^{-5}$ with a typical SNR of ~0.002 and the compensation accuracy $\delta\theta$ of 0.1° per frame in the 150 km CV-QKD experiment. Under a worse condition, for example, a measurement block with complex and worse phase drifts can be divided into slow phase drifts (< 100 ms) and fast phase drifts ($\geqslant 100$ ms), whereas the latter might be caused by Eve's phase attacks. According to Eqs. (5) and (6), the portion of block with a tendency of phase drifts towards to $\Delta\phi = 2.9°$ per frame will be discarded directly. While a randomly selected subset of the other portion will be used to compute a reliable adaptive threshold, which is used to calculated the maximum excess noise of phase compensation. Since this randomness makes it hard for Eve to guess the calculated pulses, we can guarantee the security of our phase compensation scheme in a CV-QKD experiment, and confine the phase excess noise within a tolerable limit.

Reconciliation and finite-size secret key. In a 100~150 km CV-QKD implementation, the SNR is lower by more than an order of magnitude compared with previous record[21]. Hence it imposes a greater challenge to reconcile Gaussian variables. In our experiment, the actual SNRs at Bob's side are about 0.024 at 100 km and 0.0024 at 150 km, which are achieved by optimizing the modulation variances V_A (detailed in Supplementary S2). Based on the multiedge-type low density parity check codes[34] and the technique of repetition scheme[35], we developed a 25 MHz ECC[36] which exhibits an efficiency of $\beta = 95.6\%$ at the SNR threshold of 0.002 (detailed in Supplementary S2). The target frame error rate (FER) is 0.3. We remark here that the FER is one of key characteristics of an ECC. The failure probability of error decoding cannot be neglected and should be calculated in the final key rate. Taking the finite-size effects into account, the maximum secret key rate bounded by collective attacks is given by

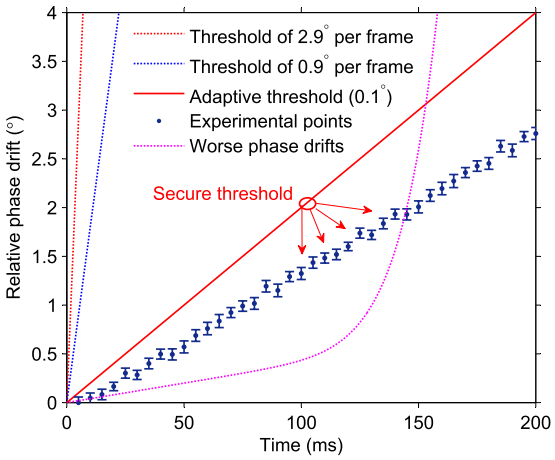

Figure 3. Characterization of phase compensation. The adaptive threshold is calculated from a subset of the raw data. The maximum length of error bar L_E represents the accuracy $\delta\theta$ of the phase compensation, which is used to confine the excess noise ε_{phase}. The slope of the adaptive threshold is determined by the L_E (°/frame, one frame is 5 ms in our case). The worse phase drifts will be confined by a straight line with a bigger slope, which means higher excess noise ε_{phase}. The total phase drifts is about 15°/s (<0.1°/5 ms) in our case.

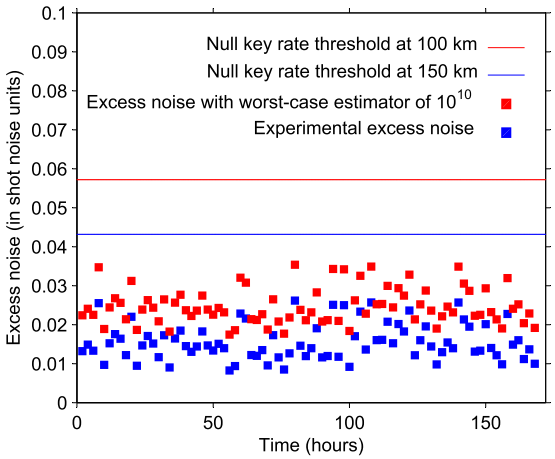

Figure 4. Excess noise measurement. The lower blue square points are measured at 100 km with 10^{10} finite-size blocks, which are subsets of a block with size of 10^{12}. The effective excess noise under worst-case estimator (red square point) is employed to compute the final secret key rate. The red line defines the tolerable maximal value of excess noise at 150 km. The blue line defines the tolerable maximal value of excess noise at 100 km.

$$K_{finite} = \frac{nR}{N}(1 - FER)[\beta I_{AB} - \chi_{BE} - \Delta(n)], \tag{8}$$

where I_{AB} is the Shannon mutual information between Alice and Bob, χ_{BE} is the Holevo bound on the information between Bob and Eve, R is the repetition rate of QKD system and it is 2 MHz in our experiment, $\Delta(n)$ is related to the security of the privacy amplification[9], N denotes the sampling length, and n denotes the block length for final key estimation. In the post-processing procedure, the block with a length of $N-n$ is used for parameters estimation and phase compensation, and $n/N \approx 2/7$ in our case.

In Fig. 4, we mainly focus on the excess noise in the parameters estimation process. The excess noise is measured on a block of size 10^{12} with 84 blocks of size 10^{10} over one week for a distance of 100 km. Fortunately, because we have employed a high sensitive homodyne detector in weak LO and high precision phase compensation under low SNR condition, we can well deal with the main excess noise due to the inherent defects of the long-distance CV-QKD experiment. The measurement of the excess noise with the finite-size block of 10^{12} is around $0.015N_0$. The corresponding excess noise under the worst-case estimator[9,21,37] is employed to compute the secret key rate when the extreme finite-size effects is taken into account.

The secret key rate respect to transmission distance is depicted in Fig. 5. The key experimental parameters that intervene in the Eq. (8) for the calculation of key rate are the modulation variances V_A, channel transmission T, excess noise ε, the quantum efficiency η_{hom}, and the electronic noise υ_{el}, which are estimated in a finite-size scenario. Results show that we have experimentally achieved a secure transmission distance over 100 km. Based on

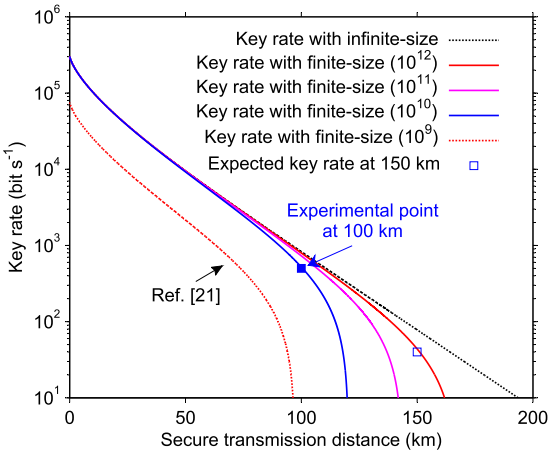

Figure 5. Secret key rate under general collective attacks in finite-size scenarios. The finite-size security model is based on the previous state-of-art experiment[21]. From left to right, curves correspond, respectively, to block lengths of $N = 10^9$,10^{10},10^{11},10^{12} and infinite. The red dash line is the state-of-art experiment with 1 MHz repetition rate. The blue square point is the 2 MHz experiment result, which is calculated from a group of time-varying excess noise. The modulation variance V_A is optimized and set as 4, the reconciliation efficiency β is 95.6%, the theoretical target excess noise is set as 0.01, the security parameter ε is set as 10^{-10}. The practical excess noise with worst-case estimator is used to compute the experimental point.

the realistic experiment conditions, the maximum achievable block size in our experiment is 10^{12}, which takes one week for the data acquisition and processing. For simplicity, we present one finite-size block with size of 10^{12} in Fig. 4 to demonstrate the ability to implement such a long-distance experiment. For comparison, we plot the previous state-of-art experimental result[21] with 10^9 finite-size block at the same finite-size security model[9,37].

We also became aware of a recent work on finite-size effects for CV-QKD[11]. It shows a tighter security bound to describe Eve's attacks in composable security framework, which requires larger blocks for parameter estimation. With such a finite-size security model, the minimum finite-size block is 10^9 at 10 km. Fortunately, the security of our system with our excess noise controlling techniques still can be guaranteed around 100 km with a block size of 10^{12}. Since the finite-size effects would severely affect the theoretic maximum distance, only getting enough and reliable raw data ($\sim 10^{14}$) can we achieve a CV-QKD beyond 150 km. In this case, a more stable system is required.

Discussion

We have demonstrated the longest CV-QKD experiment by controlling the excess noise. To deal with the excess noise under longer distance scenarios, we have investigated some practical approaches to enhance the SNR and reduce demands of the propagated LO power. On the one hand, we have investigated a photon-subtraction scheme that could increase the optimal V_A and finally improve the SNR[38]. On the other hand, the concerns of finite extinction ratio between propagated LO and quantum signal could be further reduced with frequency-shift method which was previously introduced for multichannel parallel CV-QKD[39]. While the security concerns of LO may be removed by using recent schemes with locally generated LO[40–42]. In addition, we note that some schemes with entangled states[43] and noiseless amplification[44] are also promising for long-distance CV-QKD.

Considering the finite-size effects, an efficient scheme for phase shift QKD has been proposed recently to greatly reduce the exchange information[45]. It is anticipated that this finding together with our ways of controlling excess noise will facilitate the present CV-QKD beyond 150 km. In addition, the constraint of block size and the corresponding elapsed time could be relaxed in a high-speed CV-QKD. Although several reported high-speed shot-noise-limited homodyne detectors allows us to operate at 100 MHz repetition rate[46–48], the power requirement of LO for quantum measurement is orders of magnitude larger than the minimum demanding of the detector reported in this work. Therefore so far these detectors are not suitable for long-distance CV-QKD. But we believe that more efficient schemes and pioneering technological advances will bring us to the point where, in a new era of quantum information, a global quantum cryptography network is established.

Methods

System stability. We develop two automatic feedback control modules to enhance the stability of the CV-QKD system. (1) The modulator bias control (MBC) module. In our experiment, the light source is a narrow linewidth (1.9 kHz) and low phase noise (2 μrad/rt-Hz 1 m OPD) laser producing CW coherent light at 1,550.12 nm (ITU-34). The CW light is transformed into a 2 MHz clock pulse train by a low jitter (<25 ps) digital square pulse generator and near 65 dB extinction ratio, 10 GHz $LiNbO_3$ AM. Since the bias voltage of $LiNbO_3$ modulator drifts with time, it will reduce the effective extinction ratio in the whole system. To stabilize the AM, we employ a MBC module to lock the working point automatically. This calibration process is used

during the system initialization to maximize the extinction ratio of optical pulses, and achieved by monitoring the feedback light intensity from the output of modulator. (2) The dynamic polarization control (DPC) module. The polarization-demultiplexing of signal and LO is achieved by a DPC and polarization beam splitter at Bob's side. The LO pulses split from the LO path at Bob's side is detected by a PD. The analog electrical signal from the LO is fed back to bring back the State of Polarization (SOP) towards the correct SOP, which guarantees that the LO photons enter into the LO path at Bob's side. The excess noise induced by the leaked LO photons is detailed in Supplementary S1.

Phase compensation. We proposed an auto-correlation and reverse prediction scheme to detect the phase drift ϕ. At Alice's side, Gaussian quadratures $\{X_{Alice}, P_{Alice}\}$ are employed to encode coherent states $|X_{Alice} + iP_{Alice}\rangle$, which are attenuated from a Gaussian-modulated coherent light. The quadratures can be written as

$$X_{Alice} = A \ \cos(\psi), \tag{9}$$

$$P_{Alice} = A \ \sin(\psi), \tag{10}$$

where amplitude A and phase ψ follow the Rayleigh distribution and the uniform distribution, respectively. Then the prepared coherent states will be transmitted through a Gaussian channel. Under the normal conditions, ϕ drifts with time slowly because of the instabilities in the AMZIs. Consequently, at Bob's side, the corresponding homodyne measurement results are

$$X_{Bob} = 10^{-0.02L}\eta_{hom}g_B A \ \cos(\psi + \phi) + \xi, \tag{11}$$

$$P_{Bob} = 10^{-0.02L}\eta_{hom}g_B A \ \sin(\psi + \phi) + \xi, \tag{12}$$

where ξ denotes the additive Gaussian white noise. For simplicity, only the X variable is considered in the following. In extremely low SNR scenarios, the measurement signal is buried in the noise,

$$10^{-0.02L}\eta_{hom}g_B A \ \cos(\psi + \phi) \ll \xi. \tag{13}$$

In the classical reconciliation stage, Bob announces a subset X'_B which is randomly selected from one frame. Then Alice makes a precise calculation of ϕ with Bob's noisy detection results and her original frame X'_A. This reverse prediction procedure is finished by calculating the auto-correlation of X'_A and X'_B,

$$\begin{aligned} Cov(X'_A, X'_B) &= E(X'_A \cdot X'_B) \\ &= E\{[T\eta_{hom}g_B A \ \cos(\phi + \Delta\phi) + \xi] \cdot [A \cdot \ \cos(\phi)]\} \\ &= 10^{-0.02L}\eta_{hom}g_B V_A N_0 \ \cos(\phi) \end{aligned} \tag{14}$$

Finally, Alice maps her original data $\{X_{Alice}, P_{Alice}\}$ into $\{X'_{Alice}, P'_{Alice}\}$ with the phase difference ϕ, and Alice and Bob produce a raw key from $\{X'_{Alice}, P'_{Alice}\}$ and $\{X_{Bob}, P_{Bob}\}$. Furthermore, the security of the GMCS-QKD protocol still holds. The excess noise induced by phase compensation is detailed in Supplementary S1.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. in *Proc. of the IEEE Int. Conf. on Computers, Systems and Signal Processing, Bangalore, India*, pp. 175–179 (IEEE, New York, 1984).
2. Zeng, G. H. *Quantum private communication* Ch. 3 (Springer-Verlag press, Berlin, 2010).
3. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74,** 145 (2002).
4. Lo, H. K., Curty, M. & Tamaki, K. Secure quantum key distribution. *Nature Photon*. **8,** 595–604 (2014).
5. Samuel, L. B. & Peter, V. L. Quantum information with continuous variables. *Rev. Mod. Phys.* **77,** 513 (2005).
6. Weedbrook, C. *et al.* Gaussian quantum information. *Rev. Mod. Phys.* **84,** 621 (2012).
7. Garca-Patrón, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97,** 190503 (2006).
8. Navascués, M., Grosshans, F. & Acn, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **97,** 190502 (2006).
9. Leverrier, A., Grosshans, F. & Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **81,** 062343 (2010).
10. Furrer, F. *et al.* Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.* **109,** 100502 (2012).
11. Leverrier, A. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.* **114,** 070501 (2015).
12. Grosshans, F. *et al.* Quantum key distribution using gaussian-modulated coherent states. *Nature* **421,** 238–241 (2003).
13. Leverrier, A., Alléaume, R., Boutros, J., Zémor, G. & Grangier, P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A* **77,** 042325 (2008).
14. Lodewyck, J., Debuisschert, T., Tualle-Brouri, R. & Grangier, P. Controlling excess noise in fiber-optics continuous-variable quantum key distribution. *Phys. Rev. A* **72,** 050303 (2005).
15. Lodewyck, J. *et al.* Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76,** 042305 (2007).
16. Qi, B., Huang, L. L., Qian, L. & Lo, H. K. Experimental study on the Gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A* **76,** 052323 (2007).

17. Xuan, Q. D., Zhang, Z. S. & Voss, P. L. A 24 km fiber-based discretely signaled continuous variable quantum key distribution systems. *Opt. Express* **17,** 24244 (2009).
18. Fossier, S. *et al.* Field test of a continuous-variable quantum key distribution prototype. *New J. Phys.* **11,** 045023 (2009).
19. Jouguet, P. *et al.* Field test of classical symmetric encryption with continuous variables quantum key distribution. *Opt. Express* **20,** 14030 (2012).
20. Jouguet, P., Kunz-Jacques, S. & Leverrier, A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. *Phys. Rev. A* **84,** 062317 (2011).
21. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photon.* **7,** 378–381 (2013).
22. Jain, N. *et al.* Risk analysis of Trojan-horse attacks on practical quantum key distribution systems. *IEEE J. Sel. Top. Quantum Electron.* **21,** 6600710 (2015).
23. Kunz-Jacques, S. & Jouguet, P. Robust shot-noise measurement for continuous-variable quantum key distribution. *Phys. Rev. A* **91,** 022307 (2015).
24. Ma, X. C., Sun, S. H., Jiang, M. S. & Liang, L. M. Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems. *Phys. Rev. A* **88,** 022339 (2013).
25. Ferenczi, A., Grangier, P. & Grosshans, F. Calibration attack and defense in continuous variable quantum key distribution. in Lasers and Electro-Optics, 2007 and the International Quantum Electronics Conference. CLEOE-IQEC 2007. European Conference on, Munich (IEEE, New York, 2007).
26. Jouguet, P., Kunz-Jacques, S. & Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A* **87,** 062313 (2013).
27. Huang, J. Z. *et al.* Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A* **87,** 062329 (2013).
28. Hansen, H. *et al.* Ultrasensitive pulsed, balanced homodyne detector: application to time-domain quantum measurements. *Opt. Lett.* **26,** 1714–1716 (2001).
29. Legre, M., Zbinden, H. & Gisin, N. Implementation of continuous variable quantum cryptography in optical fibres using a go-&-return configuration. *Quantum Inf. Comput.* **6,** 326–335 (2006).
30. Lvovsky, A. I. & Raymer, M. G. Continuous-variable optical quantum-state tomography. *Rev. Mod. Phys.* **81,** 299 (2009).
31. Namekata, N. *et al.* Non-Gaussian operation based on photon subtraction using a photon-number-resolving detector at a telecommunications wavelength. *Nature Photon.* **4,** 655–660 (2010).
32. Fujiwara, M. & Sasaki, M. Photon-number-resolving detection at a telecommunications wavelength with a charge-integration photon detector. *Opt. Lett.* **31,** 691–693 (2006).
33. Huang, P., Lin, D. K., Huang, D. & Zeng, G. H. Security of continuous-variable quantum key distribution with imperfect phase compensation. *Int. J. Theor. Phys.* **54,** 2613 (2015).
34. Richardson, T. & Urbanke, R. Multi-edge type LDPC codes. in *workshop honoring Prof. Bob McEliece on his 60th birthday*. California Institute of Technology, Pasadena, California, USA (2002).
35. Leverrier, A. & Grangier, P. Continuous-variable quantum key distribution protocols with a discrete modulation. Available at: http://arxiv.org/abs/1002.4083. (Accessed: 15th June 2015).
36. Lin, D. K., Huang, D., Huang, P., Peng, J. Y. & Zeng, G. H. High performance reconciliation for continuous-variable quantum key distribution with LDPC code. *Int. J. Quantum Inf.* **13,** 1550010 (2015).
37. Jouguet, P., Kunz-Jacques, S., Diamanti, E. & Leverrier, A. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A* **86,** 032309 (2012).
38. Huang, P., He, G. Q., Fang, J. & Zeng, G. H. Performance improvement of continuous-variable quantum key distribution via photon subtraction. *Phys. Rev. A* **87,** 012317 (2013).
39. Fang, J., Huang, P. & Zeng, G. H. Multichannel parallel continuous-variable quantum key distribution with Gaussian modulation. *Phys. Rev. A* **89,** 022315 (2014).
40. Soh, D. *et al.* Self-referenced continuous-variable quantum key distribution. *Phys. Rev. X* **5,** 041010 (2015).
41. Qi, B., Lougovski, P., Pooser, R., Grice, W. & Bobrek, M. Generating the local oscillator "locally" in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X* **5,** 041009 (2015).
42. Huang, D., Huang, P., Lin, D. K., Wang, C. & Zeng, G. H. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* **40,** 3695–3698 (2015).
43. Madsen, L. S., Usenko, V. C., Lassen, M., Filip, R. & Andersen, U. L. Continuous variable quantum key distribution with modulated entangled states. *Nature Commun.* **3,** 1083 (2012).
44. Chrzanowski, H. M. *et al.* Measurement-based noiseless linear amplification for quantum communication. *Nature Photon.* **8,** 333–338 (2014).
45. Toshihiko, S., Yoshihisa, Y. & Masato, K. Practical quantum key distribution protocol without monitoring signal disturbance. *Nature* **509,** 475–478 (2014).
46. Ast, S. *et al.* Continuous-wave nonclassical light with gigahertz squeezing bandwidth. *Opt. Lett.* **37,** 2367–2369 (2012).
47. Huang, D., Fang, J., Wang, C., Huang, P. & Zeng, G. H. A 300-MHz bandwidth balanced homodyne detector for continuous variable quantum key distribution. *Chin. Phys. Lett.* **30,** 114209 (2013).
48. Huang, D. *et al.* Continuous-variable quantum key distribution with 1 Mbps secure key rate. *Opt. Express* **23,** 17511 (2015).

Acknowledgements

This work was supported by the National Natural Science Foundation of China (Grants No: 61170228, 61332019, 61471239, 61501290), the Hi-Tech Research and Development Program of China (Grant No: 2013AA122901).

Author Contributions

G.-H.Z. defined the scientific goals and conceived the project. D.H. carried out the whole experiment. P.H. performed the security analysis. D.-K.L. developed the post-processing algorithm. D.H., G.-H.Z and P.H. wrote the manuscript.

Additional Information

Supplementary information accompanies this paper at http://www.nature.com/srep

Competing financial interests: The authors declare no competing financial interests.

How to cite this article: Huang, D. *et al.* Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* **6**, 19201; doi: 10.1038/srep19201 (2016).