Demonstration of high-speed and low-complexity continuous variable quantum key distribution system with local local oscillator

Shengjun Ren¹, Shuai Yang¹, Adrian Wonfor¹, Ian White¹,² & Richard Penty¹,*

We present an experimental demonstration of the feasibility of the first 20 + Mb/s Gaussian modulated coherent state continuous variable quantum key distribution system with a locally generated local oscillator at the receiver (LLO-CVQKD). To increase the signal repetition rate, and hence the potential secure key rate, we equip our system with high-performance, wideband devices and design the components to support high repetition rate operation. We have successfully trialed the signal repetition rate as high as 500 MHz. To reduce the system complexity and correct for any phase shift during transmission, reference pulses are interleaved with quantum signals at Alice. Customized monitoring software has been developed, allowing all parameters to be controlled in real-time without any physical setup modification. We introduce a system-level noise model analysis at high bandwidth and propose a new 'combined-optimization' technique to optimize system parameters simultaneously to high precision. We use the measured excess noise, to predict that the system is capable of realizing a record 26.9 Mb/s key generation in the asymptotic regime over a 15 km signal mode fibre. We further demonstrate the potential for an even faster implementation.

Quantum key distribution (QKD) allows a common random secure key exchange between two authenticated users, Alice and Bob, connected via an insecure quantum channel that can be manipulated by an eavesdropper—Eve¹–⁴. Unlike conventional public-key cryptography which assumes that the required computational complexity is too great for practical breaking of encryption, the critical information in a QKD system is unconditionally protected by the fundamental laws of quantum mechanics⁵–⁷. In contrast to dedicated single-photon detector based discrete variable (DV) QKD systems, continuous variable QKD (CVQKD) modulates both quadratures of the electromagnetic field with continuous random data which can be later extracted with shot noise limited coherent detection techniques⁸,⁹ and post-processed to distil secure keys. More importantly, CVQKD systems have the benefit of compatibility with commercial off-the-shelf (COTS) telecom components and exhibit high detection efficiency, enabling low-cost¹⁰ and possibly higher secret key rates over access and metro Dense Wave-length Division Multiplexing (DWDM) network distances¹¹–¹³. The Gaussian-modulated coherent-state (GMCS) protocol of CVQKD has undergone rigorous development to offer both theoretical and experimental security against malicious eavesdropping attacks¹⁴–¹⁶. However, several obstacles have been identified in practical CVQKD systems, especially those associated with a co-transmitted local oscillator (LO) between Alice and Bob. First, the LO can be accessed by Eve, which could result in security loopholes that compromise the secure key generation. Several attacks have been identified which manipulate the LO, for example, LO intensity fluctuation, calibration attack, and wavelength attack. Second, owing to the attenuation loss in the quantum channel, the attenuated LO power arriving at Bob fails to support shot-noise-limited detection over long distances. Third, to achieve a high-efficiency quadrature detection at Bob, the necessary LO intensity required is typically eight orders of magnitude higher than that of the quantum signal. Such a large power disparity requires a dedicated separation technique to mitigate the photon scatter contamination from LO to quantum signals¹⁷,¹⁸.

To overcome these limitations, a second independent narrow linewidth laser of the same centre wavelength located at Bob has been proposed¹⁹–²² to realize a fully protected local LO (LLO). In order to phase lock the independent lasers at two remote ends and ensure the secure key distillation, Alice shares low-intensity reference pulses with Bob to recover the phase drift during transmission and uses a phase rotation scheme to correct for the quadrature measurements in the later reconciliation stage. With the growing understanding of the LLO
CVQKD noise models, various LLO protocols\(^{25-32}\) have been proposed to enhance different aspects of the system performance at the cost of increased system complexity. The primary goal of practical QKD development has been to increase the secret key rate with cost-effective and low complexity system configurations. However, the repetition rates of the GMCS LLO-CVQKD system demonstrations to date have been less than 100 MHz\(^{22,29,30}\), which limit the asymptotic secret key rate to the 7 Mb/s level at metropolitan network scales.

In this work, we propose and demonstrate experimentally a 500 MHz, low-complexity LLO-CVQKD system based on the GMCS protocol. A record asymptotic key rate of 26.9 Mb/s over a 15 km optical fibre length is predicted from experimental results. Higher repetition rates, and hence secure key rates, are expected with higher bandwidth signal generators. In our setup, several AC coupled wideband drivers, and high bandwidth balanced homodyne detectors are employed to break the bandwidth limitation of DC coupled components and low-speed detectors\(^{33}\). Since the previous sequential-LLO CVQKD demonstrations have been run at low repetition rates and the sequentially generated quantum signal and reference signal pulses have relatively large time intervals, several approaches with increased system complexity have been deployed to minimize the phase drift noise induced from the large pulse intervals\(^{33,26,28}\). In contrast, in our system, the high repetition rate leads to very short pulse intervals, resulting in low phase drift noise, enabling us to achieve better performance with a lower complexity configuration.

The customized software enables all system parameters to be easily adjusted without any setup modification. Based upon the noise model analysis at a high repetition rate in this paper, we propose a new ‘combined-optimization’ technique, where two of the most influential parameters for excess noise, modulation variance and reference pulse intensity, are jointly optimized to enhance the predicted key rate performance beyond 20 Mb/s.

By implementing the real-time shot noise calibration, the photon contamination resulting from scattering from adjacent reference pulses is mitigated to maintain a stable low excess noise. The experimental excess noise results over the SMF link are used to validate the combined-optimization method and prove the feasibility of 20 Mb/s-level key generation over metropolitan area distances.

Results

System experimental design. The experimental setup of the high-speed GMCS-LLO-CVQKD system using COTS optical communication components is shown in Fig. 1a. For a commercially installed system, it is clear that two separated laser sources with the same wavelength will be used at Alice and Bob. We emphasize that we have done the experiments with two independent lasers by manually tuning their wavelengths. When the two lasers’ wavelengths are matched, the experimental results and noise performance are equivalent to those collected by laser splitting configuration presented in Fig. 1a. After verifying this, a single frequency laser (SFL, Thorlabs) at 1549.73 nm with a linewidth of about 100 kHz is used, for the convenience of demonstration, as both of the laser source at Alice and the local oscillator (LO) at Bob. Since the coherence length of the source is far less than that of the optical link, the quantum and reference signals arriving at Bob after a long fibre link and the LO signal arriving at Bob after the 3 m beam splitter will be incoherent. A 10:90 beam splitter (BS, Thorlabs) is used to split the laser output, and an optical isolator is located at each arm to avoid back reflections. At Alice, the continuous wave (CW) light is first carved into 0.2 ns pulses at a rate \(f_{\text{puls}}\) of 1 GHz using a 10 GHz LiNbO\(_3\) intensity modulator (AM1, iXblue). Then, the pulse amplitude is modulated by a second 10 GHz LiNbO\(_3\) intensity modulator (AM2, iXblue) with a high extinction ratio, and the phase is modulated by a cascaded pair of 10 GHz electro-optic phase modulators (PM1, PM2, iXblue). The pulse train is converted into interleaved quantum signals and reference pulses, one delayed by 1 ns relative to the other. All synchronization and modulation signals are generated by an arbitrary-waveform generator (AWG, Tektronix AWG 5204) with four 16-bit, 5 GS/s DAC channels. Several identical, 10 GHz AC coupled wideband RF amplifiers (AMP, iXblue) are deployed to drive the modulators in the LLO CVQKD system. The DAC channels and amplifiers have been carefully characterized to ensure their linearity in terms of the signal generation and modulation. The amplified signals are then shifted to the appropriate voltage levels by the bias-tees. Although the gain of the wideband amplifiers is around 30 dB, their 1 dB compression point below 1 GHz (6.32 Vpp max output) is insufficient to provide a necessary, 0—2 \(\pi\) phase modulation voltage swing (typically 8 Vpp to 12 Vpp) required for the GMCS protocol. Therefore, we use a cascaded PM configuration where two PMs (PM1 and PM2) are connected in series. Each PM is driven by an identical wideband RF amplifier and is only responsible for up to \(\pi\) phase modulation. Overall the cascaded PMs allow a linear phase modulation from 0 to 2 \(\pi\). The amplitude and phase of the signal pulses are randomly modulated, using a two-dimensional zero-centred Gaussian distribution with an adjustable modulation variance \(V_A N_0\) (tuned by a variable optical attenuator (VOA)), where \(N_0\) is the shot noise variance. In contrast, the reference pulses are modulated with a fixed intensity \(|E_R|^2\) \(N_0\) and a constant zero phase. This enables the phase sharing scheme to be used to correct for fast phase drift by tracking phase changes in the reference pulses. A 10:90 BS is used to monitor the Alice modulation and a variable optical attenuator (VOA) is placed at the output of Alice to optimize the \(V_A\). After that, the signal and reference pulses propagate through a 15 km standard single mode fibre before arriving at Bob.

At Bob, since the electronic noise increases with detection bandwidth\(^{27}\), it is necessary to have sufficient LO power to satisfy the shot-noise-limited detection when using the 1.6 GHz balanced homodyne detectors (BHD, Thorlabs). A 13 dBm continuous wave LO is deployed to provide sufficient noise to electronic noise ratio of 10 dB at full detector bandwidth. A polarization controller (PC) is used to compensate for polarization drift from environmental perturbations during transmission. Since low-complexity single heterodyne detection is applied to measure the X and P quadratures, both quantum signals and reference pulses are fed into a 90-degree optical hybrid (Kylia) before being detected by two BHDs. A 10-bit oscilloscope (Keysight, DSOS254A) with a 2.5 GHz bandwidth and a full sampling rate of 20 GS/s is used to collect the quadrature information, and the results are sent to a computer for the \(\sqrt{N_0}\) normalization and the following data analysis. The real-time shot noise is
determined by measuring the variance between the signal and reference pulses. Consequently, the effect of the photon leakage from adjacent reference pulses can be tracked and corrected correspondingly.

It is worth noting that our experimental setup is significantly simplified compared to other multiplexing techniques, such as the delay-line setup\textsuperscript{23} and extra homodyne detection module for quantum signal detection\textsuperscript{29} and also has advantages of flexibility in parameter adjustment and high repetition rates.

Data processing unit. The software-based data processing unit of our system consists of three parts: signal preparation at Alice, data measurement and post-analysis at Bob. The diagram of the overall data processing unit, along with a phase recovery scheme is illustrated in Fig. 1b. At Alice, to generate the coherent quantum signal state \( \alpha^S \), a sequence of quadrature values \( X^S_A \) and \( P^S_A \) with Gaussian variance \( V_A \) and zero mean are prepared using an industrial personal computer (IPC). Then, the Gaussian distributed quadrature values are converted into phase-space representation for signal modulation in the AWG. At Bob, the data measurement process collects the \( X \) and \( P \) of signal pulses, reference pulses and real-time shot noise from Ch1 and Ch2 of the oscilloscope. Then, the post-analysis is implemented to recover the phase rotation \( \phi^R \) by estimating the rotation in the reference phase \( \phi^R_{\text{est}} \).
that the reference pulse amplitude should not be too large, to limit the signal-reference pulse interference. Since the system repetition rate $f_{\text{rep}}$ is 500 MHz and the signal and reference pulses are alternatively produced from the light pulses generated by AM1, $f_{\text{pulse}}$ is set to 1 GHz.

At Bob, the quantum signals and reference pulses are detected with a strong LO using heterodyne measurement with a detector efficiency $\eta$. The X and P quadrature results are collected by channel 1 and channel 2 of the 20 GS/s oscilloscope (shown in the blue region) respectively. With a 500 MHz repetition rate, every pair of quantum signal and reference pulses are oversampled by 40 sample points in every repetition period $T_{\text{rep}}$. Within each $T_{\text{rep}}$ interval, four samples from each channel are recorded and sent to the IPC for phase recovery and post-analysis, including the reference pulses’ peak values ($X^B, P^B$), quantum signals’ peak values ($X^A, P^A$) and real-time shot noise measurement ($X^{SN}_A, P^{SN}_B$) using the middle point between each quantum signal and its adjacent reference pulse. It is worth noting that conventionally the pre-calibrated shot noise value is evaluated when only the LO is present (i.e. no signal transmission occurs). In addition, the calibrated shot noise is considered to be constant during communication. However, in practice, any fluctuations in the LO power and the photon leakage from the reference pulse’s tail will inevitably lead to some fluctuations in the real-time shot noise variance. In this paper, the signal and reference pulse quadrature values are analyzed with real-time shot noise measurement values to enhance the measurement accuracy and reduce the phase noise. Finally, as shown in the grey region in Fig. 1b, the collected data are post-analyzed to recover the phase misalignment of the two laser sources. The overall phase drift of the quantum signal $\phi^R$, i.e. the phase rotation between the prepared quantum signal at Alice $\theta^A$, and the received quantum signal at Bob $\theta^B$, can be recovered through its adjacent reference pulse by calculating the phase change $\phi^R = \theta^B - \theta^A$ along with propagation. However, due to the quantum uncertainty of the reference pulses and some practical measurement imperfections, a small amount of phase error $\phi$ exists in the phase estimation, resulting in extra phase noise in the system. The resultant phase change estimation $\phi^R_{\text{est}}$ obtained in the experiment has $\phi$ deviation from the real quantum signal phase drift as

$$\phi^R = \phi^R_{\text{est}} + \phi$$  \hspace{1cm} (1)

With the publicly announced mean reference pulses’ quadrature values at Alice, $\phi^R_{\text{est}}$ can be calculated based on ($X^A, P^A$), as

$$X^R = \sqrt{\frac{T\eta}{2}} (X^A \cos \phi^R_{\text{est}} + P^A \sin \phi^R_{\text{est}})$$  \hspace{1cm} (2)

$$P^R = \sqrt{\frac{T\eta}{2}} (-X^A \sin \phi^R_{\text{est}} + P^A \cos \phi^R_{\text{est}})$$  \hspace{1cm} (3)

Without loss of generality by our prepared zero initial phase angle (i.e., $p^R_A = 0$),

$$\phi^R_{\text{est}} = \tan^{-1} \left( \frac{p^R_A}{X^A} \right)$$  \hspace{1cm} (4)

Such a phase recovery scheme has been verified to maintain the CVQKD security\textsuperscript{21} since the phase of the reference signal is assumed to be manipulable by Eve in standard CVQKD protocols. Consequently, the estimated phase angles are sent back to Alice for correcting the initial quadratures by

$$\left( X^S_A, P^S_A \right) = \left( \frac{\cos(-\phi^R_{\text{est}})}{-\sin(-\phi^R_{\text{est}})} \frac{\sin(-\phi^R_{\text{est}})}{\cos(-\phi^R_{\text{est}})} \right) \left( X^S_A, P^S_A \right)$$  \hspace{1cm} (5)

After the phase recovery process, the measurement bases are almost aligned between Alice and Bob. The data block size is chosen as $10^7$ in our experiment, and we sacrifice 10% of data for parameter estimation.

In our system, we have created a real-time data monitoring and parameter estimation application programming interface (API) to execute real-time data analysis of transmittance $T$, Alice’s variance $V_A$, and the excess noise $\xi_e$ of each data block. The asymptotic key rate is calculated through experimental results.

**Combined-optimization algorithm.** We encourage readers to read the “Methods” section before reading the following section. In the “Methods” section, we present the details of the noise model analysis of our system at high repetition rates and the corresponding secret key rate evaluation. All parameters used in our simulation and experiment are listed in Table 1 and all excess noise sources and their values are listed in Table 2. We use the notations and values defined in the “Methods” section.

Both $V_A$ and $|E^R|^2$ play significant roles in determining the system excess noise and secure key rate. Specifically, a too weak $|E^R|^2$ will introduce an unacceptable large phase noise; while a large $|E^R|^2$ will indeed lead to less phase noise due to the more precise phase estimation. However, this will be at the expense of photon interference and other noise sources (e.g. $\xi_{AM}$ and $\xi_{ADC}$) will increase accordingly at large $|E^R|^2$. The choice of $V_A$, not only jointly determines the excess noise with the reference pulse intensity $|E^R|^2$, but also has a critical influence on the secret key functions in our LLO CVQKD protocol. In previous studies, the two parameters have been calibrated individually with low precision: $V_A$ is numerically optimized at a target distance with a maintained $|E^R|^2$\textsuperscript{29}, while the number of optimal reference pulse photons or $|E^R|^2/V_A$ is normally selected in the regime where $V_A$ is fixed\textsuperscript{29,34}. However, to achieve an optimized system performance, it is necessary to evaluate these two interrelated parameters conjointly. We propose for the first time a combined-optimization method to simultaneously calibrate the two parameters. The combined-optimization method uses a 3-dimensional value
optimization where the system performance (secure key rate or excess noise) is evaluated by \( V_A \) ranging from 0 to 10 with a resolution of 0.01, and the reference pulse intensity \( |E_R|^2 \) varies between 0 and 4000 with an interval of 1. All values are normalized to shot noise units. Following the analysis of our system shown above, the theoretical system performances at 15 km, in terms of secure key rate and excess noise, for various \( V_A \) and \( |E_R|^2 \) are shown in Fig. 2a,b, respectively.

The combined-optimization results among \( V_A \), \( |E_R|^2 \) and key rate are shown in Fig. 2a. The secret key rate relies heavily on both parameters, and the global maximum can be estimated using our combined searching method. The peak key rate of 27.3 Mb/s is marked as a black star and occurs when \( V_A=2.52 \) and \( |E_R|^2=1056 \). Any other combinations have shown to reduce the key rate performance and the choices of \( V_A \) and \( |E_R|^2 \) should be limited within a certain range to ensure high rates of secure key exchange (\( V_A \in [2.05, 3.10] \) and \( |E_R|^2 \in [750, 1400] \)). We also demonstrate the corresponding excess noise \( \xi_e \) performance with respect to different \( V_A \) and \( |E_R|^2 \) combinations in Fig. 2b. At the key rate peak represented as a black star, the excess noise \( \xi_e \) is 0.083. One can note from the figure that a low \( \xi_e \), and hence a low \( \chi_{BE} \), does not necessarily lead to a high key rate since \( V_A \) also participates in the mutual information evaluation \( I_{AB} \) between Alice and Bob. For instance, the region of low excess noise operation, \( \xi_e <10^{-3} \), as shown as the dark blue region in Fig. 2b, can be achieved when \( V_A \) and \( E_R^2 \) are both small enough. However, a small \( V_A \) will significantly reduce \( I_{AB} \), which in turn results in a tiny or even null useful key exchange. Similarly, even with a fixed \( V_A \), either too small or too large \( |E_R|^2 \) will also increase the system excess noise \( \xi_e \) and hence lead to poor system performance. The highest achievable key rate for each \( V_A \) choice occurs at the optimal \( |E_R|^2 \) is located at the valley line shown in Fig. 2b. As a result, both \( E_R^2 \) and \( V_A \) need calibration, and it is of utmost importance to implement the combined-optimization method to find the global maximum key rate point. In our system, these two parameters can be freely adjusted within the software.

Combined-optimization method experimental validation. In order to demonstrate the effectiveness of the combined-optimization method and verify the relationship between \( |E_R|^2 \) and the excess noise \( \xi_e \) at the pre-defined \( V_A \), we compare the simulated excess noise \( \xi_e \) with experimental measurements for a range of reference pulse intensities over a 15 km optical fibre link at the optimal \( V_A=2.52 \). The excess noise measurement is similar to that in conventional CVQKD systems. We evaluated the excess noise using a linear model \( y_i = \frac{\sqrt{T}}{2} x_i + z \), where \( x_i \) and \( y_i \) are correlated variables at Alice and Bob, and \( z \) is the overall noise following a zero centred normal distribution with a variance of \( \sigma^2 = \frac{nT}{T} \xi_e + 1 + v_{iec} \). By exchanging 10% of the corrected raw data, we can estimate the overall excess noise \( \xi_e \) of our system. The excess noise along with the corresponding calculated key rates, are shown in Fig. 3. As can be seen, the measured excess noise (grey circles) with \( \pm 0.01 \) error at six different \( |E_R|^2 \) are a good fit to the theoretical excess noise derivation (blue line) calculated by Eq. (16). The minimum excess noise in the experiment is 0.085 at \( |E_R|^2=1050 \). The slightly higher experimental excess noise is likely due to the small overestimation in the original system excess noise. The excess noise exceeds the null key threshold \( \xi_e = 0.167 \) when \( |E_R|^2 \) is either smaller than 185 or larger than 6000, which proves the relationship between \( |E_R|^2 \) and \( \xi_e \). The theoretical secure key rate is drawn as an orange dashed line, and the experimental key rates predicted with the measured excess noise values are represented as grey squares. The experimental key rates are slightly smaller than simulation results but overall follow the theoretical trend. The key rate is verified to be inversely proportional to the excess noise at a fixed \( V_A \) and the highest key rate of 26.9 Mb/s occurs at the minimum excess noise. Therefore, the practical optimal \( |E_R|^2 \) is confirmed as 1050 at \( V_A = 2.52 \) which validates the feasibility of our proposed combined-optimization method.

Excess noise stability and secure key rate performance. With the setup and optimal parameters discussed above, we investigate the practical system stability in terms of fluctuations in real-time excess noise \( \xi_e \).

The experimental results of excess noise over 50 consecutive data blocks (each with \( 10^7 \) signals) over the 15 km SMF optical fibre link are collected. The received data in each data block follows a Gaussian distribution. The phase noise variance is suppressed to \( V_{phase} \approx 0.01 \) by the phase recovery scheme. As shown in Fig. 4a, the excess noise measurements of each data block are marked as blue dots and can be seen to take values between 0.06 to 0.1. A small variation in the real-time excess noise is caused by the output fluctuation of the LO and the statistical errors in the parameter estimation process. The calculated average excess noise \( \xi_{ave}^{exp} \) shown as the red surface is 0.085, which is almost the same as the theoretical excess noise 0.083 obtained by the combined-optimization method. In order to demonstrate the key rate performance of the collected excess noise values intuitively, we draw several secure key rate thresholds in Fig. 4a. These thresholds are obtained from Fig. 4b where the asymptotic secure key rate estimation as a function of \( \xi_e \) is plotted. The null key, 10 Mb/s, 20 Mb/s, 30 Mb/s and 40 Mb/s estimated secret key rates can be achieved by excess noise values of 0.167, 0.134, 0.104, 0.076 and 0.052 respectively. The average measured excess noise 0.085 contributes to 26.9 Mb/s predicted secure key rate and all our measured excess noise values are less than 0.1, which guarantee a stable secure key rate generation greater than 20 Mb/s in the asymptotic regime. It is worth noting that the excess noise can be further reduced if complicated multiplexing and separate detection techniques are employed. The simulation predictions of key rate performance at 100 MHz, 250 MHz and 500 MHz repetition rate with respect to different transmission distances, together with measured results from the experiments, are shown in Fig. 5. Previous LLO CVQKD asymptotic regime experimental results are also shown in Fig. 5 for performance comparison. The combined-optimization method is applied every 0.1 km to adjust \( V_A \) and \( |E_R|^2 \), which ensures the optimal asymptotic theoretical key rates (solid lines) under each repetition rate scenarios. All other experimental parameters are listed in Table 1 and remain unchanged over different transmission distances.
We experimentally measured the excess noise of 50 data blocks over the 15 km link at these three repetition rates. Based on the average excess noise values $\xi_{\text{100M}} = 0.084$, $\xi_{\text{250M}} = 0.082$ and $\xi_{\text{500M}} = 0.085$ collected in the experiments, the asymptotic final key rates are computed as 25.5 Mb/s (red circle), 14.2 Mb/s (red cross) and 26.9 Mb/s (red diamond) at 100 MHz, 250 MHz and 500 MHz repetition rate respectively. The experimental results match the simulation results of the theoretical model, and we can further predict that the transmission distance of our 500 MHz system can reach 43 km beyond which the excess noise will rise above the null key threshold. It can be seen that the final predicted key rate is not perfectly linear with the repetition rate and the excess noise obtained at 250 MHz repetition rate is lower than the other two cases. This is because the phase drift noise $\xi_{\text{drift}}$ plays an important role at relatively low rates and decreases with the increase of repetition rate. However, when the repetition rate goes higher, the effective resolution bit of DAC, and the electronic noise start to limit the key rate. The experimental results have verified the feasibility of implementing an asymptotic 20 + Mb/s low-complexity LLO-CVQKD system of over 15 km optical fibre link. When finite-size effects, with a data block size of $10^7$ and 10% data scarification for parameter estimation, are considered following the calculation described in, the average worst excess noise of our system under the finite size effect is around 0.106 and the predicted key rate is 15.9 Mb/s. Further increase in the data block size can improve the key rate performance, achieving the key rate of 20.8 MBps with data block size of 10^7 and key rate of 22.7 MBps with data block size of 10^10. Since the bandwidths of all optical components are in order of GHz, our system remains potential for higher key rate by further pushing the repetition rate beyond current limitations.

**Discussion**

We present a low complexity 500 MHz pulse repetition rate LLO-CVQKD system that could enable a record asymptotic key rate of 26.9 Mb/s over a 15 km optical fibre to be predicted from experimental results. In terms of the system setup design, we deploy a low-complexity configuration with real-time software control to realize a cost-effective system with a high degree of adjustment flexibility. A set of wideband components and a continuous wave LO are used to overcome the repetition rate limitation of previous LLO CVQKD systems. The combined-optimization method and the real-time shot noise calibration are integrated through comprehensive noise model analysis to achieve a stable low excess noise performance. Investigation of the post-processing procedures and block size increments will be carried out in the future. Currently, the repetition rate is limited mainly by the bandwidth of the electrical signal generation equipment, and there is no fundamental reason why GHz pulse repetition rate systems are not achievable. This work verifies the feasibility of 20 Mb/s secure key rates in LLO CVQKD and paves the way for the cost-effective quantum communications in practical applications.

**Methods**

**Noise model analysis.** Optimal performance requires a comprehensive noise analysis, especially for the excess noise that arises from the experimental imperfections and noise introduced by Eve’s manipulation. We derive the noise model of our system at high repetition rates and all noise sources presented here are referred to as the channel input noise and are normalized to shot noise unit $N_0$.

**Phase noise.** In an LLO CVQKD system, owing to the random relative phase drift between two free-running lasers, the main experimental challenge is to agree on a common phase reference between Alice and Bob. According to Eq. (1), even though the phase recovery scheme has been employed for the drift amendment, the phase rotation of the quantum signals cannot be completely corrected through the phase drift estimation of the reference pulse. We have considered the system security where the phase noise is not trusted. The phase noise $\xi_{\text{phase}}$ is one of the most critical contributions to the excess noise that limits the performance of the LLO CVQKD system. Under the GMCS protocol with $V_A$, the phase noise is assumed to be Gaussian distributed with a variance $V_{\text{phase}}$ which represents the variance of residual phase error $\phi$ 19. The $\xi_{\text{phase}}$ has contributions from three uncertainties: (1) phase estimation error noise $\xi_{\text{esti}}$, (2) drift noise induced from laser sources $\xi_{\text{drift}}$, and (3) drift noise induced from the propagation length difference between quantum signals and reference pulses $\xi_{\text{Ch}}$. Their relationship can be modeled as:

$$\xi_{\text{phase}} = \xi_{\text{esti}} + \xi_{\text{drift}} + \xi_{\text{Ch}} \approx V_A \ast V_{\text{phase}}$$

where $V_{\text{phase}}$ is:

$$V_{\text{phase}} = \text{var}(\psi_{\text{esti}} - \psi) = \text{var}(\phi)$$

The phase estimation error noise $\xi_{\text{esti}}$ is originated from reference pulse quantum uncertainty $V_{\text{esti}}$ at the detector due to the fundamental shot noise and total noise $\chi_{\text{tot}}$ of our system. It describes noise induced from the deviation between the exact phase $\psi^R$ and the measured phase $\psi_{\text{esti}}^R$ of the reference pulse. The value is inversely proportional to the reference pulse intensity $|E^R|^2$ at the Bob output as,

$$\xi_{\text{esti}} = V_A \ast \text{var}(\psi_{\text{esti}}^R - \psi^R) = \frac{V_A \ast (\chi_{\text{tot}} + 1)}{|E^R|^2}$$

The drift noise $\xi_{\text{drift}}$ results from the phase frames instability of two independent free-running laser sources with the spectrum linewidths $\Delta v_A$ and $\Delta v_B$ at Alice and Bob respectively. Due to the temporal separation of the generation of the quantum signal and reference pulse, the relative phase drift $\xi_{\text{drift}}$ can be modeled as a Gaussian stochastic process centered at the laser central frequency. The value can be characterized by the variance of phase drift $V_{\text{drift}}$ within a half repetition interval $1/2$.
\[
\xi_{\text{drift}} = V_A \ast \text{var}(\theta_A^R - \theta_A^S) = V_A \ast \pi \frac{\Delta V_A + \Delta V_R}{f_{\text{rep}}}
\]

In our system, with a narrow laser linewidth of 100 kHz and a high repetition rate \( f_{\text{rep}} = 500 \, \text{MHz} \), the \( V_{\text{drift}} \) is suppressed within the order of \( 10^{-3} \, \text{rad}^2 \).

The \( \xi_{\text{Ch}} \) represents the relative phase drift accumulated by the quantum signal and reference pulse during propagation. The value is assumed to be dominated by the optical path length difference of two components. In our system, the optical path of two components are the same, the phase rotations accumulated by two components \( \theta_{\text{Ch}}^R \) and \( \theta_{\text{Ch}}^S \) are hence identical.

\[
\xi_{\text{Ch}} = V_A \ast \text{var}(\theta_{\text{Ch}}^R - \theta_{\text{Ch}}^S) \approx 0
\]

**Conversion noise.** In our system, two types of conversion noise are induced by the imperfect conversion between digital bits and analogue voltages. The first occurs at Alice's modulation voltage preparation. When the AWG and wideband drivers are used to translate signal bits into analogue modulation voltages, the modulation voltage fluctuation \( \Delta U_{\text{mod}} \) is caused by the imperfect conversion of those components and the adjacent sample interferences in the amplification process. Based on the analysis in\(^\text{27}\), such fluctuation noise \( \xi_{\text{fluc}} \) can be evaluated as:

\[
\xi_{\text{fluc}} = V_A \left( \pi \frac{\Delta U_{\text{mod}}}{U_\pi} + \frac{1}{2} \pi^2 \frac{\Delta U_{\text{mod}}^2}{U_\pi^2} \right)^2
\]

where \( U_\pi \) is the voltage assigned to the phase modulator to achieve a \( \pi \) phase modulation.

The second conversion noise is the ADC quantization noise \( \xi_{\text{ADC}} \) that appears in Bob's detection process. The output voltages of BHDs are sent to an oscilloscope and digitized by the ADCs. Also, with the same sampling rate, the effective resolution bit number \( n_{\text{eff}} \) of ADC decreases with the increment of the ADC input frequency, specifically 1 bit of \( n_{\text{eff}} \) is lost for every doubling of the ADC input frequency\(^\text{38}\). Such \( \xi_{\text{ADC}} \) can be evaluated as\(^\text{27,40}\)

\[
\xi_{\text{ADC}} = \frac{u t_s}{h f^2 \rho^2 P_{\text{LO}} \eta T} \ast \frac{U_{\text{full}}^2}{12 \times 2^{2n_{\text{eff}}}}
\]

where \( u = 1 \) for homodyne detection and \( u = 2 \) for heterodyne detection, \( t_s \) is the signal pulse duration, \( U_{\text{full}} \) is the full voltage range of the ADC, \( h \) is Planck's constant. \( f \) is the laser frequency, \( \rho \) is the gain factor of the transimpedance amplifier (TIA, V/A), \( \eta \) is the photodiode responsivity (A/W), \( P_{\text{LO}} \) is the LO power at Bob, and \( n_{\text{eff}} \) is the effective number of bit of the ADC at our system pulse rate. To recover all quantum states correctly, \( U_{\text{full}} \) needs to cover the full voltage range of the received signals, which means \( U_{\text{full}} \) needs to be larger than the reference pulse voltage range \( U_R \):

\[
U_{\text{full}} \geq U_R = \sqrt{g \rho \ast \frac{\left| E^R \right|^2 h f}{t_s} \ast \eta T \ast \sqrt{g \rho P_{\text{LO}}}}
\]

Combine Eq. \( 12 \) and Eq. \( 13 \), the lower bound of \( \xi_{\text{ADC}} \) can be calculated by:

\[
\xi_{\text{ADC}}^{\text{min}} = \frac{u \left| E^R \right|^2}{12 \ast 2^{2n_{\text{eff}}}}
\]

As can be seen for CVQKD systems operating at high repetition rates, due to the reduction in \( n_{\text{eff}} \) at high speed, the ADC quantization noise will play an essential role in determining the excess noise and hence the system performance.

**AM dynamic range noise.** During the signal preparation stage at Alice, the interleaved intense reference pulses and the weak quantum signals are generated using a single amplitude modulator (AM2) with a finite dynamic range. After we generate the reference pulse, the finite dynamic range of AM2 will induce amplitude leakage on the weak quantum signal and introduce AM dynamic range noise \( \xi_d \) on the quadratures of quantum signals\(^\text{23}\). With a reference pulse intensity \( \left| E^R \right|^2 \) and an extinction ratio \( \tau_{\text{AM2}} \) (in dB), the \( \xi_d \) can be approximated as

\[
\xi_d = \left| E^R \right|^2 10^{-\tau_{\text{AM2}}/10}
\]

Compared with the large photon-leakage noise induced by the split and combination of quantum signal and reference pulse in the delay-line scheme\(^\text{28}\), our system does not require split and combination interferometer and delay line at both Alice and Bob and hence has zero photon-leakage noise. Other noise contributions such as relative intensity noise, common-mode rejection ratio noise and BHD imbalanced drift noise, are deemed small enough in our experimental setup to be included within the original system excess noise \( \xi_{\text{ori}} = 0.01 \). The overall excess noise model can be described as:

\[
\xi_e = \xi_{\text{ori}} + \xi_{\text{esti}} + \xi_{\text{drift}} + \xi_{\text{Ch}} + \xi_{\text{ADC}} + \xi_{\text{fluc}} + \xi_d
\]
Figure 2. The demonstration of the proposed combined-optimization method with respect to different $V_A = [0, 10]$ and $E_{ref} = [0, 4000]$ at $L = 15$ km and $f_{ref} = 500$ MHz. All other parameters used in the estimations are listed in Methods section. (a) The secure key rate analysis for various $V_A$ and $|E_R|^2$. The key rate peak (the black star) in the simulation is 27.3 Mbps obtained when $V_A = 2.52$ and $|E_R|^2 = 1056$. (b) The excess noise evaluation for various $V_A$ and $|E_R|^2$. The excess noise at the key rate is 0.083 and the optimal $|E_R|^2$ is located in the valley of the graph.

Figure 3. Experimental validation of noise model and optimization method by collecting excess noise at different $|E_R|^2$ with a fixed optimal $V_A = 2.52$ and $L = 15$ km. The blue solid line represents the theoretical excess noise evaluation and the grey circles with ± 0.01 error bars denote the measured excess noises with a data block size of $10^7$. The dashed orange line represents the theoretical secure key rate performance and the grey squares are the corresponding secure key rate with measured excess noises. The black line is the null key threshold with $\xi = 0.167$. The peak secure key rate occurs at the minimum excess noise point with $|E_R|^2 = 1050$. Other parameters are listed in Table 1 in the “Methods” section.

Electronic noise. In this paper, we adopt the assumption of the trusted detector model widely used in an LLO CVQKD system\(^{20-26}\), where the electronic noise $V_{ele}$ and the efficiency associated with the detector $\eta$ are well-protected from Eve. The electronic noise arises from the thermal noise inside the BHD. The electronic to shot noise ratio should be low enough to achieve a precise quantum signal detection. The electronic noise in shot noise unit at the inputs of detectors can be expressed as\(^{27,40}\):

$$V_{ele} = \frac{NEP^2_{ele} B}{T_{LO} h \nu_{PLO}}$$

(17)
Figure 4. Excess noise stability in our LLO CVQKD system. (a) Experimental measurement of excess noise. The blue dots represent the collected excess noise at each data block and the red surface is their average value. Surfaces with different colours are theoretical secure key rate thresholds for null key, 10 Mb/s, 20 Mb/s, 30 Mb/s and 40 Mb/s secret key rates. (b) Secure key rate with respect to different excess noises where $L = 15$ km and $f_{\text{rep}} = 500$ MHz. The stars denote the secure key rates at different excess noise thresholds shown in Fig. 4a and the red star represents the secure key rate with an average measured excess noise $\xi_{\text{ave}} = 0.085$.

Figure 5. The secret key rate performance of our LLO CVQKD system. The secret key rate as a function of transmission distance at 100 MHz, 250 MHz and 500 MHz repetition rates, together with the average experimental measurements of excess noises over a 15 km SMF fibre. The red circle, cross and diamond represent the estimated key rate of 5.5 Mbps, 14.2 Mbps and 26.9 Mbps at 100 MHz, 250 MHz and 500 MHz repetition rates respectively. The data block size is $10^7$. $V_A$ and $|E_\text{R}|^2$ are optimized every 0.1 km using the combined optimization method and other parameters are listed in "Methods".
where $B$ is the bandwidth of the detector, which is chosen to be $3f_{\text{rep}}$ in our system, $\text{NEP}_{\text{ele}}$ is the noise equivalent power of the BHD at $B$, and $r_{\text{LO}}$ is the rate of incoming signals interfering with LO, which is equivalent to pulse generation rate in this system. The electronic noise increases with system repetition rate, but it can be improved with an increased LO power. The electronic noise of our system is verified experimentally as 0.1.

The linear model to represent the quadrature values measured by Bob with a transmittance $T$ and a heterodyne detection efficiency $\eta$ is derived as:

$$X_{S_{B}} = \sqrt{\frac{T}{2}} \left( X_{\xi} + X_{N} \right) + \left( \frac{cos(\psi_{\xi})}{P_{A}} \right) \left( \frac{X_{\xi}^{R}}{P_{A}} \right) + \left( \frac{X_{\xi}^{\prime}}{P_{A}} \right)$$ (18)

where the rotation matrix applied to the initial signal quadratures accounts for the phase noise while $X_{\xi}$ and $P_{\xi}$ represent the phase-noise-exclusive excess noise. $X_{N}$ and $P_{N}$ are vacuum quadratures of unit shot noise variance $N_{e}$. $X_{\xi}$ and $P_{\xi}$ are electronic noise quadratures with variance $V_{\text{ele}}$.

All parameters used in our simulation and experiment are listed in Table 1.

To clearly show the order of magnitude of the different excess noise sources at 500 MHz repetition rate, the contributions of all excess noise sources and their values are listed in Table 2.

**Secret key rate evaluation.** The asymptotic secret key estimation of our LLO-CVQKD scheme follows the same procedures used in a conventional CVQKD system [12]. Under a collective attack with heterodyne detection and reverse reconciliation, the secure key rate $K_{\text{col}}$ is:

$$K_{\text{col}} = f_{\text{rep}} \beta I_{A_B} - X_{BE}$$ (19)
where $\beta$ is the reconciliation efficiency, $I_{AB}$ is the mutual information between Alice and Bob, and $\chi_{BE}$ is the upper bound of Eve’s information related to the Holevo bound\cite{32}. $I_{AB}$ with heterodyne detection can be derived through Shannon equation as\cite{32}:

$$I_{AB} = \log_2 \frac{V_B}{V_{B/A}} = \log_2 \frac{V_A + 1 + \chi_{tot}}{1 + \chi_{tot}}$$  \hspace{1cm} (20)

The total noise $\chi_{tot}$ of our system has two contributions: the line noise $\chi_{line}$, and the imperfect detection noise $\chi_{het}$. The line noise $\chi_{line}$ induced in the channel consists of transmission loss and all untrusted noises referred to the channel input and can be expressed as $\chi_{line} = \frac{1}{\eta} - 1 + \xi_e$. According to the heterodyne detection setup for reference pulses and quantum signals, the noise introduced by the detector can be expressed as $\chi_{het} = \frac{1}{\eta}(-\eta + 2\sqrt{\eta})$. The information accessed by Eve $\chi_{BE}$ can be evaluated by the Von Neumann entropy $S(.)$ using the symplectic eigenvalues\cite{32} of the covariance matrix. The derivation of $\chi_{BE}$ in our system follows exactly the same as that of a conventional CV-QKD system, but with an updated excess noise model in $\chi_{line}$. The mutual information between Eve and Bob is given by:

$$\chi_{BE} = \sum_{i=1}^{2} G(\frac{\lambda_i - 1}{2}) + \sum_{i=3}^{5} G(\frac{\lambda_i - 1}{2})$$  \hspace{1cm} (21)

where $G(x) = (x + 1) \log_2(x + 1) - x \log_2 x$, and $\lambda_i$ are the symplectic eigenvalues. Specifically

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

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

and $\lambda_5 = 1$, where

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

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

$$C = \frac{1}{(T(V + \chi_{line}))^2}$$

$$D = \left( \frac{V + \sqrt{\chi_{het}}}{T(V + \chi_{line})} \right)^2$$  \hspace{1cm} (25)

**Data availability**

The data that support the findings of this study are available in Apollo, the University of Cambridge Repository with the identifier https://doi.org/10.17863/CAM.68384.

Received: 14 December 2020; Accepted: 25 March 2021

Published online: 04 May 2021

**References**

1. Bennett, C. & Brassard, G. Quantum cryptography: Public key distribution and coin tossing. in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 175–179 (IEEE Press, New York, 1984).

2. Ekert, A. K. Quantum cryptography based on Bell’s theorem. \textit{Phys. Rev. Lett.} \textbf{67}, 661–663 (1991).

3. Scarani, V. et al. The security of practical quantum key distribution. \textit{Rev. Mod. Phys.} \textbf{81}, 1301–1350 (2009).

4. Lo, H. K., Curty, M. & Tamaki, K. Secure quantum key distribution. \textit{Nat. Photonics} \textbf{7}, 022339 (2013).

5. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. Science (80-) \textbf{283}, 2050–2056 (1999).

6. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. \textit{Phys. Rev. Lett.} \textbf{85}, 441–444 (2000).

7. Mayers, D. Unconditional security in quantum cryptography. \textit{J. ACM} \textbf{48}, 351–406 (2001).

8. Ralph, T. C. Continuous variable quantum cryptography. \textit{Phys. Rev. A} \textbf{61}, 1 (2000).

9. Braunstein, L. S. & Van Loock, P. Quantum information with continuous variables. \textit{Rev. Mod. Phys.} \textbf{77}, 513–577 (2005).

10. Diamanti, E. & Leverrier, A. Distributing secret keys with quantum continuous variables: Principle, security and implementations. \textit{Entropy} \textbf{17}, 6072–6092 (2015).

11. Weedbrook, C. et al. Gaussian quantum information. \textit{Rev. Mod. Phys.} \textbf{84}, 621–669 (2012).

12. Wang, C. et al. 25 MHz clock continuous-variable quantum key distribution system over 50 km fibre channel. \textit{Sci. Rep.} \textbf{5}, 1–8 (2015).

13. Huang, D. et al. Continuous-variable quantum key distribution with 1 Mbps secure key rate. \textit{Opt. Express} \textbf{23}, 17511 (2015).

14. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. \textit{Phys. Rev. Lett.} \textbf{88}, 4 (2002).

15. Grosshans, F. et al. Quantum key distribution using Gaussian-modulated coherent states. \textit{Nature} \textbf{421}, 238–241 (2003).

16. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. \textit{Nat. Photonics} \textbf{7}, 378–381 (2013).

17. 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. \textit{Phys. Rev. A} \textbf{80}, 022339 (2013).

18. Jouguet, P., Kunz-Jacques, S. & Diamanti, E. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. \textit{Phys. Rev. A} \textbf{87}, 062313 (2013).

19. Huang, J. Z. et al. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. \textit{Phys. Rev. A} \textbf{87}, 062329 (2013).
20. Qi, B., Lougovski, P., Posser, 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).

21. Soh, D. B. S. *et al.* Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X* 5, 041010 (2015).

22. Huang, D., Huang, P., Lin, D., Wang, C. & Zeng, G. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.* 40, 3695 (2015).

23. Marie, A. & Alleaume, R. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Phys. Rev. A* 95, 012316 (2017).

24. Ren, S. *et al.* Reference pulse attack on continuous variable quantum key distribution with local local oscillator under trusted phase noise. *I. Opt. Soc. Am. B* 36, B7 (2019).

25. Corvaja, R. Phase-noise limitations in continuous-variable quantum key distribution with homodyne detection. *Phys. Rev. A* 95, 022315 (2017).

26. Klein, S., Rueckmann, M. & Schaeffer, C. G. Continuous variable quantum key distribution with a real local oscillator using simultaneous pilot signals. *Opt. Lett.* 42, 1588 (2017).

27. Laudenbach, F. *et al.* Continuous-Variable Quantum Key Distribution with Gaussian Modulation-The Theory of Practical Implementations. *Adv. Quantum Technol.* 1, 1800011 (2018).

28. Wang, T., Huang, P., Zhou, Y., Liu, W. & Zeng, G. Pilot-multiplexed continuous-variable quantum key distribution with a real local oscillator. *Phys. Rev. A* 97, 012310 (2018).

29. Wang, T. *et al.* High key rate continuous-variable quantum key distribution with a real local oscillator. *Opt. Express* 26, 2794 (2018).

30. Wang, H. *et al.* High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. *Opt. Express* 28, 32882 (2020).

31. Ye, W. *et al.* Improvement of self-referenced continuous-variable quantum key distribution with quantum photon catalysis. *Opt. Express* 27, 17186 (2019).

32. Su, Y., Guo, Y. & Huang, D. Kalman filter-based phase estimation of continuous-variable quantum key distribution without sending local oscillator. *Phys. Lett. Sect. A. Gen. At. Solid State Phys.* 383, 2394–2399 (2019).

33. Qi, B. & Lim, C. C. W. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator. *Phys. Rev. Appl.* 9, 054008 (2018).

34. Ren, S. *et al.* Noise and Security Analysis of Trusted Phase Noise Continuous Variable Quantum Key Distribution using a Local Local Oscillator. in *IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC 2019-July* (Institute of Electrical and Electronics Engineers Inc., 2019).

35. Milovancev, D. *et al.* Spectrally-shaped continuous-variable QKD operating at 500 MHz over an optical pipe lit by 11 DWDM channels. in *Optics InfoBase Conference Papers Part F174-, T3D.4* (OSA—The Optical Society, 2020).

36. Ren, S., Yang, S., Wordor, A., Penny, R. & White, I. Demonstration of Robust Self-Referenced Continuous Variable Quantum Key Distribution over 25km Fibre Link. in *2020 Conference on Lasers and Electro-Optics, CLEO 2020—Proceedings FF3C.4* (2020).

37. Huang, D., Huang, P., Lin, D. & Zeng, G. Long-distance continuous-variable quantum key distribution by controlling excess noise. *Sci. Rep.* 6, 1–9 (2016).

38. Lodewyck, J., Debuisschert, T., Tualle-Broui, R. & Grangier, P. Controlling excess noise in fibre-optics continuous-variable quantum key distribution. *Phys. Rev. A* At. Mol. Opt. Phys. 72, 050303 (2005).

39. Walden, R. H. Analog-to-digital converter survey and analysis. *IEEE J. Sel. Areas Commun.* 17, 539–550 (1999).

40. Tang, X. *et al.* Performance of continuous variable quantum key distribution system at different detector bandwidth. *Opt. Commun.* 471, 126034 (2020).

41. Holevo, A. S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Peredachi Informatsii* 9, 3–11 (1973).

42. Shannon, C. E. A communication. *Bell Syst. Tech. J.* 27, 379–423 (1948).

43. Von Neumann, J., Beyer, R. T. (Robert T. & Goldstine, H. H. (Herman H. Mathematical foundations of quantum mechanics. (Princeton University Press, 1955).

44. Fossier, S., Diamanti, E., Debuisschert, T., Tualle-Broui, R. & Grangier, P. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. *J. Phys. B At. Mol. Opt. Phys.* 42, 114014 (2009).

**Acknowledgements**

We would like to acknowledge support from the UK EPSRC through the Quantum Technology Hub for Quantum Communications Technologies, project EP/M013472/1 and the EPSRC Quantum Communications Hub, project EP/T001011/1.

**Author contributions**

S.R. developed the theory and analyzed the noise model. S.R., S.Y. and A.W. designed the system. S.R. and S.Y. performed the experiment. A.W., R.P. and I.W. provided experimental assistance and suggestions. R.P. and I.W. supervised the work. S.R. analyzed the experimental results and wrote the manuscript with input from all authors.

**Competing interests**

The authors declare no competing interests.

**Additional information**

**Correspondence** and requests for materials should be addressed to R.P.

**Reprints and permissions information** is available at [www.nature.com/reprints](http://www.nature.com/reprints).

**Publisher’s note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.
