communications physics

A Nature Portfolio journal

Article

https://doi.org/10.1038/s42005-025-02317-5

Enhanced continuous-variable quantum key distribution protocol via adaptive signal processing

Özlem Erkılıç [1,5] ✉, Biveen Shajilal [1,2,5], Lorcán O. Conlon [1,2], Angus Walsh[1], Aritra Das [1], Sebastian Kish[3], Thomas Symul[4], Ping Koy Lam [1,2], Syed M. Assad[1,2] & Jie Zhao [1] ✉

Quantum key distribution (QKD) provides secure communication using quantum mechanics, with continuous-variable QKD (CV-QKD) being an attractive solution due to its compatibility with existing telecommunication technology. Its main drawback is susceptibility to signal loss in fibres and free-space links, including satellites, which limits performance. Here we show a software-based protocol enhancing CV-QKD by applying adaptive filters at the transmitter and receiver, allowing the system to dynamically respond to changing channel conditions. Our security analysis avoids relying on Gaussian extremality, giving accurate bounds on an eavesdropper's information. The protocol can also extract keys in regions that would normally be considered insecure. We demonstrate a threefold increase in secret-key rates compared with the best existing CV-QKD protocol, and in satellite simulations, up to a 400-fold improvement. Because it requires no hardware modifications, our method can be readily integrated into existing systems, paving the way for more practical and robust quantum communication networks.

Quantum key distribution (QKD) is a method used to securely establish a secret key between two distant parties, Alice and Bob[1–3]. One variant of QKD is continuous-variable (CV) protocols, where keys are encoded in the amplitude and phase quadratures of the optical field and measured using heterodyne or homodyne detection[4,5]. CV-QKD can be categorised into different types, one of which includes protocols with Gaussian modulation (GM), where coherent states are modulated with a Gaussian distribution[6–16]. The most commonly used CV-QKD protocol with GM is the GG02 protocol[6–8], which optimises the variance of Gaussian modulation for each transmission distance to achieve the best key rates. A key step in QKD is parameter estimation, which is often performed after error reconciliation to assess channel noise and loss, helping to bound Eve's information[17]. This helps optimise experimental parameters, assuming the channel varies slowly. However, if parameter estimation falls within a non-secure region, key data must be discarded, and rapid variations like atmospheric scintillation can render these estimates ineffective.

In CV-QKD, passive methods that do not require feedback loops to optimise experimental parameters can enhance key rates by employing quantum processes such as noiseless linear amplifiers (NLAs)[18,19], phase-sensitive amplifiers[20], photon subtraction[21,22], and photon catalysis[22–24]. While these techniques can increase key rates, they are challenging to implement. Recent post-selection protocols emulate such physical processes using digital filtering, where applying a quantum process becomes equivalent to first detecting the quantum state and then digitally filtering the measured outcomes. This approach is particularly useful for point-to-point applications like QKD. For example, measurement-based NLA (MB-NLA) replaces physical NLAs by employing Gaussian post-selection on detection outcomes. This approach extends the transmission distance of CV-QKD[25–27] and also provides overall performance enhancements in CV-based quantum communications[28–31]. Similar approaches have been applied to photon subtraction and photon catalysis protocols, where physical processes are replaced with non-Gaussian virtual photon-subtraction[32,33] and Gaussian zero-photon catalysis post-selection[34]. However, since these methods still emulate physical processes, the post-selection filters are constrained by the characteristics of those processes. Additionally, these protocols rely on Gaussian extremality, which states that Gaussian states maximise the von Neumann entropy for a given covariance matrix[35,36]. This results in an

[1]Centre of Excellence for Quantum Computation and Communication Technology, The Department of Quantum Science and Technology, Research School of Physics and Engineering, The Australian National University, Canberra, ACT, Australia. [2]A*STAR Quantum Innovation Centre (Q.InC), Agency for Science, Technology and Research (A*STAR), Singapore, Republic of Singapore. [3]Data61, Commonwealth Scientific and Industrial Research Organisation, Sydney, NSW, Australia. [4]Quintessence Labs, Canberra, ACT, Australia. [5]These authors contributed equally: Özlem Erkılıç, Biveen Shajilal.
✉e-mail: ozlemerkilic1995@gmail.com; Jie.Zhao@anu.edu.au

overestimation of Eve's information with non-Gaussian filters, leading to an underestimation of the key rate.

In this work, we present a CV-QKD protocol using Gaussian modulations and homodyne or heterodyne detection followed by post-selection. The protocol introduces a paradigm shift by eliminating the need to simulate physical processes for filtering. It combines post-selection at both Alice's and Bob's stations: Alice's Gaussian filter optimises modulation variance to achieve key rates near the optimal GG02 performance, while Bob's non-Gaussian filter emulates a higher-performing channel, surpassing optimal GG02 key rates. To avoid overestimating Eve's information, we developed a security analysis that tightly bounds Eve's information after Bob's filter. The protocol dynamically optimises key rates for rapidly changing channels, such as satellite-to-ground links, where rapid channel changes render any parameter estimation unreliable. Moreover, it can extract keys even in regions where unfiltered channel parameters would not allow secure QKD under the GG02 protocol.

Results

Protocol overview

The experimental setup is shown in Fig. 1(a), where Alice generates two variables, x_a and p_a, from a zero-mean Gaussian distribution with variance V_{mod} in units of vacuum noise using two independent function generators. In our implementation, Alice's Gaussian-modulated variables are encoded onto the sidebands of a 1064 nm continuous-wave laser using amplitude and phase electro-optic modulators driven at 3-5 MHz. This generates a thermal state with quadrature variance $V_{mod} + 1$, as required by the protocol. Alice retains these variables to apply a Gaussian filter to both x_a and p_a after the states have been sent to Bob and measured. The encoded state is sent through a quantum channel with transmittance T and thermal noise W, simulated by a half-wave plate and polarising beamsplitter. Bob performs homodyne detection, randomly measuring the x or p quadrature. The homodyne signal is filtered by a $3-5$ MHz bandpass filter and then fed to the oscilloscope with a sampling rate of 25 MSamples/s, collecting 10 million samples. Both homodyne data and Alice's data were digitally filtered with a $3-3.5$ MHz bandpass filter.

While the experimental setup follows the well-known GG02 protocol[6,7], which utilises Gaussian modulated coherent states and homodyne detection, our protocol diverges at the software level. This software-level protocol can be applied to any system with Gaussian modulated states and coherent detection. After the data acquisition, Alice's post-selection is applied on the samples x_a and p_a where Alice's Gaussian post-selection filter is defined by the following expression

$$F_A(x_a) = e^{-g_x^2 x_a^2}, \tag{1}$$

where x_a is the randomly generated variable and $g_x \geq 0$ represents the filter gain. Each symbol, x_a, is either kept or discarded based on the probability $F_A(x_a)$ (See the Methods section for details on how the filter is applied). The same function applies to p_a, replacing g_x with g_p. This post-selection on x_a and p_a imitates attenuating the modulation variance, as shown in Fig. 1(b). When $g_x = 0$, no filtering is applied, but as g_x increases significantly (e.g., $g_x = 10^5$), the modulation variance approaches zero, effectively turning the state into vacuum. In the GG02 protocol, there is an optimal modulation variance for each distance and noise combination to achieve the best key rates. While Alice's post-selection does not alter the channel parameters, it reduces the modulation variance to match the optimal GG02. Unlike GG02, which requires modulation variance optimisation, Alice's approach optimises both the variance and key rates without needing prior channel

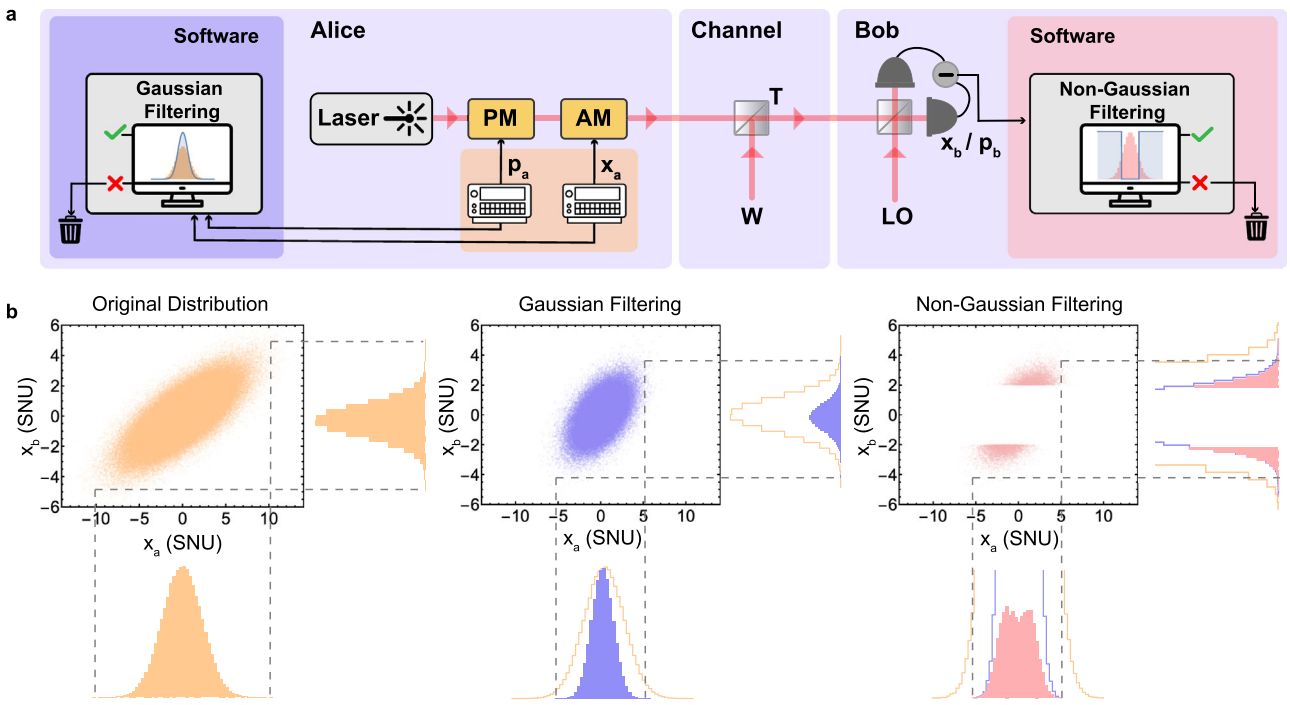

Fig. 1 | Experimental schematic and illustrative diagram of the filtering process. **a** Alice encodes coherent states $|(x_a + ip_a)/2\rangle$ from a Gausssian distribution with zero mean and variance, V_{mod}, using white noise generated by function generators (orange box). She samples x_a and p_a simultaneously, then sends the encoded states through a quantum channel with transmittivity T and thermal noise W. Bob performs homodyne detection to measure x_b and p_b, randomly switching between these two quadratures. After data acquisition and once the states have been sent to Bob and measured, Alice applies a Gaussian filter to the data kept on her computer (purple box), followed by Bob applying a non-Gaussian filter to his measurement outcomes (pink box). **b** Left: The correlation between Alice's variables x_a and Bob's measurement outcomes x_b before any post-selection. Middle: The correlation after Alice's Gaussian post-selection superimposed by the original distribution (orange), which reduces the variance of the Gaussian-modulated variables, effectively creating a thermal state with this reduced variance. Right: The correlations after Bob's non-Gaussian post-selection, resulting in highly non-Gaussian distributions for x_a and x_b. PM/AM Electro-optic phase/amplitude modulators and LO Local oscillator.

characterisation. The optimisation also inherently depends on the reconciliation efficiency, β, which quantifies how efficiently Alice and Bob can extract shared bits from their correlated data during classical post-processing (see Eq. (18)). Lower values of β reduce the mutual information between Alice and Bob, shifting the modulation variance that maximises the final key rate. Therefore, when comparing key rates or optimising filters, the effect of β must be taken into account.

The key rates can be further optimised by using a non-Gaussian post-selection performed by Bob. Bob's post-selection filter can be expressed as

$$F_B(x_b) = \begin{cases} 0 & -c_x < x_b < c_x \\ 1 & \text{elsewhere,} \end{cases} \tag{2}$$

where x_b represents Bob's homodyne measurement outcome and c_x is the cut-off parameter of the filter which can take values from 0 to the largest measurement outcome of Bob. Bob's post-selection discards all the numbers within the cut-off, therefore, it creates a highly non-Gaussian distribution as shown in Fig. 1(b). This post-selection effectively simulates a channel with better performance than the original one used by Alice to send the quantum states.

In QKD, Eve holds the purification of Alice and Bob's joint state σ_{AB}, meaning her von Neumann entropy matches that of the state shared by Alice and Bob. Therefore, Eve's information can be bounded by the Holevo bound[37], which represents the maximum classical information extractable from a quantum channel. It is expressed as

$$I_E = S(\sigma_{AB}) - S(\sigma_{A|B}), \tag{3}$$

where $S(\sigma_{AB})$ and $S(\sigma_{A|B})$ are the von Neumann entropies of Alice and Bob's joint state and Alice's state conditioned on Bob's measurement outcome x_b, respectively. Since Bob's post-selection is non-Gaussian, using the covariance matrices σ_{AB} and $\sigma_{A|B}$ would overestimate Eve's information due to Gaussian extremality, leading to lower key rates. Instead, we directly calculate Eve's information from her density matrix, assuming that she performs a general Gaussian attack. In this attack, Eve prepares a two-mode squeezed vacuum (TMSV) state with a variance that mimics the quantum channel[38]. She replaces the channel between Alice and Bob with a beamsplitter, injecting one mode (E_1) into the beamsplitter to interact with Alice's state, while retaining the other mode (E_2)[39]. While the optimal strategy after post-selection is not known, our assumption follows from the intuition that Alice and Bob can verify (within some tolerance) that the channel remains Gaussian by computing higher-order moments from their measurement outcomes such as skewness and kurtosis, thereby restricting Eve to Gaussian attacks. Eve's information is then calculated using the Holevo bound as follows

$$I_E = S(\rho_{E_1E_2}) - S(\rho_{E_1E_2|B}(x_b)), \tag{4}$$

where $S(\rho_{E_1E_2})$ represents the von Neumann entropy of Eve's average state, and $S(\rho_{E_1E_2|B})$ gives the von Neumann entropy of Eve's conditional state given Bob measures an outcome x_b. This equation saturates Eq. (3) when Bob performs no post-selection, and everything remains Gaussian. In that case, Eve's average state is the sum of all Gaussian conditional states measured by Bob. With non-Gaussian post-selection, the conditional states remain Gaussian, but Eve's average state becomes non-Gaussian. Since Bob can discard measurement outcomes within the filter cut-off, Eve's average state is no longer obtained by simply summing all the states, but is derived from the filtered results as follows

$$\rho_{E_1E_2} = \sum_{x_i=-n}^{n} p'_b(x_i)\rho_{E_1E_2|B}(x_i), \tag{5}$$

where n is the maximum number that Bob measures and $p'_b(x_i)$ denotes Bob's probability of getting a given outcome, x_i (For a detailed derivation of how to obtain the density matrices $\rho_{E_1E_2}$ and $\rho_{E_1E_2|B}$, refer to the Methods section). This method is particularly beneficial because it does not rely on Gaussian extremality to determine key rates. Previously, this reliance limited the performance of some protocols when non-Gaussian post-selection was used[32].

It is important to note that post-selection by both parties is not always required. Depending on the channel parameters, either Alice's post-selection or Bob's post-selection alone may be sufficient, while in some cases, both may be necessary. The advantage of our protocol lies in its ability to be augmented into existing CV-QKD setups without any hardware modifications, as it operates entirely at the software level.

Experimental results

Fig. 2 shows the experimental results for a transmission of $T = 0.26$ with thermal noise values of $W_x = 1.02$ SNU and $W_p = 1.01$ SNU for the x and p quadratures, respectively. This loss corresponds to an equivalent fibre distance of 29.1 km assuming a fibre loss of 0.2 dB per km. The key rate extracted from the raw data is initially negative, as illustrated in Fig. 2(a). This is because the modulation variance used in the experiment is not optimal for the 29.1 km distance with the given noise parameters. The experimental modulation variances for the x and p quadratures were $V_{mod_x} = 12.73$ SNU and $V_{mod_p} = 13.52$ SNU, while the optimal GG02 modulation variances required for this regime are $V_{mod_x} = 6.14$ SNU and $V_{mod_p} = 5.97$ SNU. The asymmetry in the variances is due to asymmetric noise in the state preparation stage. A portion of this preparation noise, primarily due to modulator electronics, is considered trusted in our security analysis (see the Methods). Alice applies a Gaussian filter with gains of $g_x = 0.213$ and $g_p = 0.259$ to reduce the modulation variances. These gains yield the optimal key rate, as indicated in Fig. 2(b) where the reported key rates in bits/use are normalised to the original number of transmitted states, with the filtering success probabilities included in the calculation to account for the reduction in usable states (refer to Eq. (35)). Although the key rate becomes positive after Alice's post-selection, it does not reach the optimal GG02 key rate as shown in Fig. 2(a) due to the success probability penalty of the post-selection process ($P_{A_x} = 0.68$ and $P_{A_p} = 0.60$ are the probability of success of Alice's post-selection on the x and p quadratures, respectively, giving a total probability of success of 0.41).

To further optimise the key rate, Bob applies a non-Gaussian filter with cut-off parameters of $c_x = 0$ and $c_p = 8.95$ which is shown in Fig. 2(c). Bob keeps the x quadrature unchanged as it is already optimal but discards most measurements in the p quadrature where the maximum value is $p_b = 9$. The key rate increases and saturates at 0.0038 ± 0.001 bits/use, surpassing the optimal GG02 key rate of 0.0036 bits/use. Our protocol turned regions with negative key rates, deemed insecure by the GG02 protocol, into regions with positive key rates. In these regions, we achieved key rates close to the optimal GG02 rates that are only achievable using optimal modulation which requires accurate channel estimations.

Next, we investigate distinct regimes where the system benefits from varying post-selection strategies. Fig. 3(a) and (b) show that at 6 km and 15.1 km, the key rates with Alice's Gaussian filter match those without post-selection, as the system parameters were already optimal. In this protocol, Alice's Gaussian filter attenuates the quantum signal by reducing the modulation variance, which is useful at long distances where photon losses require smaller optimal variances for the GG02 protocol. For shorter distances, where higher modulation variances are preferred, an inverted Gaussian filter can be used to increase the effective variance and optimise key rates. In contrast to the 6 km and 15.1 km regimes, Alice and Bob's post-selection improves the key rate when experimental parameters are sub-optimal. For example, without post-selection, the chosen parameters yield no positive key rate (solid line, Fig. 3(c)), but Alice's post-selection makes the key rate positive, surpassing the optimal GG02 rate when Bob also applies post-selection. Similarly, at 39.1 km (transmission of $T = 0.17$), Alice's post-selection increased the key rate by 1.7 times (Fig. 3(d)), but Bob's post-selection did not lead to further improvement, as it is more effective in extreme loss regimes where the GG02 protocol approaches negative key rates.

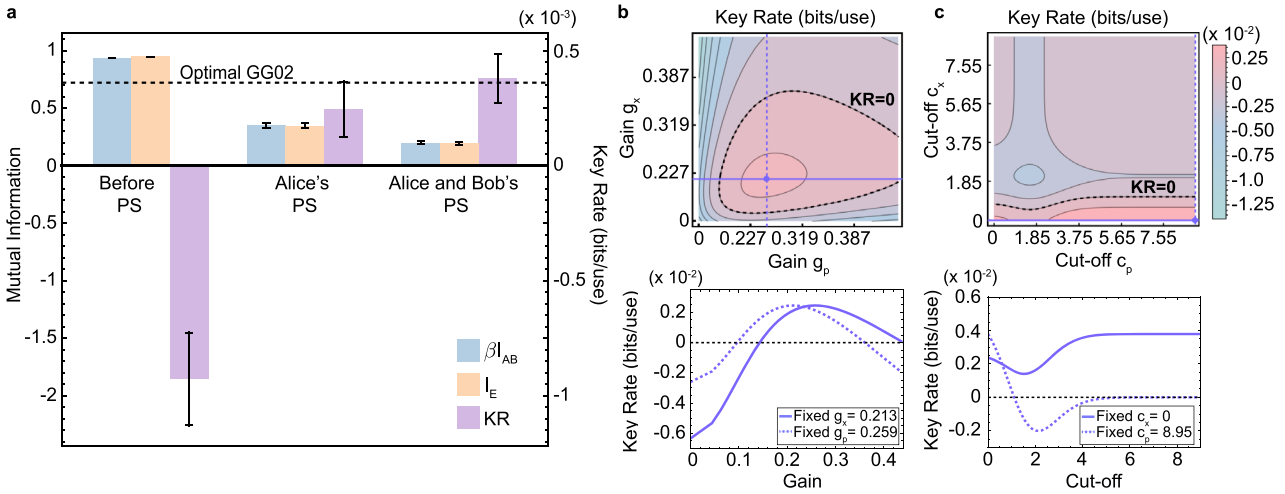

Fig. 2 | Experimental results of the protocol at a fixed channel. The channel has a transmission of $T = 0.26$, equivalent to a fibre distance of 29.1 km (assuming 0.2 dB loss per km), with a thermal noise of $W_x = 1.02 \pm 0.001$ and $W_p = 1.01 \pm 0.001$ in shot noise units (SNU) in x and p quadratures, respectively. **a** From left to right, we give the mutual information between Alice and Bob (blue boxes), Eve's information (orange boxes) and the key rates of the protocol (purple boxes) before any post-selection, after Alice's post-selection and after Alice and Bob's post-selection combined, respectively. The key rate is initially negative, indicating that Eve's information exceeds the mutual information of Alice and Bob, making it a non-secure region. After Alice's post-selection, the key rate becomes positive but remains below the optimal GG02 rate for that distance. The key rate is further optimised by applying a post-selection on Bob's side where the key rate achieves the optimal GG02 line. **b** The top panel shows the contour plot of the key rates after Alice's post-selection along the x and p quadratures, with gains ranging from 0 to 0.436. The bottom panel illustrates the key rate slices at optimal performance after Alice's post-selection with fixed gains g_x and g_p. The solid line represents fixed g_x while varying g_p, and the dashed line represents fixed g_p while varying g_x. **c** Top panel demonstrates the contour plot of the key-rates after Bob's post-selection with the cut-off parameters ranging from 0 to 8.95, while the bottom panel shows the key rates after Bob's post-selection with fixed optimal cut-offs in the x (solid line) and p (dashed line) quadratures. The solid line varies the cut-off in the p quadrature while keeping the x cut-off fixed, and the dashed line varies the cut-off in the x quadrature while keeping the p cut-off fixed. KR Key rate, I_{AB} Mutual information between Alice and Bob, I_E Eve's information and β Reconciliation efficiency. The reconciliation efficiency is set to 92% throughout the experiment. The error bars indicate the statistical uncertainties in the data. For details on how they are calculated, refer to the Methods section.

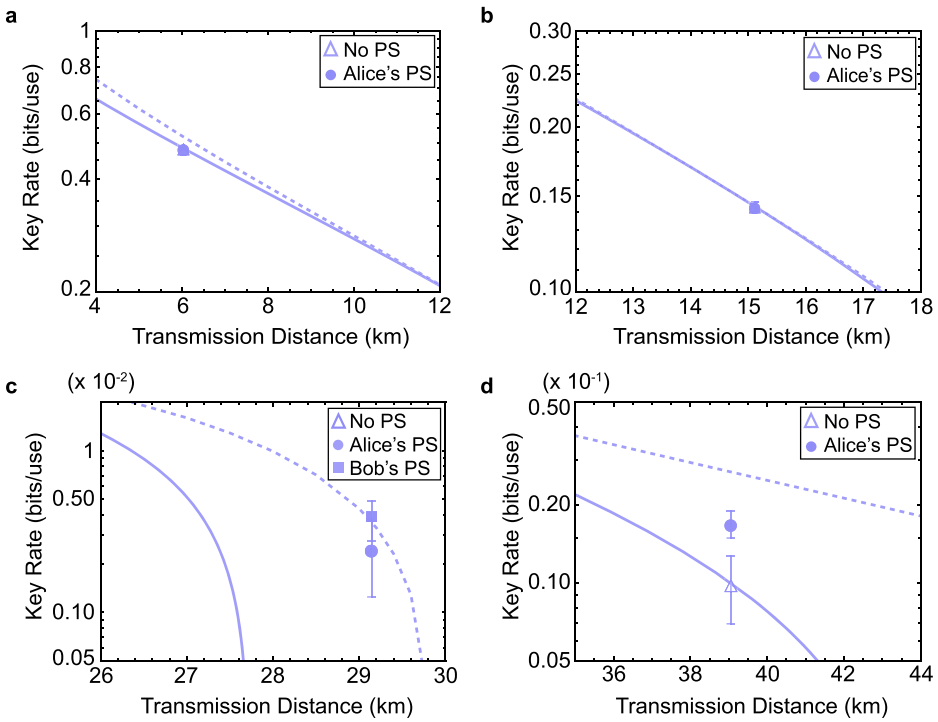

Fig. 3 | Experimental key rates for various channel parameters. Solid lines represent theoretical key rates of the GG02 protocol with fixed modulation variance, while dashed lines show theoretical key rates with optimal variances. Triangle markers indicate raw key rates before post-selection, circles show key rates after Alice's post-selection, and the square marker represents results after Bob's post-selection. **a**, **b** show the experimental results at $d = 6$ km ($T = 0.76$) and $d = 15.1$ km ($T = 0.50$), respectively. For $d = 6$ km, thermal noise is $W_x = 1.02 \pm 0.004$ SNU and $W_p = 1.04 \pm 0.004$ SNU; for $d = 15.1$ km, $W_x = 1.02 \pm 0.002$ SNU and $W_p = 1.03 \pm 0.002$ SNU. Key rates before and after Alice's post-selection overlap, indicating optimal operations. **c** Key rates at $d = 29.1$ km ($T = 0.26$) with thermal noise $W_x = 1.02 \pm 0.001$ SNU and $W_p = 1.01 \pm 0.001$ SNU. The post-selections enhance the key rate which is otherwise negative; as a result, the data without post-selection (triangular marker) does not appear on the logarithmic scale. **d** Key rates at $d = 39.1$ km ($T = 0.17$) with thermal noise $W_x = 1.00 \pm 0.001$ SNU and $W_p = 1.00 \pm 0.001$ SNU, where only Alice's post-selection was applied, as Bob's post-selection did not lead to any further improvements in this region. The error bars represent statistical uncertainties in the measured data (see Methods for details).

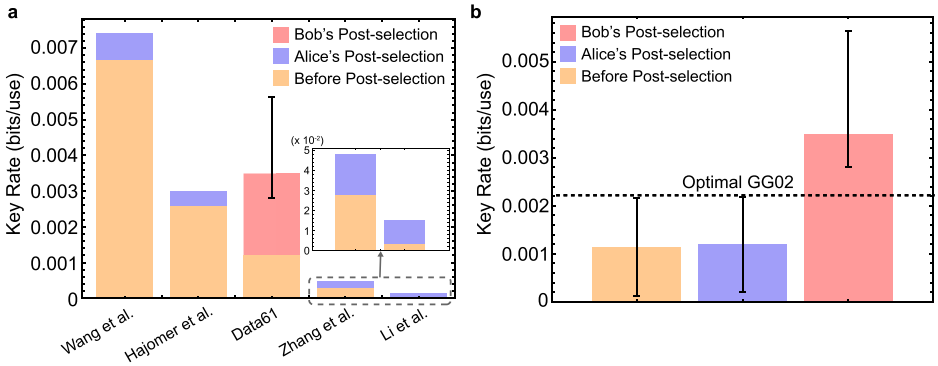

Fig. 4 | Key rates of the existing experiments after applying our protocol. Results are based on the original experimental parameters listed in Table 1. **a** Key rates from various experiments[13,14,16,40] and the experimental data from Data61 using the CV-QKD setup from Quintessence Labs. Orange boxes represent the key rates before post-selection, purple boxes denote the results after Alice's post-selection, and the pink box shows the key rate after Bob's post-selection. **b** Key rates of Data61 at each step, with a reconciliation efficiency of $\beta = 92.5\%$ (Refer to Supplementary Note II for the derivation of the key rate with heterodyne detection). The error bars indicate statistical uncertainties: for data before post-selection and after Alice's post-selection, they are derived from experimental fluctuations, while for Bob's post-selection, they correspond to worst and best-case estimates.

Table 1 | Experimental parameters of the state-of-the-art CV-QKD demonstrations

Experiment	Detection	V_{mod} (SNU)	Distance (km)	Loss (dB)	ξ_{ch} (SNU)	ξ_d (SNU)	ξ_t (SNU)	η (%)	β (%)	Key Rate Improvement (%)	Distance Improvement(km)
Wang et al.[13]	Homodyne	15	50	10	0.07	0.05	-	60.141	96.7	11.3	42
Hajomer et al.[16]	Heterodyne	8.41	100	15.52	0.212×10^{-3}	0.06272	-	68	92.5	16.4	19
Data61—CSIRO	Heterodyne	4.06 4.21	41.71	7.92	0.0437 0.0654	0.4401 0.4459	0.0867 0.0933	20.6	92.5	206.2	1
Zhang et al.[14]	Homodyne	14.23	140.52	23.46	0.0219	0.2717	-	61.34	96	74.5	42
Li et al.[40]	Heterodyne	10	100	18.96	0.0692	0.18	-	42	96.7	401.5	23

For the Data61-CSIRO experiment, experimental imperfections lead to asymmetry between the x and p quadratures: the first row shows the values for x, and the second row shows the values for p. For the other demonstrations, only one row is presented since the quadratures are symmetric. V_{mod} Modulation variance in shot noise units (SNU), ξ_{ch} Channel noise, ξ_d Dark noise, ξ_t Trusted noise attributed to state preparation, η Detection efficiency, β Reconciliation efficiency. Key rate improvements are calculated at the experimental distances (Fig. 4). Distance improvements are estimated by extrapolating performance beyond the experimental range (Fig. 5). As such, Figs. 4, 5 are evaluated under different conditions.

Integration with state-of-the-art demonstrations

Furthermore, we applied our protocol to state-of-the-art CV-QKD experimental demonstrations and showed improved performance (see Fig. 4(a)). Our protocol increased the key rates of the experimental results of Wang et al.[13] and Hajomer et al.[16], while doubling the key rate of Zhang et al.[14] and achieving a fivefold improvement for Li et al.[40] using Alice's post-selection where the percentage improvements are shown in Table 1. We projected their experimental demonstrations to larger distances by simulating their protocols using the parameters listed in Table 1, assuming these parameters remain constant across all distances. Under these conditions, our protocol extended the effective transmission distance by 42 km for Wang et al.[13] and Zhang et al.[14], while also enhancing the transmission distance for Hajomer et al.[16] and Li et al.[40] by 19 km and 23 km, respectively as shown in Fig. 5.

Application to a commercial CV-QKD system

Our protocol was also implemented on the Quintessence Labs qOptica system at Data61, CSIRO Sydney, for a fibre distance of 41.71 km, using heterodyne detection with a modulation variance of approximately 4. Since this variance is close to the optimal value, Alice's post-selection offered little improvement. However, Bob's post-selection tripled the original key rate, surpassing the optimal GG02 rate by emulating a better performing channel as shown in Fig. 4(b). This improvement can be explained by considering an entanglement-based experiment where Alice creates a two-mode squeezed vacuum state, sending one arm to Bob and measuring the other. With a Gaussian filter, the best achievable key rate is the optimal GG02 rate, as Gaussian operations cannot distill entanglement[41]. Non-Gaussian operations, however, enable entanglement distillation, allowing Bob to outperform the GG02 key rate. This was also observed in Hosseinidehaj et al.[27] when the MB-NLA filter was made slightly non-Gaussian. However, since their approach emulates a physical filter, it cannot be made highly non-Gaussian without deviating from its intended function as a noiseless amplifier. In contrast, our protocol offers the flexibility to choose any filter cut-off.

Performance in satellite-to-ground CV-QKD links

Our protocol's applicability extends beyond terrestrial setups and can be applied to improve satellite-to-ground communication links for CV-QKD. Fig. 6(a) and (b) show how our protocol expands the communication window between the ground station and satellite under varying weather conditions, using the satellite-to-ground link model of Sayat et al.[42]. Assuming the satellite is in Low Earth orbit at 500 km altitude, the orange lines represent the conventional GG02 protocol with a modulation variance of $V_{mod} = 8$ SNU, while the purple lines show the results of our protocol with Alice's post-selection. In good weather (Fig. 6(a)), the GG02 protocol supports communication between the optical ground station (OGS) and satellite at angles from 20° to 160°. In contrast, Alice's post-selection enables communication at all angles, boosting key rates by up to 40 times at the extremes where GG02 achieves the lowest key rates. In poor weather (Fig. 6(b)), our protocol further expands the communication window by 76°, achieving a 400-fold improvement in key rates under extreme conditions. In addition to higher key rates, our protocol offers a longer active communication window, defined as the time during which a positive key rate above 10^{-4} bits/use is maintained. Traditional CV-QKD protocols using LEO satellites allow for windows of 1.28 h in favourable weather and 38 minutes in poor conditions. In contrast, our protocol extends this window to 3 hours in any weather, maintaining a minimum key rate of 10^{-4} bits/use. If a higher key rate threshold were used, the GG02 protocol would have even smaller

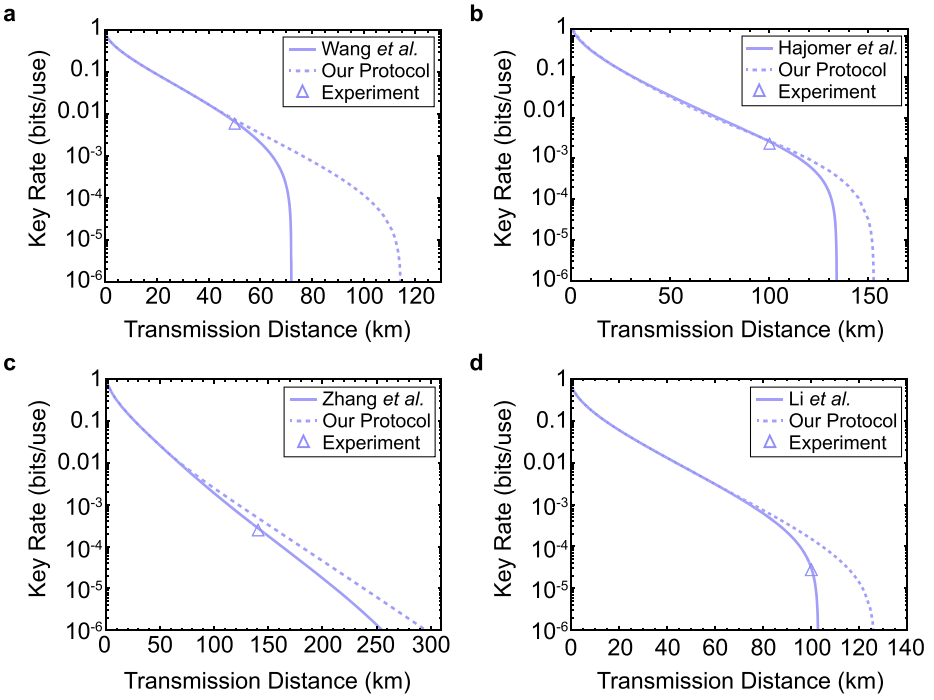

Fig. 5 | Simulated key rates for state-of-the-art experiments extended beyond their original demonstration distances. Solid lines indicate the projected key rates using the experimental parameters, while dashed lines show the key rates when applying our protocol with these same parameters. Triangle markers denote the original experimental results from the cited works. Simulation results are presented for Wang et al.[13] (42 km improvement), Hajomer et al.[16] (19 km improvement), Zhang et al.[14] (42 km improvement), and Li et al.[40] (23 km improvement) in (**a**–**d**), respectively. Refer to Table 1 for the experimental parameters.

windows, while our protocol would still provide significantly longer active times (For more details, refer Supplementary Note IV). This showcases that our protocol can be particularly useful in free-space channels, such as satellite-to-ground communication links, where rapid changes in the quantum channel are common.

Discussion

QKD plays a crucial role in securing communications against potential eavesdropping in the quantum era. However, challenges such as limited key rates and vulnerability to environmental factors have impeded its practical deployment.

Addressing these issues, we introduced a protocol which enhances CV-QKD by combining post-selection at both Alice and Bob's stations. This protocol utilises a Gaussian filter at Alice's end and a non-Gaussian box-like filter at Bob's end to optimise key rates even under non-ideal conditions. Our approach dynamically adjusts to varying quantum channel conditions, making it particularly effective in free-space channels such as ground-to-satellite communication links.

Experimental results demonstrated significant improvements in key rates when applying our protocol to state-of-the-art CV-QKD systems. We observed up to a five-fold increase in key rates using Alice's post-selection and tripling of the original key rate with Bob's post-selection on different systems. Additionally, our protocol extended the communication window between ground stations and satellites, showing robustness under both good and adverse weather conditions. Specifically, under poor weather conditions, our protocol expanded the communication window to all elevation angles and achieved a 400-fold improvement in key rates under extreme conditions.

The ability of our protocol to achieve secure key distribution even in rapidly changing quantum channels highlights its potential for practical implementation in challenging environments. By leveraging software-level modifications without the need for hardware changes, our approach provides a flexible and efficient solution for advancing CV-QKD technology.

Our current work focuses on asymptotic key rates, with potential extensions to account for finite-size effects and composable security. In practical applications, data sizes are finite, and smaller block sizes can adversely affect key rates. Nevertheless, our protocol can be effective in scenarios where block sizes degrade key rate quality; however, a full composable security analysis remains an important direction for future work. As Bob's post-selection involves a non-Gaussian filter, the security analysis cannot follow the Gaussian extremality. Instead, Eve's information is bounded by representing her state as a density matrix with some finite truncation in the Fock-number basis. This is computationally demanding and can be challenging if Alice's variance is too high. A recent paper by Denys et al.[43] provides an analytical lower bound on the asymptotic secret key rate for CV-QKD with arbitrary modulation schemes. Extending this to include Bob's post-selection could bypass the need for density matrices, making the security analysis less time-consuming. In this work, we restrict Eve to Gaussian attacks. However, the optimal eavesdropping strategy in the presence of non-Gaussian post-selection remains an open question. Future studies should consider whether Eve could perform a non-Gaussian attack to compromise the key.

Our protocol could potentially be applied to CV-QKD protocols with discrete modulation (DM CV-QKD)[44–46], which utilise a constellation of modulated coherent states. In particular, Bob's non-Gaussian post-selection could enable dynamic switching between different types of DM CV-QKD protocols by selectively combining states from the constellation of modulated coherent states. While Bob's post-selection filter is similar in shape to those used in the DM CV-QKD protocol proposed by Kanitschar and Pacher[47], which demonstrated switching between formats like 8PSK and QPSK, our approach differs in that Alice sends Gaussian-modulated states. This allows Bob to emulate a wider range of modulation formats (e.g., BPSK, QPSK, or multiring) through flexible filter design, enabling more general DM or GM CV-QKD switching.

Methods

Alice's Gaussian post-selection

The random variables generated by Alice's function generator follow a Gaussian distribution as described below

$$p_a(x_a) = \frac{1}{\sqrt{2\pi V_{mod_x}}} \exp\left[\frac{-x_a^2}{2V_{mod_x}}\right], \tag{6}$$

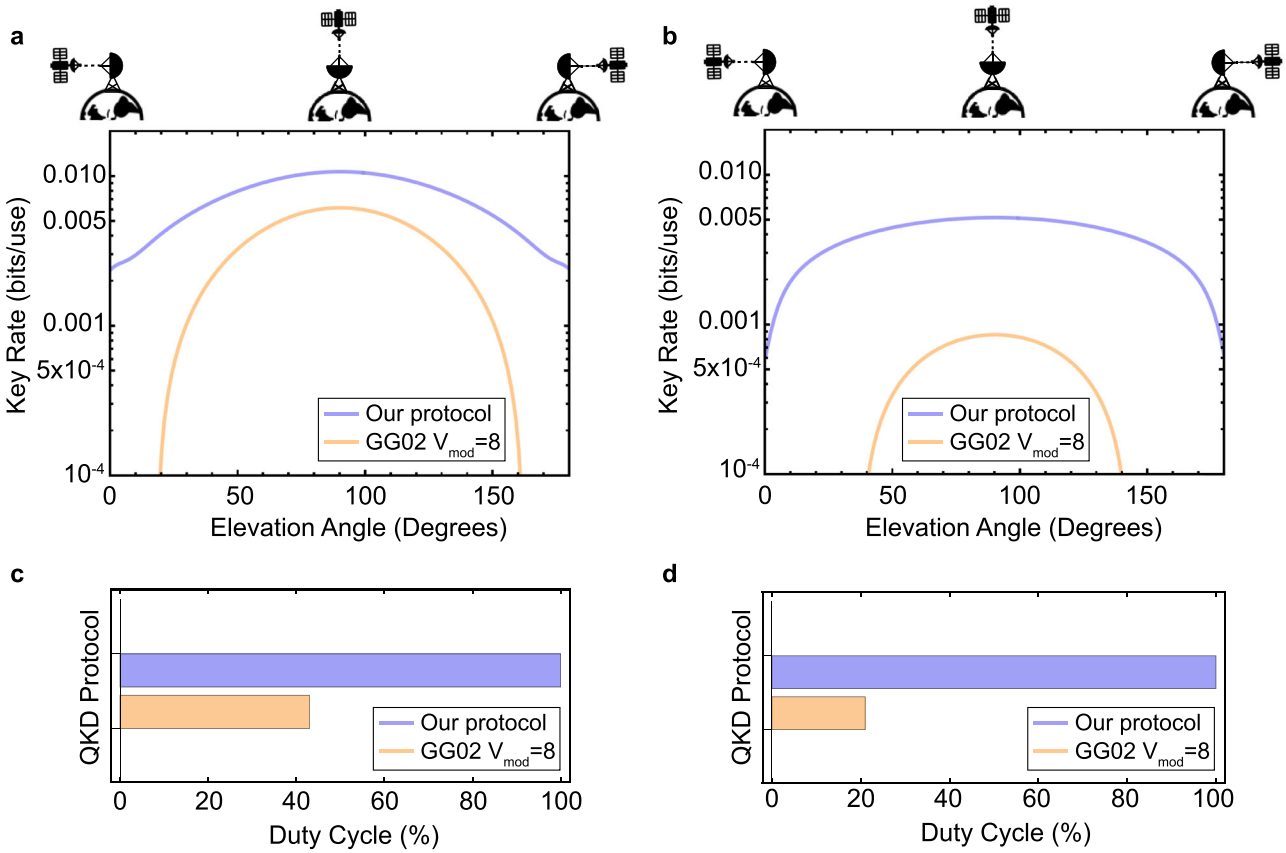

Fig. 6 | Key rates for satellite-to-ground communication as a function of elevation angle. Results are obtained using our protocol applied to the GG02 scheme with homodyne detection, assuming the satellite orbits at an altitude of 500 km in low-Earth orbit and the optical ground station is at an elevation of 0 km. We used the model and parameters from Sayat et al.[42] with a reconciliation efficiency of $\beta = 90\%$ (Refer to the Supplementary Note IV for the parameters). **a** The orange lines represent key rates with a fixed modulation variance of $V_{mod} = 8$ SNU, while the purple lines show key rates using our protocol with Alice's post-selection only. This simulation assumes good weather conditions with a visibility of $V = 200$ km and low turbulence corresponding to $C_n^2 = 10^{-16}$ m$^{-2/3}$. At each elevation angle, the post-selection gain was optimised to achieve the best key rates. **b** Key rates under bad weather conditions with a visibility of $V = 20$ km and high turbulence where $C_n^2 = 10^{-13}$ m$^{-2/3}$. **c** The duty cycle of our protocol and the GG02 protocol in good weather conditions using a key rate threshold of 10^{-4} from (**a**). **d** The duty cycle of our protocol and the GG02 protocol in bad weather conditions using a key rate threshold of 10^{-4} from (**b**).

where V_{mod_x} represents the modulation variance of Alice along the x quadrature with random variables x_a. The modulation variance of the x and p quadratures are not symmetric due to the experimental imperfections. However, as Bob performs a homodyne measurement, Alice's Gaussian distribution of the x and p quadrature variables can be expressed individually. In the following, we explicitly present the analysis for the x quadrature, which can be similarly applied to the p quadrature. When Alice applies the filter shown in Eq. (1), the probability of success is given by

$$P_{A_x} = \int_{-\infty}^{\infty} F_A(x_a) p_a(x_a)\, dx_a = \frac{1}{\sqrt{2g_x^2 V_{mod_x} + 1}}, \tag{7}$$

where g_x is the gain of the Gaussian filter for the x quadrature. Experimentally, Alice's filter, as described in Eq. (1), is implemented by generating a random number uniformly distributed between 0 and 1. The filter then retains the variables whose corresponding filter function values are greater than or equal to this random number. The probability of success is determined by the ratio of samples kept after filtering to the total number of samples. For our experiment, the gains were optimised to maximise the key rates. For a distance of 29.1 km, we used $g_x = 0.213$ and $g_p = 0.259$, while for a distance of 39.1 km, the gains were $g_x = 0.178$ and $g_p = 0.213$.

After Alice's post-selection, the modulation variance of the effective thermal state is reduced. The equivalent modulation variance is expressed as follows

$$\tilde{V}_{mod_x} = \int_{-\infty}^{\infty} \frac{x_a^2 F_A(x_a) p_a(x_a)}{P_{A_x}}\, dx_a = \frac{V_{mod_x}}{2g_x^2 V_{mod_x} + 1}. \tag{8}$$

Alice's post-selection cannot modify the channel parameters. However, Bob's effective variance also reduces, as he must disregard the data that Alice discards. Therefore, Bob's variance, using Alice's new variance $V_x = \tilde{V}_{mod_x} + 1$, can be expressed as

$$V_{b_x} = T(V_x + \xi_x) + (1 - T)W_x, \tag{9}$$

where ξ_x is trusted excess noise coming from the state preparation, T is the channel transmittance that is introduced experimentally using a half-wave plate followed by a PBS. This loss is equivalent to a distance of $d = -\log_{10} T/0.02$ assuming a loss of 0.2 dB per km. W_x denotes the thermal noise from the quantum channel, attributed to Eve. Similarly, the covariance between Alice and Bob after Alice's post-selection scales to $T\tilde{V}_{mod_x}$ in the prepare-and-measure (PM) scheme. QKD protocols can be expressed in either entanglement-based (EB) or prepare-and-measure schemes. While mathematically equivalent[38,48], the EB representation is more convenient for security analysis. Therefore, the new covariance

between Alice and Bob in the equivalent EB scheme can be expressed as

$$C_x = \sqrt{T(V_x^2 - 1)}. \tag{10}$$

The EB-based covariance matrix of the quantum state between Alice and Bob can be written as ref. 49 (Refer to Supplementary Note I for the derivation of the PM covariance matrix and Supplementary Note III for derivation of the covariance matrices starting from the EB model)

$$\sigma_{AB}^{\mathrm{EB}} = \begin{pmatrix} V_x & 0 & C_x & 0 \\ 0 & V_p & 0 & -C_p \\ C_x & 0 & V_{b_x} & 0 \\ 0 & -C_p & 0 & V_{b_p} \end{pmatrix}. \tag{11}$$

Note that C_p has the same form as C_x, but with a different variance, V_p. Similarly, Bob's variance V_{b_p} follows the same formula as Eq. (9), with the variance V_p, trusted noise ξ_p, and thermal noise W_p.

The mutual information between Alice and Bob can be calculated using the EB-based covariance matrix shown in Eq. (11). In our protocol, we employ reverse reconciliation, meaning the direction of classical communication is from Bob to Alice[17]. While the direction of reconciliation does not affect the mutual information between Alice and Bob, it influences how much information Eve can access. CV-QKD protocols with reverse reconciliation, unlike direct reconciliation, allow key distribution beyond the 3 dB loss limit[7,50]. The mutual information between Alice and Bob is calculated from

$$I_{AB_x} = \frac{1}{2}\log_2 \frac{V_{A_x}}{V_{A_x|B_x}}, \tag{12}$$

where V_{A_x} represents Alice's variance of the classical data in the EB scheme where she performs a heterodyne measurement on the mode she keeps. This variance is given by $V_{A_x} = (V_x + 1)/2$ and $V_{A_x|B_x} = V_{A_x} - C_x^2/(2V_{b_x})$ denotes Alice's variance conditioned on Bob's measurement outcomes.

Eve's average covariance matrix also scales after Alice's post-selection, as Alice and Bob keep fewer states than originally. As previously mentioned, Eve injects a TMSV state with modes E_1 and E_2. Mode E_1 interacts with incoming signal from Alice, while mode E_2 is retained by Eve. After Alice's post-selection, the variance of E_1 is updated as follows, while the variance of E_2 remains unchanged

$$V_{E_{1_x}} = TW_x + (1 - T)(V_x + \xi_x). \tag{13}$$

Note that the variance of the p quadrature for this mode follows the same formula, but with Alice's variance V_p, trusted excess noise ξ_p and a thermal noise of W_p. In practice, there exists a slight discrepancy between W_x and W_p due to the asymmetry in the experimental measurements. This implies that Eve introduces slightly different noise in the x and p quadratures, expressed as W_x and W_p, respectively. To achieve this, Eve must create two separate TMSV states[38] and combine them at a 50/50 beamsplitter before interacting with Alice's signal. Based on these, Eve's average covariance matrix can be expressed as

$$\sigma_{E_1E_2} = \begin{pmatrix} V_{E_{1_x}} & 0 & C_{E_x} & 0 \\ 0 & V_{E_{1_p}} & 0 & C_{E_p} \\ C_{E_x} & 0 & W_x & 0 \\ 0 & C_{E_p} & 0 & W_p \end{pmatrix}, \tag{14}$$

where $C_{E_x} = 0.5(-\mathrm{e}^{2r_1} + \mathrm{e}^{2r_2})$ and $C_{E_p} = 0.5(-\mathrm{e}^{-2r_1} + \mathrm{e}^{-2r_2})$ where r_1 and r_2 are the squeezing parameters of the TMSV states of Eve which are given by $r_1 = 0.5\ln(W_x + \sqrt{W_x^2 - W_x/W_p})$ and $r_2 = 0.5\ln(W_x/W_p) - 0.5\ln(W_x + \sqrt{W_x^2 - W_x/W_p})$. Eve's information is calculated using the Holevo bound[37], which is used to upper bound the information leaked to Eve as shown below

$$I_{E_x} = S(\sigma_{E_1E_2}) - S(\sigma_{E_1E_2|B_x}), \tag{15}$$

where $S(\sigma_{E_1E_2})$ and $S(\sigma_{E_1E_2|B_x})$ represent the von Neumann entropy of Eve's average state and Eve's state conditioned on Bob's measurement outcome x_b, respectively. Eve's conditional covariance matrix can be found from[49]

$$\sigma_{E_1E_2|B_x} = \sigma_{E_1E_2} - \frac{1}{V_{b_x}}\sigma_c \Pi_x \sigma_c^T, \tag{16}$$

where $\Pi_x = \mathrm{diag}(1, 0)$ if Bob measures x quadrature and $\Pi_p = \mathrm{diag}(0, 1)$ for p quadrature. σ_c is the covariance terms between Eve and Bob, given as

$$\sigma_c = \begin{pmatrix} C_{E_1B_x} & 0 \\ 0 & C_{E_1B_p} \\ C_{E_2B_x} & 0 \\ 0 & C_{E_2B_p} \end{pmatrix}, \tag{17}$$

where $C_{E_1B_x} = \sqrt{T(1-T)}\big(W_x - (V_x + \xi_x)\big)$, $C_{E_1B_p} = \sqrt{T(1-T)}\Big(W_p - (V_p + \xi_p)\Big)$, $C_{E_2B_x} = \sqrt{(1-T)}C_{E_x}$ and $C_{E_2B_p} = \sqrt{(1-T)}C_{E_p}$. Refer to Laudenbach et al.[49] for the full derivation of σ_c.

The secret key rate is calculated using Eqs. (12) and (15):

$$K = \beta I_{AB} - I_E, \tag{18}$$

where β represents the reconciliation efficiency, with $0 \le \beta < 1$. In our experiment, we assume $\beta = 92\%$ when calculating the key rates.

As Bob performs homodyne measurements on the x quadrature half of the time and on the p quadrature the other half, and since the variances and noise parameters differ between these quadratures due to experimental imperfections, Alice and Bob's mutual information, as well as Eve's information, must be averaged over both quadratures. This leads to $I_{AB} = 0.5P_{A_x} \times I_{AB_x} + 0.5P_{A_p} \times I_{AB_p}$ and $I_E = 0.5P_{A_x} \times I_{E_x} + 0.5P_{A_p} \times I_{E_p}$.

Bob's non-Gaussian post-selection

Bob's initial distribution before his post-selection can be expressed as

$$p_b(x_b) = \frac{1}{\sqrt{2\pi V_{b_x}}} \exp\left[\frac{-x_b^2}{2V_{b_x}}\right], \tag{19}$$

where x_b corresponds to Bob's measurement outcome. Following Alice's post-selection, Bob applies the filter shown in Eq. (2), which gives a probability of success of

$$P_{B_x} = \int_{-\infty}^{\infty} F_B(x_b) p_b(x_b)\, dx_b = 1 - \mathrm{erf}\left[\frac{c_x}{\sqrt{2V_{b_x}}}\right], \tag{20}$$

where c_x is the cut-off parameter of the filter function.

Following Bob's post-selection, his output probability distribution becomes

$$\tilde{p}_b(x_b) = \begin{cases} 0 & -c_x < x_b < c_x \\ \frac{p_b(x_b)}{P_{B_x}} & \text{elsewhere.} \end{cases} \tag{21}$$

As Bob's filter is non-Gaussian, we avoid using the Gaussian extremality as this approach underestimates the secret key rate due to overestimating Eve's information. Therefore, we propose calculating the absolute bound on Eve's information directly from her density matrix.

To express Eve's conditional state shown in Eq. (16) as a density matrix, we first use Williamson's decomposition, which provides a symplectic matrix s and a diagonal matrix ω, following $s\sigma_{E_1E_2|B_x}s^T = \omega$[51]. We then decompose the symplectic matrix, s, further using the Bloch-Messiah decomposition[52], representing s as a series of beamsplitters, squeezers, and phase rotations: $s = s_u s_l s_v$ in the covariance matrix notation and $S = S_U S_I S_V$ in the density matrix notation. In our case, both s_u and s_v are expressed through phase rotations and beamsplitters: $S_U = R(\theta_1, \theta_2)B(\tau_U)R(\theta_3, \theta_4)$ and $S_V = R(\theta_5, \theta_6)B(\tau_V)R(\theta_7, \theta_8)$, where each parameter needs to be solved. The s_l component is expressed through two-mode squeezing operations, $S_I = S(r_1, r_2)$. Therefore, Eve's overall conditional density matrix is written in terms of the symplectic density matrix S and a mixed thermal state Λ

$$\rho_{E_1E_2|B_x}(x_b = 0) = S\Lambda S^\dagger, \tag{22}$$

where $\Lambda = \rho_1 \otimes \rho_2$, with ρ_1 and ρ_2 being thermal states given by $\sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}}|n\rangle\langle n|$, having mean photon numbers $\bar{n}_1$ and $\bar{n}_2$, respectively. Note that $\bar{n}_i = (\lambda_i - 1)/2$, where λ_i represents the i^{th} diagonal terms of the diagonal matrix ω. In our case, ω has two unique diagonal terms, λ_1 and λ_2, which are used to calculate the mean photon numbers $\bar{n}_1$ and $\bar{n}_2$.

To calculate Eve's information, we need to determine her average density matrix, which is the sum of her all conditional matrices over Bob's measurement outcomes weighted by the probability density for the respective outcome. Given that Bob measures an outcome x_b, Eve's conditional state is

$$\begin{aligned}\rho_{E_1E_2|B_x}(x_b) \quad = \quad & D(\alpha_1(x_b), \alpha_2(x_b))\rho_{E_1E_2|B_x}(x_b = 0) \\ & D^\dagger(\alpha_1(x_b), \alpha_2(x_b)),\end{aligned} \tag{23}$$

where $D(\alpha_1(x_b), \alpha_2(x_b))$ represents the displacement operator for Eve's modes 1 and 2 in the form of

$$\begin{aligned}D(\alpha_1(x_b), \alpha_2(x_b)) \quad = \quad & \exp(\alpha_1(x_b)a^\dagger - \alpha_1(x_b)a)\otimes \\ & \exp(\alpha_2(x_b)a^\dagger - \alpha_2(x_b)a),\end{aligned} \tag{24}$$

where α_1 and α_2 are functions of Eve's conditional means based on Bob's measurement outcomes, x_b. The matrix of Eve's conditional means is calculated from

$$\mu_{E_1E_2}(x_b, p_b) = \sigma_c \begin{pmatrix} V_{b_x} & 0 \\ 0 & V_{b_p} \end{pmatrix}^{-1} \begin{pmatrix} x_b \\ p_b \end{pmatrix}, \tag{25}$$

where $p_b = 0$ for homodyne detection when x_b is measured and $x_b = 0$ when p_b is measured. Therefore $\alpha_1(x_b) = \mu_{E_1}(x_b)/2$ and $\alpha_2(x_b) = \mu_{E_2}(x_b)/2$ where $\mu_{E_1}(x_b)$ and $\mu_{E_2}(x_b)$ are obtained from the entries of the $\mu_{E_1E_2}(x_b, 0)$ vector as follows: $\mu_{E_1}(x_b) = \mu_{E_1E_2}(x_b, 0)_1$ and $\mu_{E_2}(x_b) = \mu_{E_1E_2}(x_b, 0)_3$.

Although each conditional state has the same entropy, they contribute differently to Eve's average state due to the varying probabilities of obtaining each conditional state. Therefore, we determine Eve's average density matrix by multiplying each conditional state with their corresponding probabilities from Bob's post-selected probability distribution followed by summing them all up. Note that Bob's probability of getting a given outcome is obtained from

$$p'_b(x_i) = \int_{x_i-\Delta}^{x_i+\Delta} \tilde{p}_b(x_i)\, dx_b. \tag{26}$$

To calculate the key rates after the non-Gaussian post-selection, we discretise Eve's information to determine the conditional states for each of Bob's measurement outcomes. Therefore, Δ in Eq. (26) is the width of the discretised bins and in our results $\Delta = 0.1$. Consequently, Eve's average state can be calculated from Eq. (5). Eve's information is then calculated using the Holevo bound which is

$$I_{E_x} = S(\rho_{E_1E_2}) - S(\rho_{E_1E_2|B_x}(0)), \tag{27}$$

where $S(\rho_{E_1E_2})$ represents the von Neumann entropy for Eve's average state while $S(\rho_{E_1E_2|B_x}(0))$ gives the von Neumann entropy of Eve's conditional state which remains the same irrespective of Bob's measurement outcome x_b.

In order to find Alice and Bob's mutual information, the new bivariate Gaussian distribution between Alice and Bob following Alice's post-selection is fitted to the following function

$$\begin{aligned}f_{AB}(x_a, x_b) = & \frac{1}{2\pi\sigma_a\sigma_b\sqrt{1-\rho^2}} \\ & \exp\left[-\frac{1}{2(1-\rho^2)}\left(\frac{x_a^2}{\sigma_a^2} - \frac{2\rho x_a x_b}{\sigma_a\sigma_b} + \frac{x_b^2}{\sigma_b^2}\right)\right],\end{aligned} \tag{28}$$

where $\sigma_a = \sqrt{(V_x + 1)/2}$ and $\sigma_b = \sqrt{V_{b_x}}$ are the standard deviations of Alice and Bob, respectively, and $\rho = C_x/\sqrt{2}\sigma_a\sigma_b$ represents the correlation term between them.

Using Eq. (28), we generate a probability table between Alice and Bob for each values of x_a and x_b where $x_a = -15, -15 + \Delta, \cdots, 15$ and $x_b = -9, -9 + \Delta, \cdots, 9$. The mutual information then is calculated from

$$I_{AB_x} = H_{A_x} + H_{B_x} - H_{AB_x}, \tag{29}$$

where H_{A_x}, H_{B_x}, and H_{AB_x} represent the Shannon entropy of Alice's classical variable, Bob's classical variable, and the joint entropy of Alice's and Bob's classical variables, respectively.

After Bob's post-selection H_{AB_x} can be computed from

$$\begin{aligned}H_{AB_x} = & -\sum_{x_a=-n_a}^{n_a}\sum_{x_b=-n_b}^{-c_x-\Delta/2}\frac{f_{AB}(x_a,x_b)}{P_{B_x}} \\ & \log_2\left[\frac{f_{AB}(x_a,x_b)}{P_{B_x}}\right] - \sum_{x_a=-n_a}^{n_a}\sum_{x_b=c_x+\Delta/2}^{n_b}\frac{f_{AB}(x_a,x_b)}{P_{B_x}} \\ & \log_2\left[\frac{f_{AB}(x_a,x_b)}{P_{B_x}}\right],\end{aligned} \tag{30}$$

where c_x is the cut-off parameter of Bob's filter function in Eq. (2); where n_a and n_b represent the maximum number that Alice prepares and Bob measures, respectively.

Alice's probabilities after Bob's post-selection can be found from

$$f_A(x_a) = \sum_{x_b=-n_b}^{-c_x-\Delta/2}\frac{f_{AB}(x_a,x_b)}{P_{B_x}} + \sum_{x_b=c_x+\Delta/2}^{n_b}\frac{f_{AB}(x_a,x_b)}{P_{B_x}}, \tag{31}$$

which is used to compute H_{A_x}

$$H_{A_x} = -\sum_{x_a=-n_a}^{n_a} f_A(x_a)\log_2\left[f_A(x_a)\right]. \tag{32}$$

Similarly, Bob's probabilities from the probability table after his post-selection can be found from

$$f_B(x_b) = \sum_{x_a=-n_a}^{n_a}\frac{f_{AB}(x_a,x_b)}{P_{B_x}}, \tag{33}$$

which is used to calculate H_{B_x} as

$$H_{B_x} = -\sum_{x_b=-n_b}^{-c_x-\Delta/2} f_B(x_b)\log_2\left[f_B(x_b)\right] - \sum_{x_b=c_x+\Delta/2}^{n_b} f_B(x_b)\log_2\left[f_B(x_b)\right]. \quad (34)$$

Calculating the final key rate

Since both Alice and Bob perform post-selection, we need to consider the probabilities of success and average the key rates over the x and p quadratures. Following Bob's filtering process, the average mutual information between Alice and Bob becomes $I_{AB} = 0.5P_{B_x}P_{A_x}I_{AB_x} + 0.5P_{B_p}P_{A_p}I_{AB_p}$. Eve's information is averaged in the same manner as the mutual information. Finally, the key rate is calculated using Eq. (18) as

$$KR = 0.5P_{B_x}P_{A_x}(\beta I_{AB_x} - I_{E_x}) + 0.5P_{B_p}P_{A_p}(\beta I_{AB_p} - I_{E_p}) \quad (35)$$

Error bars

In QKD, key rate calculations typically rely on a worst-case estimation of the channel parameters derived from parameter estimation. In our approach, we fit the raw data to a bivariate Gaussian distribution with the same formula as Eq. (28) within a 95% confidence interval to obtain the values of σ_a, σ_b and ρ. In this case, σ_a and σ_b the standard deviations of Alice's modulation, $\sqrt{V_{mod_x}}$, and Bob's measurement outcomes, $\sqrt{V_{b_x}}$, respectively, while ρ denotes the correlation parameter between Alice and Bob's data.

Since our data sample is finite, the error bars in the key rates represent statistical errors, calculated by bootstrapping the data. We resample the data 100 times, with 10 million samples in each iteration, effectively simulating the experiment 100 times. The variance across these simulations provides the error bars.

Data availability

The data that supports the findings of this study are available from the corresponding author upon reasonable request.

Code availability

The codes that support the findings of this study are available from the corresponding author upon reasonable request.

Received: 2 July 2025; Accepted: 9 September 2025;
Published online: 15 October 2025

References

1. Ekert, A. & Renner, R. The ultimate physical limits of privacy. *Nature* **507**, 443–447 (2014).
2. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
3. Pirandola, S. et al. Advances in quantum cryptography. *Adv. Opt. Photonics* **12**, 1012–1236 (2020).
4. Ralph, T. C. Continuous variable quantum cryptography. *Phys. Rev. A* **61**, 010303 (1999).
5. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **61**, 022309 (2000).
6. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
7. Grosshans, F. et al. Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
8. Weedbrook, C. et al. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
9. Lance, A. M. et al. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.* **95**, 180503 (2005).
10. Lodewyck, J. et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A* **76**, 042305 (2007).
11. Madsen, L. S., Usenko, V. C., Lassen, M., Filip, R. & Andersen, U. L. Continuous variable quantum key distribution with modulated entangled states. *Nat. Commun.* **3**, 1083 (2012).
12. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P. & Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat. Photonics* **7**, 378–381 (2013).
13. Wang, C. et al. 25 mhz clock continuous-variable quantum key distribution system over 50 km fiber channel. *Sci. Rep.* **5**, 14607 (2015).
14. Zhang, Y. et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.* **125**, 010502 (2020).
15. Jain, N. et al. Practical continuous-variable quantum key distribution with composable security. *Nat. Commun.* **13**, 4740 (2022).
16. Hajomer, A. A. et al. Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator. *Sci. Adv.* **10**, eadi9474 (2024).
17. Garcia-Patron Sanchez, R. Quantum information with optical continuous variables: from Bell tests to key distribution (2007).
18. Xiang, G.-Y., Ralph, T. C., Lund, A. P., Walk, N. & Pryde, G. J. Heralded noiseless linear amplification and distillation of entanglement. *Nat. Photonics* **4**, 316–319 (2010).
19. Winnel, M. S., Hosseinidehaj, N. & Ralph, T. C. Generalized quantum scissors for noiseless linear amplification. *Phys. Rev. A* **102**, 063715 (2020).
20. Bencheikh, K., Symul, T., Jankovic, A. & Levenson, J.-A. Quantum key distribution with continuous variables. *J. Mod. Opt.* **48**, 1903–1920 (2001).
21. Huang, P., He, G., Fang, J. & Zeng, G. Performance improvement of continuous-variable quantum key distribution via photon subtraction. *Phys. Rev. A* **87**, 012317 (2013).
22. Hu, L., Al-Amri, M., Liao, Z. & Zubairy, M. Continuous-variable quantum key distribution with non-Gaussian operations. *Phys. Rev. A* **102**, 012608 (2020).
23. Ye, W. et al. Improvement of self-referenced continuous-variable quantum key distribution with quantum photon catalysis. *Opt. Express* **27**, 17186–17198 (2019).
24. Hu, J., Liao, Q., Mao, Y. & Guo, Y. Performance improvement of unidimensional continuous-variable quantum key distribution using zero-photon quantum catalysis. *Quantum Inf. Process.* **20**, 1–20 (2021).
25. Walk, N., Ralph, T. C., Symul, T. & Lam, P. K. Security of continuous-variable quantum cryptography with Gaussian postselection. *Phys. Rev. A* **87**, 020303 (2013).
26. Fiurášek, J. & Cerf, N. J. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. *Phys. Rev. A* **86**, 060302 (2012).
27. Hosseinidehaj, N., Lance, A. M., Symul, T., Walk, N. & Ralph, T. C. Finite-size effects in continuous-variable quantum key distribution with Gaussian postselection. *Phys. Rev. A* **101**, 052335 (2020).
28. Chrzanowski, H. M. et al. Measurement-based noiseless linear amplification for quantum communication. *Nat. Photonics* **8**, 333–338 (2014).
29. Zhao, J., Haw, J. Y., Symul, T., Lam, P. K. & Assad, S. M. Characterization of a measurement-based noiseless linear amplifier and its applications. *Phys. Rev. A* **96**, 012319 (2017).
30. Zhao, J. et al. Enhancing quantum teleportation efficacy with noiseless linear amplification. *Nat. Commun.* **14**, 4745 (2023).

31. Shajilal, B. et al. Improving Gaussian channel simulation using nonunity-gain heralded quantum teleportation. *Phys. Rev. Appl.* **22**, 054070 (2024).
32. Li, Z. et al. Non-Gaussian postselection and virtual photon subtraction in continuous-variable quantum key distribution. *Phys. Rev. A* **93**, 012310 (2016).
33. Zhong, H. et al. Enhancing of self-referenced continuous-variable quantum key distribution with virtual photon subtraction. *Entropy* **20**, 578 (2018).
34. Zhong, H., Guo, Y., Mao, Y., Ye, W. & Huang, D. Virtual zero-photon catalysis for improving continuous-variable quantum key distribution via Gaussian post-selection. *Sci. Rep.* **10**, 17526 (2020).
35. García-Patrón, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
36. Wolf, M. M., Giedke, G. & Cirac, J. I. Extremality of Gaussian quantum states. *Phys. Rev. Lett.* **96**, 080502 (2006).
37. Holevo, A. S. The capacity of the quantum channel with general signal states. *IEEE Trans. Inf. Theory* **44**, 269–273 (1998).
38. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).
39. Weedbrook, C., Pirandola, S. & Ralph, T. C. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **86**, 022318 (2012).
40. Li, L. et al. Continuous-variable quantum key distribution with on-chip light sources. *Photonics Res.* **11**, 504–516 (2023).
41. Eisert, J., Scheel, S. & Plenio, M. B. Distilling Gaussian states with Gaussian operations is impossible. *Phys. Rev. Lett.* **89**, 137903 (2002).
42. Sayat, M. et al. Satellite-to-ground continuous variable quantum key distribution: The gaussian and discrete modulated protocols in low earth orbit. *IEEE Trans. Commun*. (2024).
43. Denys, A., Brown, P. & Leverrier, A. Explicit asymptotic secret key rate of continuous-variable quantum key distribution with an arbitrary modulation. *Quantum* **5**, 540 (2021).
44. Leverrier, A. & Grangier, P. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.* **102**, 180504 (2009).
45. Ghorai, S., Grangier, P., Diamanti, E. & Leverrier, A. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Phys. Rev. X* **9**, 021059 (2019).
46. Tian, Y. et al. High-performance long-distance discrete-modulation continuous-variable quantum key distribution. *Opt. Lett.* **48**, 2953–2956 (2023).
47. Kanitschar, F. & Pacher, C. Optimizing continuous-variable quantum key distribution with phase-shift keying modulation and postselection. *Phys. Rev. Appl.* **18**, 034073 (2022).
48. Grosshans, F., Cerf, N. J., Wenger, J., Tualle-Brouri, R. & Grangier, P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *arXiv preprint quant-ph/0306141* (2003).
49. Laudenbach, F. et al. Continuous-variable quantum key distribution with Gaussian modulation-the theory of practical implementations. *Adv. Quantum Technol.* **1**, 1800011 (2018).
50. Grosshans, F. & Grangier, P. Reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv preprint quant-ph/0204127* (2002).
51. Williamson, J. On the algebraic problem concerning the normal forms of linear dynamical systems. *Am. J. Math.* **58**, 141–163 (1936).
52. Cariolaro, G. & Pierobon, G. Reexamination of bloch-messiah reduction. *Phys. Rev. A* **93**, 062115 (2016).

Acknowledgements

We extend our gratitude to Mikhael Sayat for his valuable discussions on satellite communication link budget calculations. We also extend our thanks to Dr. Aaron Tranter for his support in troubleshooting the opto-electronics involved in this experiment and to Dr. Oliver Thearle for constructing the detectors, helping with the experimental setup, and assisting with trouble-shooting. Lastly, we thank Dr. Hao Jeng for his valuable contributions to discussions on post-selection and security analysis. This research was funded by the Australian Research Council Centre of Excellence for Quantum Computation and Communication Technology (Grant No. CE170100012) and by A*STAR grants C230917010 (Emerging Technology), C230917004 (Quantum Sensing) and Q.InC Strategic Research and Translational Thrust.

Author contributions

P.K.L. and S.M.A. conceived the project. O.E., B.S., and S.M.A. developed the protocol. O.E., L.O.C., B.S., and J.Z. constructed the experiment. A.W. assisted with troubleshooting. O.E. conducted the experiment and analysed the data. T.S. set up the experiment at Data61, and S.K. collected the GG02 data with heterodyne detection. A.D. provided theoretical help in mapping Eve's covariance matrix to the density matrix. P.K.L., S.M.A., and J.Z. supervised the project. O.E. drafted the manuscript with contributions from all authors.

Competing interests

The authors declare no competing interests.

Additional information

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s42005-025-02317-5.

Correspondence and requests for materials should be addressed to Özlem Erkılıç or Jie Zhao.

Peer review information *Communications Physics* thanks Yoann Pietri for their contribution to the peer review of this work.