Supplementary Figure S 1: Maximum distance as a function of the channel noise for a fixed post processing efficiency of 95%. Dotted curve is the experimentally measured data from Fig. 4 a,d), while the solid is the coherent state bound. The gray zone represents the regime accessible with coherent state protocols. The distance scale assumes 0.2 dB loss per km. We see that the squeezing is even more important for this lower value of $\beta$ as the relative increase in achievable communication distance is larger than in the cases shown in Fig. 4 h).
Supplementary Figure S 2: Tolerable excess noise ($\epsilon_{\text{max}}$) as a function the post-processing efficiency ($\beta$) assuming a channel transmission of 10%. The dashed line corresponds to the performance of the experimentally obtained states. The kink of the dashed line relates to the fact that the experimental modulation was not optimized for each given $\beta$. The solid line gives the limit set by the optimally modulated coherent state protocol. The gray zone represents the regime accessible with coherent state protocols.
Supplementary Figure S 3: Finite size effects. We start with a subset of size $2 \cdot 10^3$ and sequentially expanding it towards the $2 \cdot 10^5$ of our experimentally obtained data blocks. For each step we build the covariance matrices and estimate the maximum tolerable channel excess noise and maximum applicable distance, comparing it to the perfect coherent protocol. Effect of the data ensemble size on the maximum secure distance upon channel noise $\epsilon = 0.1$ (left) and on the maximum tolerable channel noise upon transmittance $\eta = 0.1$ (right): the theoretical predictions based on the obtained experimental data (upper curves) compared to the results for the perfect coherent protocol (lower curves). The gray zone represents the regime accessible with coherent state protocols.
Supplementary Discussion

Imperfect post-processing

As it was already mentioned, the post-processing of the classical Gaussian data, possessed by the trusted parties, is never perfect, and the Shannon classical information cannot be exactly reached. Thus, the post-processing efficiency $\beta \in [0, 1]$ is typically introduced to the expression of the lower bound on the key rate to account for imperfect post-processing. Moreover, imperfect post-processing appeared to be the main limiting factor for the previous practical CV-QKD implementation with coherent states [6], reducing the achievable distance or, equivalently, tolerable channel noise.

The parameter $\beta$ depends on the effectiveness of the post-processing algorithms of Gaussian data decoding and error correction which depends on the signal-to-noise ratio (SNR) of the received signals, and thus depends on the attenuation and noise of the channel. The typical values previously obtained were $\beta \approx 85\%$ [6] and it was shown that the modulation must be limited upon reduced $\beta$ both for coherent [6] and squeezed state [31] protocols. However, the recently introduced multi-edge low density parity check codes [30] with the proper code rates can potentially reach efficiencies up to 98\% upon low SNR.

We make the pessimistic assumption that the post-processing efficiency does not increase with the higher nonclassicality of the states and thus the same efficiency can be reachable for both protocols. The assumption is pessimistic as the squeezing of our states is expected to yield higher SNR than the corresponding coherent state protocol. However, following this pessimistic assumption, we recalculate the performance of our experimentally obtained states for $\beta = 98\%$ and compare it to the coherent state protocol, see inset Fig. 4 g) (main text). The upper and lower curves represent the tolerable excess noise for the squeezed and coherent state protocol for identical energies, respectively, and the horizontal line represents the ideal coherent state protocol with optimized modulation. The channel transmittance was set to 10\% corresponding to 50 km of the telecom fiber.

It is evident from the graphs that the advantage of our protocol over the optimized coherent state-based one remains for imperfect post-processing. It should also be noted that the maximal tolerable excess noise is maximized for a finite sized modulation depth for both protocols. As $\beta$ further decreases no additional modulation should be applied, as enough of the modulation is effectively provided by anti-squeezing of the initial states.

We compare the performance of the protocols against continuously decreasing $\beta$ with optimized modulation of coherent states and optimally chosen modulation from our experimental results. The corresponding curves are presented in Supplementary Figure S2.

As another example we plot the tolerable loss (and distance) as a function of the excess noise for $\beta = 95\%$ on Supplementary Figure S1, similar to the inset in Fig. 4 h) (main text).

Overall the calculations confirm that the advantage of the proposed protocol is preserved upon limited reconciliation efficiency. For extremely low $\beta$, the advantage of using squeezed state is even more pronounced as recently shown in ref. [31].

Finite size effects

The number of signals, which are transmitted in a practical implementation of a QKD scheme, is never infinite, and the effect of the finiteness of the data sets must be addressed in the analysis of applicability and reliability of the protocols. The proofs of security and methods for its estimation which would take into account the finite size effects are still being developed in the field of CV-QKD with the first steps made in [33].

We numerically address the reliability of our experimentally obtained channel estimation and the subsequent theoretical predictions taking into account the finite size of the measured data. To do so we construct the covariance matrices using subsets of data points of the different length and check the stability of our results with respect to such sampling. The convergence is shown in Fig. S3.

We see that the graphs exhibit very good convergence and stability of our results with respect to the data ensemble size.

Supplementary Methods

Security analysis

In this section we show in detail how to calculate the necessary quantities for estimating the security thresholds of the proposed protocol.

The Shannon information is calculated directly from the variances and correlations between the channel input and output in the measured quadrature (which can be arbitrarily chosen by the trusted parties), prior to and conditioned on the measurements of Bob. In our theoretical description, with no loss of generality (considering symmetrical entangled state preparation by coupling of two equivalent squeezed states), we assume that the amplitude quadrature is measured by the trusted parties.

The covariance matrix of elements $\gamma_{ij} = \langle r_i r_j \rangle - \langle r_i \rangle \langle r_j \rangle$, where $\mathbf{r} = \{x_{A,B}, p_{A,B}\}$ (indices $A,B$ represent the modes of Alice and Bob), before the channel has the form

$$\gamma_{AB} = \begin{pmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB} & \gamma_B \end{pmatrix}, \quad (S1)$$

where $\gamma_A$ and $\gamma_B$ are individual mode matrices, and $\sigma_{AB}$ is their correlation matrix.
Assuming that an entangled state is optimally prepared from orthogonally squeezed states with squeezing $V_0$ and antisqueezing $V_0 + 1/\sqrt{2}$ (where $V_0$ is the excess noise of the antisqueezed quadrature), the variance of the resulting two-mode squeezed vacuum state is given by $\frac{1}{2}(\Delta V_0 + V_0 + 1/\sqrt{2})$, while the correlations between the modes quadratures are given by $\pm \frac{1}{2}(\Delta V_0 - V_0 + 1/\sqrt{2})$.

Now if Alice applies additional coherent modulation of variance $\Delta V$ on the Bob's mode and combines it with her quadrature homodyne measurement on the two-mode squeezed vacuum state applying weight factor of $g$ so that $x_A = gx_{HD} + x_M$ (where $x_{HD}$ is the result of homodyne detection and $x_M$ is the displacement due to modulation), then the resulting sub-matrix of Alice's mode is:

$$\gamma_A = \left[ g^2 \frac{V_0}{2} \left( \frac{1 + V_0^2}{V_0} + \Delta V_0 + \Delta V \right) \right] \mathbb{I} = V_A \mathbb{I},$$  \hfill (S2)

where $\mathbb{I}$ is the identity matrix. Similarly, the correlation matrix is

$$\sigma_{AB} = \left[ \frac{g^2}{2} \left( \frac{1 - V_0^2}{V_0} + \Delta V_0 + \Delta V \right) \right] \sigma_\alpha \equiv C_{AB} \sigma_z,$$  \hfill (S3)

where $\sigma_z$ is the Pauli matrix and

$$\gamma_B = \left[ \frac{1}{2} \left( \frac{1 + V_0^2}{V_0} + \Delta V_0 + \Delta V \right) \right] \mathbb{I} = V_B \mathbb{I}.$$  \hfill (S4)

Note, that the anti-squeezed excess noise effectively increases the correlation between the modes, thus acting as additional modulation of the entangled states. This effect reveals one of the advantages of the entanglement-based scenario.

Characterizing the channel by the transmission $\eta$ and the excess noise $\epsilon$, the covariance of Bob's mode is transformed to

$$\gamma_B = \left[ \eta (V_B + \epsilon) + 1 - \eta \right] \mathbb{I} = V'_B \mathbb{I}.$$  \hfill (S5)

and the covariance with Alice is given by

$$\sigma'_{AB} = \sqrt{\eta} C_{AB} \sigma_z \equiv C'_{AB} \sigma_z.$$  \hfill (S6)

The mutual Shannon information is then given by

$$I_{AB} = \frac{1}{2} \log_2 \frac{V_A}{V_A - C'_{AB}}.$$  \hfill (S7)

The gain factor $g$ is optimized so that it maximizes the mutual information $I_{AB}$. After straightforward calculation of the local extremum of mutual information, the optimal gain factor appears to be independent on the channel parameters and modulation variance, and is given by

$$g = \frac{1}{V_0} + \Delta V_0 - V_0$$  \hfill (S8)

being simply the ratio of the correlation between two modes of the initial entangled state to the variance of its modes.

The Holevo quantity is expressed through the von Neumann entropies of the state $\rho_E$, which is available to Eve and the same state, $\rho_E^{\rho}$, conditioned by Bob's measurement (in the reverse reconciliation scenario). Then $\chi_{BE} = S(\rho_E) - S(\rho_E^F)$, where $S(\cdot)$ denotes the von Neumann entropy of the respective state.

To investigate the effects of loss and noise on the security, we use two different strategies. First, we implement the entangling cloner attack, which was shown to be an optimal individual attack in [26] and used for the collective attacks in [7]. In this case, Eve's von Neumann entropies are calculated directly from the state of her two-mode entangling cloner, emulating the noisy and lossy untrusted channel. Then we cross-check our results by applying the general method of security analysis for the case of collective attacks [6, 13].

Thus, in order to calculate the Holevo quantity we need to purify the two-mode state, described by the covariance matrix (S1).

**Theoretical purification.** For the theoretical estimate we start with an EPR source. We vary the weight factor by variably coupling the mode, going towards Alice, to a strongly squeezed vacuum state (the squeezing direction is the same, as measured by Alice). The coherent modulation is emulated by coupling each mode to a strong two-mode entangled state on two strongly unbalanced beamsplitters. The resulting 5-mode state $\tilde{\rho}_{AB} = \tilde{\rho}_{ABCDF}$ is pure and so is the conditional state $\tilde{\rho}_{AB}^{x_{AB}} = \tilde{\rho}_{ACDF}^{x_{ACDF}}$ and the excess auxiliary modes can be trusted. (In case Bob's trusted detection noise is considered, two more entangled modes should be added to purify the overall 7-mode state). The calculation of respective covariance matrix $\gamma_{ABCDF}$ is then straightforward using the beamsplitter transformations. The covariance matrix of the state $\rho_{ACDFB}$ conditioned by Bob's measurement $x_B$ is given by [6]

$$\gamma_{ABCD} = \gamma_{ABCD} - \sigma'_{ACDF} (X_{ABX})^{MP} \sigma'_{ACDF}, \hfill (S10)$$

where $\gamma_{ABCD}$ is the submatrix of matrix $\gamma_{ABCDF}$ (describing the state $\rho_{ABCD}$), which corresponds to modes
A, C, D and F and their correlations, while $\sigma_{ACDF}^x$ is submatrix of $\gamma_{ABCD}$, describing the correlations between mode $B$ and modes $A, C, D$ and $F$. Matrix $X$ is $2 \times 2$ diagonal matrix with diagonal elements $\{1, 0\}$, and $MP$ stands for Moore-Penrose inverse. The corresponding eigenvalues of matrices $\gamma_{ABCD}$ and $\gamma_{ACDF}^x$ can be then calculated numerically and give the resulting Holevo quantity and the final lower bound on the secure key rate.

Experimental security analysis. For the experimental estimate we have to use the general scheme. The measured covariance matrix is of the form

$$\gamma_{AB} = \begin{pmatrix} V_A^x & V_B^x \\ 0 & V_A^p \\ C_{AB}^x & 0 \\ 0 & C_{AB}^p \end{pmatrix}, \quad (S11)$$

where each of the $V$’s and $C$’s have the measured values. Indices $x$ and $p$ reflect the asymmetry of the matrix for different quadratures, which means that in a realistic case the mutual information depends on the choice of quadrature (contrary to the ideal case, where identical squeezed states are coupled to construct the entangled states).

To purify this matrix we imagine it to be mode A and B of the pure 4-mode state shown on Fig. 1 b) (main text). The general 4-mode covariance is of the form

$$\gamma'_{ABCD} = \begin{pmatrix} V_A^x & V_B^x & C_{AB}^x & 0 \\ 0 & V_A^p & 0 & V_B^p \\ C_{AC}^x & C_{BC}^x & 0 & V_C \\ 0 & C_{AC}^p & 0 & C_{BC}^p \end{pmatrix},$$

where

$$V_A^x = -2at_1t_2 + \frac{t_2(V_2 + d)}{s_2^2} + \frac{(1 - t_2)(V_1 - d)}{s_2^2},$$

$$V_B^x = 2at_1t_2 + \frac{t_2(V_1 - d)}{s_1^2} + \frac{(1 - t_2)(V_2 + d)}{s_1^2},$$

$$V_A^p = -2bt_1t_2 + T_2s_2^2(V_2 + d) + (1 - T_2)s_2^2(V_1 - d),$$

$$V_B^p = 2bt_1t_2 + T_2s_1^2(V_1 - d) + (1 - T_2)s_1^2(V_2 + d),$$

$$C_{AB}^x = at_1(1 - 2T_2) + t_2\left(\frac{s_1^2}{s_2^2} - \frac{V_1 - V_2}{s_2^2}\right),$$

$$C_{AB}^p = bt_1(1 - 2T_2) + t_2\left(\frac{s_2^2}{s_1^2} - \frac{V_1 - V_2}{s_1^2}\right),$$

and similarly for other elements of the matrix (S12). Here we denoted $s_{1(2)} = \exp r_{1(2)}; r_{1(2)} = \sqrt{T_{1(2)}(1 - T_{1(2)})}; a = (V_1 - V_2)/(s_1s_2); b = (V_1 - V_2)s_1s_2,$

and $d = T_1(V_1 - V_2)$. $r_{1(2)}$ is the $r$-parameter of squeezer 1 (2), $V_{1(2)}$ is the EPR variance of EPR source 1 (2) and $T_{1(2)}$ is the transmittance of beamsplitter 1 (2) as shown on Fig. 1 b) (main text).

Now the proper parameters of the purification $r_1, r_2, V_1, V_2, T_1, T_2$ can be found from the set of 6 equations. Then the matrix (S12), constructed from the obtained parameters, will correspond to the 4-mode purification of the arbitrary 2-mode state, described by the

Supplementary References