npj | Quantum Information

www.nature.com/npjqi

Correction: Author correction

ARTICLE OPEN

Complete elimination of information leakage in continuous-variable quantum communication channels

Christian S. Jacobsen[1], Lars S. Madsen[1], Vladyslav C. Usenko[2], Radim Filip[2] and Ulrik L. Andersen[1]

In all lossy communication channels realized to date, information is inevitably leaked to a potential eavesdropper. Here we present a communication protocol that does not allow for any information leakage to a potential eavesdropper in a purely lossy channel. By encoding information into a restricted Gaussian alphabet of squeezed states we show, both theoretically and experimentally, that the Holevo information between the eavesdropper and the intended recipient can be exactly zero in a purely lossy channel while minimized in a noisy channel. This result is of fundamental interest, but might also have practical implications in extending the distance of secure quantum key distribution.

npj Quantum Information (2018)4:32 ; doi:10.1038/s41534-018-0084-0

INTRODUCTION

Security in communication is of utmost importance in modern society. It allows for the delivery of information to the intended recipients while preventing unauthorized eavesdroppers from accessing it. Conceptually, it can be treated as a tripartite communication network in which two entities (e.g., Alice and Bob) intend to communicate while a third party—the eavesdropper (known as Eve)—tries to intercept the message. See Fig. 1, where the mutual information between the three parties is represented schematically. If successful, the interception will generate correlations between all three parties, as in Fig. 1a, possibly rendering the communication scheme insecure. To regain security, the correlations between the intended recipient and the interceptor must be suppressed. This can be done by means of data post-processing such as privacy amplification—a method commonly used to establish security in quantum key distribution (QKD) schemes.[1,2] However, privacy amplification is only successful if the information I_{AB} between the trusted parties Alice and Bob is larger than the information between Bob and Eve prior to the implementation of the procedure.[3]

As an alternative to data post-processing, the information gained by an eavesdropper can be suppressed by using an entanglement-based protocol followed by entanglement distillation or purification.[4] Here the two communicating parties seek to share entangled states but due to the interception, the system ends up in a three-party entangled state, subsequently reduced to a purified two-party entangled state between Alice and Bob, thereby eliminating the correlations with the eavesdropper. This strategy is however very challenging as it requires multi-copy non-Gaussian transformations in conventional communication schemes based on Gaussian states encoding and homodyne/heterodyne detection.[5–7]

In this letter, we present a completely different approach for minimizing information leakage which is not based on conventional a posteriori error correction or privacy amplification and therefore does not rely on any prior information advantage. Instead of suppressing the information of Eve by privacy amplification or distillation at Bob's station, we propose the opposite approach of designing the Gaussian input states and alphabet at Alice's station in such a way that Eve cannot gain any information at any time in a purely lossy channel, as in Fig. 1b. We show that by encoding the information into squeezed states of a restricted Gaussian alphabet it is possible to completely and deterministically eliminate the presence of an eavesdropper, corresponding to the realization of a channel with a Holevo information of zero. The protocol is based on continuous variables (CV) in which quadratures are modulated and measured with homodyne detectors,[4,8,9] which is contrasted with discrete variables communication where photon counters are used. We note that no analogue of our proposed scheme for the complete elimination of the Holevo information is known for discrete variables. Unlike covert communication[10,11] where the transmission of information is hidden from the eavesdropper, the presence of the signal states are still detectable by Eve in the proposed scheme. In contrast to the private states known from discrete variables,[12,13] which still rely on distillation procedures, our method allows for direct elimination of the information accessible by an eavesdropper using proper state preparation and ideally needs no distillation.

RESULTS

We consider the elimination of information leakage in the context of QKD. In CVQKD protocols with reverse reconciliation[14–22] the lower bound on the rate of secret key generation in the asymptotic limit of an infinitely long key is given by:

$$R = \beta I_{AB} - \chi_{EB}, \tag{1}$$

where I_{AB} is the mutual information between Alice and Bob as defined through the Shannon entropy,[3,23] $\beta \in]0; 1]$ is the post-processing efficiency, and χ_{EB} is the Holevo information which is an upper bound on the information I_{EB} acquired by Eve.[24] A secret

[1]Center for Macroscopic Quantum States (bigQ), Department of Physics, Technical University of Denmark, Fysikvej 2800 Kongens Lyngby, Denmark and [2]Department of Optics, Palacky University, 17. listopadu 12, 771 46 Olomouc, Czech Republic
Correspondence: Christian S. Jacobsen (chrsch@fysik.dtu.dk) or Ulrik L. Andersen (ulrik.andersen@fysik.dtu.dk)

Received: 5 December 2017 Revised: 6 June 2018 Accepted: 4 July 2018
Published online: 24 July 2018

Published in partnership with The University of New South Wales

key can therefore only be generated when $\beta I_{AB} > \chi_{EB}$. In all previously proposed protocols, the Holevo information has been non-zero (even in principle), which in turn has put stringent conditions onto the processed mutual information between Alice and Bob, βI_{AB}. This condition has been experimentally fulfilled by applying state-of-the-art post-processing protocols[25] with high efficiency and low-noise homodyne detectors.[8,26–31] These stringent conditions on Bob's measurements and data processing to enable security can however be largely relaxed by reducing the Holevo information that upper-bounds the information leakage.

Minimization of information leakage

We consider a prepare-and-measure CVQKD protocol where information is encoded solely into a single quadrature (here the amplitude quadrature X with a variance V_{sig}) of a Gaussian squeezed state of amplitude quadrature variance V_{sqz} (Fig. 2a), and investigate theoretically under which condition it is possible to completely decouple a potential eavesdropper from the channel.

The maximal information, that is the capacity, between Eve and Bob is given by the Holevo quantity:

$$\chi_{EB} = S(E) - S(E|B), \tag{2}$$

where S(E) is the von Neumann entropy of the state received by Eve and S(E|B) is the von Neuman entropy of the state at Eve conditioned on the measurement at Bob. In the case of a noisy quantum channel, the general collective attack can be accessed by assuming that Eve holds the purification of the state shared between Alice and Bob.[32,33] Using the triangle inequality, one can derive the self-duality property of the von Neumann entropy, which states that S(E) = S(AB) and S(E|B) = S(A|B).[34] From (2), it is clear that a Holevo information of zero requires S(E) = S(E|B), and from the purification this translates into S(AB) = S(A|B). This condition is evaluated in the following by individually deducing S(AB) and S(A|B).

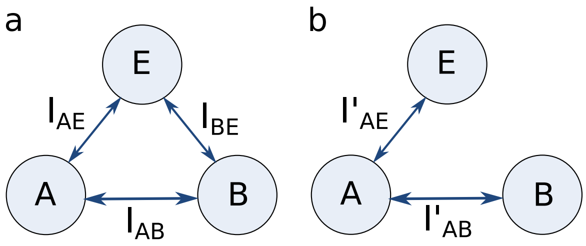

Fig. 1 A tripartite communication scenario between Alice (A), Eve (E) and Bob (B). **a** Each party shares some amount of mutual information, given in terms of Shannon entropies as $I_{XY} = H(X) + H(Y) - H(X, Y)$, with the other two parties. **b** In the context of message security, it is the goal of the honest parties, Alice and Bob, to completely eliminate the information that they share with Eve. By removing all correlations between Eve and Bob (that is $I'_{BE} = 0$), the adversary obtains no information about what Bob has measured, and thus secret communication between A and B can be established

For a Gaussian protocol, where Gaussian attacks are optimal in the asymptotic limit,[32,35] the von Neumann entropies may be easily calculated from the symplectic spectrum of the covariance matrices of the corresponding states.[8] To enable an explicit protocol description, we switch to the equivalent EPR based protocol[36] where an asymmetric two-mode squeezed state is shared between Alice and Bob as shown in Fig. 2b.[37–39]

The variance of a symmetric two-mode squeezed vacuum state is denoted μ while the single mode squeezing transformation is represented by the squeezing parameter r such that amplitude and phase quadrature variances of the modes sent to Bob are μe^{-2r} and μe^{2r}, respectively. The shared state is represented by a covariance matrix, which we may generally write as,

$$\gamma_{AB} = \begin{bmatrix} \gamma_A & \sigma_{AB} \\ \sigma_{AB} & \gamma_B \end{bmatrix}, \tag{3}$$

where $\gamma_A = \mathrm{diag}[\mu, \mu]$ is the covariance matrix of the EPR mode kept by Alice, $\gamma_B = \mathrm{diag}[T(e^{-2r}\mu + \epsilon) + 1 - T, T(\mu e^{2r} + V_\epsilon + \epsilon) + 1 - T]$ is the covariance matrix of the mode received by Bob, and $\sigma_{AB} = \mathrm{diag}\left[\sqrt{Te^{-2r}(\mu^2 - 1)}, -\sqrt{T(\mu^2 - 1)e^{2r}}\right]$ is the sub-block of the global covariance matrix describing the correlation between modes. Here T is the transmittance, V_ϵ is the variance of the excess noise of the anti-squeezed quadrature while ϵ represents the quadrature symmetric excess noise contribution of the channel. γ_{AB} is constructed such that the prepare-and-measure scheme, in Fig. 2a, and the EPR scheme, in Fig. 2b, are equivalent if $\mu = \sqrt{1 + V_{sig}/V_{sqz}}$ and $r = -1/2 \ \ln\left[\sqrt{V_{sqz}\left(V_{sqz} + V_{sig}\right)}\right]$.[36] By equivalence we mean that the mutual information shared between Alice and Bob is the same in the two schemes and that the signal mode through the quantum channel looks the same to an outside observer, such as Eve, in both schemes.

The symplectic eigenvalues of (3),[40] denoted $\nu_{AB,+}$ and $\nu_{AB,-}$, can now be used to find the entropy S(AB) via the relation $S(AB) = g(\nu_{AB,+}) + g(\nu_{AB,-})$ where g is the bosonic information function, g

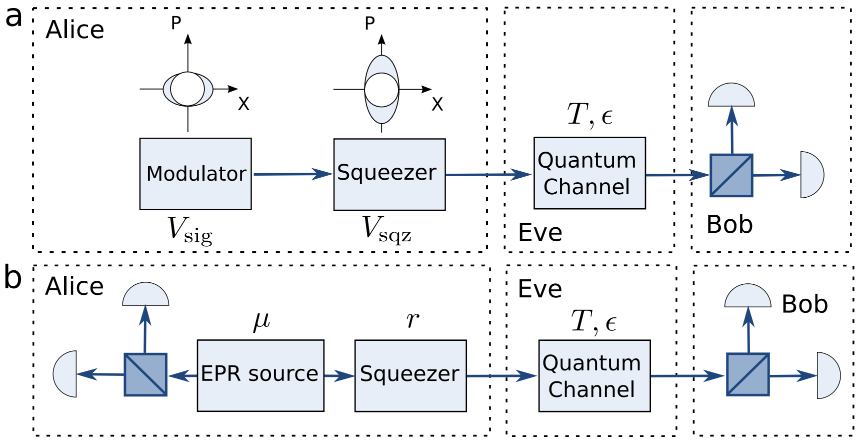

Fig. 2 Equivalent protocol schemes. **a** Prepare-and-measure scheme for a quantum communication protocol with zero information leakage. An ensemble of amplitude quadrature displaced coherent states is squeezed to have an overall amplitude quadrature noise variance of vacuum before being sent into the quantum channel. **b** Equivalent entanglement-based scheme of the quantum communication protocol with zero information leakage. An EPR state is prepared, with a local mode measured by Alice and the outgoing mode squeezed before being sent into the quantum channel

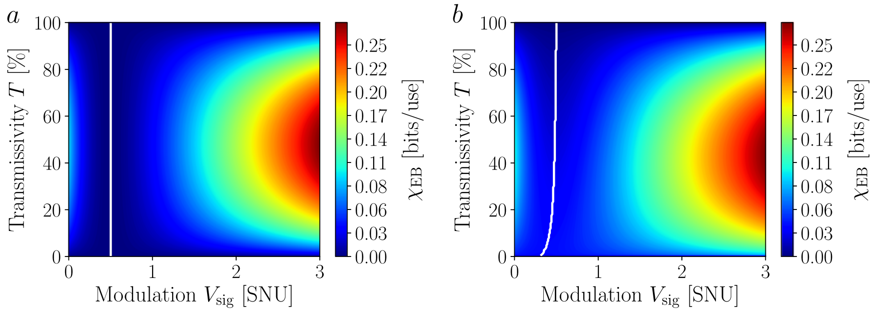

Fig. 3 Numerical calculation of leakage elimination. **a** Contour plot of the Holevo information bound in terms of signal modulation and transmittance in the quantum channel, with no excess noise and 0.5 SNU squeezing, corresponding to -3 dB. The white line indicates the minimum information leakage. **b** Contour plot of the Holevo information bound in terms of signal modulation and transmittance loss in the quantum channel, with excess noise $\epsilon = 0.01$ SNU and 0.5 SNU squeezing, corresponding to -3 dB. The white line indicates the minimum, but non-zero, information leakage

$(x) = \frac{x+1}{2}\log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2}\log_2\left(\frac{x-1}{2}\right)$.[41] Likewise we find the conditional entropy S(A|B) from the symplectic eigenvalue, $\nu_{\rm A|B}$, of the conditional covariance matrix $\gamma_{\rm A|B} = \gamma_{\rm A} - \gamma_{\rm B,11}^{-1}\sigma_{\rm AB}\Pi\sigma_{\rm AB}$, where $\Pi = {\rm diag}[1, 0]$ assuming an X-quadrature measurement at Bob, and $\gamma_{\rm B,11}$ is the first diagonal element of $\gamma_{\rm B}$. It follows then that S(A|B) $= g(\nu_{\rm A|B})$.

Finally, we arrive at the condition, $g(\nu_{\rm AB,+}) + g(\nu_{\rm AB,-}) = g(\nu_{\rm A|B})$, for the complete elimination of Holevo information between Eve and Bob. For more details on this derivation, see the Supplementary Information. For a purely lossy channel without any excess noise ($\epsilon = 0$) this translates into the simple relation: $V_{\rm sqz} + V_{\rm sig} = 1$. This implies that $\chi_{\rm EB}$ can become zero while $R \neq 0$. It is clear that this relation cannot be realized with coherent states as in this case $V_{\rm sqz} = 1$ thus rendering the alphabet of zero size; $V_{\rm sig} = 0$. Squeezed states for which $V_{\rm sqz} < 1$ are thus required to eliminate the Holevo quantity. To fulfill the condition, the size of the Gaussian alphabet has to be $V_{\rm sig} = 1 - V_{\rm sqz}$, and for very large squeezing degrees ($V_{\rm sqz} \to 0$) the secure information rate in (1) approaches $R = \beta I_{\rm AB} = -\beta\frac{1}{2}\log_2(1-\eta)$. This shows that a secret key can in principle be generated for any channel loss and for any post-processing efficiency. It is also interesting to note that the elimination of the Holevo information is completely independent on the noise in the anti-squeezed quadrature, that is, it is independent on the impurity of the squeezed states.[42] We further remark that for ideal reconciliation efficiency, $\beta = 1$, the rate reaches half of the fundamental repeaterless bound for which $R = -\log_2(1-\eta)$.[43]

Evaluation of the Holevo quantity for the general case is found numerically and is shown in Fig. 3 for a purely lossy channel (Fig. 3a) and for a channel with an untrusted excess noise of $\epsilon = 0.01$ shot-noise units (SNU) (Fig. 3b). The minima of the Holevo information are marked by the white curves which for the purely lossy channel is exactly zero ($\chi_{\rm EB} = 0$) regardless of the transmittance for $V_{\rm sig} = V_{\rm sqz} = 0.5$ SNU.

While proper state modulation can eliminate the Holevo information between Eve and Bob, it does not eliminate the quantum mutual information between them, defined as S(E) + S(B) − S(EB). This means that the subsystems E and B remain correlated in the quantum sense despite the fact that the information leakage is terminated. Such quantum mutual information vanishes completely only when no squeezing and no modulation is realized by the sender, which is shown in detail in the Supplementary Information. We also note that the correlations remain non-zero in the conjugate quadrature, but this is irrelevant since information is only encoded in the amplitude quadrature. Though single quadrature encoding reduces the alphabet, it does not compromise security, once basis switching and channel estimation are performed. In an actual implementation the conjugate quadrature would have to be measured to check the magnitude of the excess noise.[37,38]

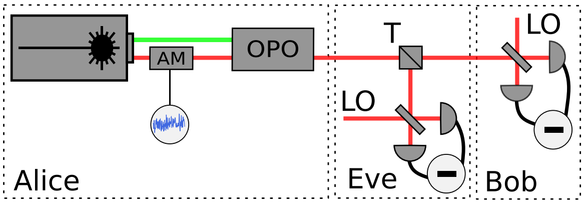

Fig. 4 Scheme of the experimental implementation of the quantum communication protocol with zero information leakage. An ensemble of coherent states is prepared by adding white noise to an amplitude modulator. The ensemble is squeezed by injecting it into an OPO, which is pumped by light at λ/2. The resulting ensemble of squeezed coherent states is sent to the quantum channel, with transmissivity T. Bob measures the channel output using homodyne detection, using an LO from the same laser. Eve also uses homodyne detection with an LO from the same laser. AM: Amplitude Modulator, OPO: Optical Parametric Oscillator, LO: Local oscillator, T: Transmissivity of the quantum channel

The obtained result is based on the security analysis of Gaussian CVQKD protocols against collective attacks, which has been shown to be valid against the most general coherent attacks in the asymptotic limit.[44] The estimation of the lower bound on the key rate is thus performed in the asymptotic regime. In the finite-size regime the lower bound on the key rate is further decreased by the security parameter Δ,[45] which depends on the failure probability of the privacy amplification and speed of convergence of smooth min-entropy to von Neumann entropy.[46] For finite data, the minimization of information leakage becomes even more important, allowing trusted parties to partly compensate the reduction of the key rate due to finite-size effects, using proper state engineering, which does not affect the implementation-dependent Δ parameter directly.

Generation of states with no information leakage

We now implement a proof of principle experiment demonstrating the complete elimination of the information to an eavesdropper in a lossy channel. A schematic of the setup is depicted in Fig. 4. The state is produced experimentally by squeezing an asymmetric thermal state: A bright laser beam at 1064 nm is modulated using an electro-optical modulator that is driven by a function generator. It produces white noise within the detection bandwidth, and forms sidebands on the bright beam. These sidebands (at 4.9 MHz with a bandwidth of 90 kHz) carry the information and correspond to an asymmetric thermal state. The modulated light beam is subsequently injected into an optical parametric oscillator (OPO) which squeezes, in this case, the

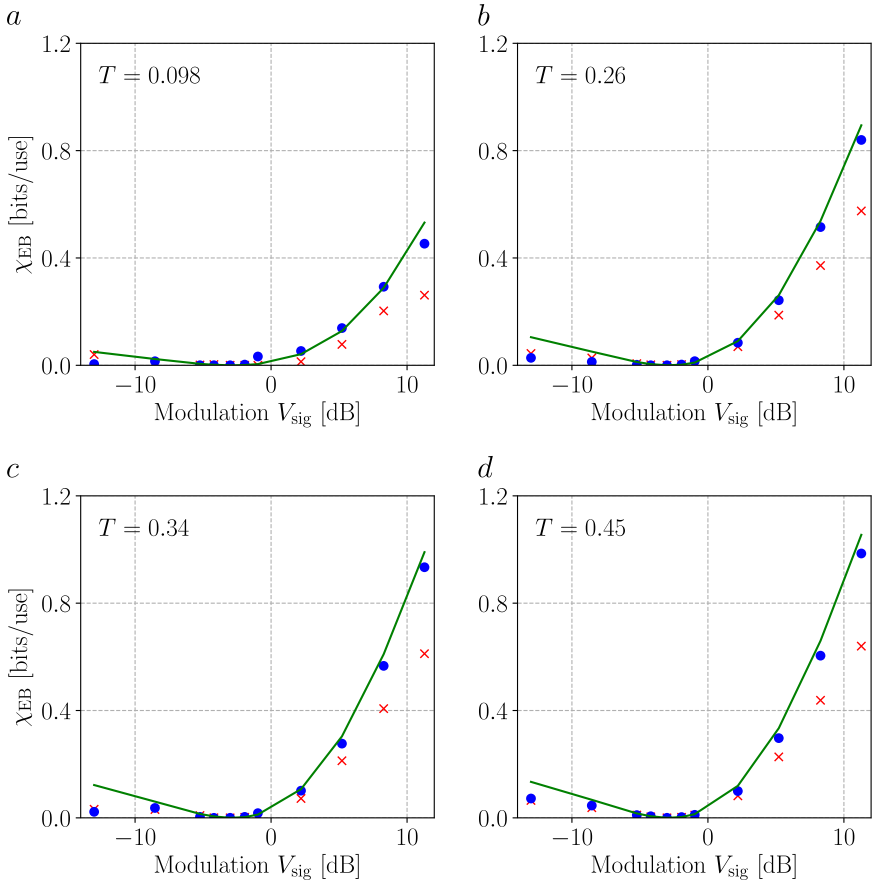

Fig. 5 Holevo information versus modulation depth for various transmittances. The modulation depth is normalized to the variance of shot noise. The Holevo information estimation was performed using three different approaches, namely direct estimation, general purification-based estimation, and a theoretical prediction from the channel parameters, shown with red crosses, blue dots and a green line respectively

amplitude quadrature by 3 dB. For more details on the OPO we refer to.[28] The final output state is thus an asymetric squeezed state alphabet where the amplitude quadrature signal information is sent to a computer while the states are injected into the lossy transmittance channel. Channel loss is simulated by a beam splitter with controllable transmittances. Eve measures the amplitude and phase quadrature of the reflected part using a homodyne detector with an efficiency of 95%, while Bob uses a homodyne detector with 85% efficiency to measure the amplitude and phase quadratures of the transmitted part. The measured data are electronically down-converted to dc, low-pass filtered and digitized. We thus have access to the covariance matrices of Alice, Bob and Eve as well as the amplitude quadrature correlation coefficients between Alice and Bob and both quadrature correlation coefficients between Eve and Bob. By means of these entities, we are now in the position to estimate the Holevo information using two different approaches: Either conservatively assuming that Eve holds the entire purification of the state shared by Alice and Bob or, as a comparison, directly from Eve's measurements.

Purification-based estimation of Holevo information. In the first approach to finding the Holevo information, Eve is powerful and thus holds the entire purification of the virtually entangled state shared between Alice and Bob, as is the case in a standard QKD analysis.[8] In order to do this we need to perform the purification on Alice's site. This is done by transforming the measured parameters at Bob backward through the channel knowing its transmittance. This includes the amplitude quadrature correlations between Alice and Bob, $C^{(0)}_{\mathrm{AB},X} = C_{\mathrm{AB},X}/\sqrt{T}$, and the quadrature variances $V^{(0)}_{\mathrm{B},i} = \left(V_{\mathrm{B},i} + T - 1\right)/T$ where $i = X, P$. We are then in the position to construct the covariance matrix of the entanglement-equivalent scheme at Alice with the modes that we name *A* and *A*′. This state is then purified according to a 4-mode purification procedure based on the Bloch-Messiah reduction theorem,[47] also known as Euler decomposition,[8] similarly to what was done in ref. [28] The result of this procedure is a pure state of 4-modes which we label *AA′CD*. Mode *A′* is then propagated through the channel to obtain the global state *ABCD*, which is then assumed to be purified by modes accessible only to Eve. Using this global state we finally calculate the Holevo information, and plot the result for different modulation strenghts and different transmittances as shown in Fig. 5 (blue dots).

Direct estimation of Holevo information. In the second approach, we directly estimate the Holevo bound by performing homodyne detection on the mode of light reflected from the channel, which is accesible to Eve. We use the measured data at Eve and Bob as well as the correlation coefficients, to deduce their individual covariance matrices and the associated correlations. This allows us to simulate Eve's collective attack by finding the conditional von Neumann entropy S(E|B) and Eve's von Neumann entropy S(E). Finally, using relation (2), we directly find the Holevo information and plot the results in Fig. 5 (red crosses) for different values for the modulation depth.

Theoretical prediction of Holevo information. In addition to the direct and purification-based estimation of the Holevo information, we also plot the theoretically expected Holevo information in terms of the signal modulation in the prepare-and-measure scheme, by numerically evaluating Holevo information of the derived covariance matrix with the experimentally established channel parameters.

Complete elimination of the Holevo information for any of the realized transmittances is clearly visible at the previously established condition, namely for $V_{\mathrm{sig}} = 0.5$ SNU $= -3$ dB given a $V_{\mathrm{sqz}} = 0.5$ SNU $= -3$ dB squeezed state such that $V_{\mathrm{sig}} + V_{\mathrm{sqz}} = 1$ SNU, regardless of the method used for the estimation. The direct estimation approach tends to underestimate the Holevo information, while the purification-based approach closely follows the theoretical prediction of the entanglement-based scheme described previously. We provide further details on the three approaches in the Supplementary Information.

It is evident from Fig. 5 that the direct estimation method underestimates the Holevo bound. This is caused by measurement imperfections that Eve ideally would not have. On the contrary, the purification-based approach corresponds to Eve perfectly obtaining maximum information associated with the noise level. This approach then closely follows the theoretical prediction obtained from the entangled-based scheme.

The measured data ensemble size of the order of 10^5 was sufficiently large to provide good convergence of the Holevo bound and correspondence to the theory predictions. In a practical realization of QKD, however, the key is degraded by the finite-size effects and larger data ensemble sizes would be required to make this effect negligible. We estimate the value of the Δ parameter[45] in the Supplementary Information.

It is worth mentioning that the aim of our experiment is not to produce a secret key, but to demonstrate the complete elimination of the Holevo information in a purely lossy channel. To produce a secret key, it is important to implement random detection of conjugate quadratures at Bob's station and to modulate the anti-squeezed quadrature at Alice's station for increased key rate or use a slightly modified analysis assuming single quadrature modulation.[37,38]

DISCUSSION

In our study, we first considered purely lossy channels, in which complete elimination of information leakage can be achieved. Noise may appear first of all as the result of imperfect detection, but in this case it can be calibrated and assumed trusted, i.e., being out of control by Eve. Since such noise does not contribute to Eve's information on Bob's measurement results,[48] the complete elimination of information leakage can also be achieved upon detection noise using the same modulation setting. In the case when untrusted noise is present in the channel, however, the information leakage to Eve cannot be completely eliminated, but it can be effectively minimized using the same condition on state preparation as for a lossy channel.[42]

We have shown theoretically that a properly modulated squeezed state can be used to completely and deterministically decouple an eavesdropper from a purely lossy quantum channel without the use of entanglement distillation. The scheme has been confirmed experimentally using squeezed states of light and homodyne detection. The decoupling was shown to be completely independent on the amount of losses in the channel and the purity of the squeezed states used in the alphabet. This result is of fundamental interest in the context of quantum security, and we believe that the proposed protocol could offer an advantage, particularly in conjunction with a simple Gaussian error correcting scheme such as[49] for the removal of non-Markovian excess noise, with channel multiplexing[50] or increased repetition rate.

A direction of further study can be the application of our proposed scheme in CVQKD with low efficiency error correcting codes, where an overall speedup in secret key generation may result from a partial reduction of Eve's information, even though the size of the alphabet is reduced. This can be useful in schemes where the error correction step limits the key generation rate.

METHODS

We refer to the Supplementary Information for additional details on the derivation of the information elimination condition and experimental methods.

Data availability

Raw data and scripts for the computation of the Holevo quantity are available from the authors upon reasonable request.

ACKNOWLEDGEMENTS

We acknowledge the support from the Center for Quantum Innovation (Qubiz), supported by the Innovation Foundation Denmark. We also acknowledge support from the Danish National Research Foundation (bigQ). V.C.U. acknowledges the project LTC17086 of the INTER-EXCELLENCE program of the Czech Ministry of Education, project 7AMB17DE034 of the Czech Ministry of Education and COST Action CA15220 "QTSpace". R.F. acknowledges grant No. GB14-36681G of the Czech Science Foundation.

AUTHOR CONTRIBUTIONS

R.F and V.C.U. developed the theory. L.S.M. and U.L.A. conceived the experiment. C.S.J and L.S.M. performed the experiment. C.S.J., V.C.U., and L.S.M. analyzed the data. All authors contributed to the manuscript.

ADDITIONAL INFORMATION

Supplementary information accompanies the paper on the *npj Quantum Information* website (https://doi.org/10.1038/s41534-018-0084-0).

Competing interests: The authors declare no competing interests.

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

REFERENCES

1. Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **74**, 145–195 (2002).
2. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
3. Devetak, I. & Winter, A. In *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, vol. **461**, 207–235 (2005).
4. Braunstein, S. L. & Loock, Pv Quantum information with continuous variables. *Rev. Mod. Phys.* **77**, 513–577 (2005).
5. Eisert, J., Scheel, S. & Plenio, M. B. Distilling Gaussian states with Gaussian operations is impossible. *Phys. Rev. Lett.* **89**, 137903 (2002).
6. Fiurášek, J. Gaussian transformations and distillation of entangled Gaussian states. *Phys. Rev. Lett.* **89**, 137904 (2002).
7. Giedke, G. & Cirac, J. I. Characterization of Gaussian operations and distillation of Gaussian states. *Phys. Rev. A* **66**, 032316 (2002).
8. Weedbrook, C. et al. Gaussian Quantum Information. *Rev. Mod. Phys.* **84**, 621–669 (2011).
9. Andersen, U. L., Leuchs, G., & Silberhorn, C. Continuous-variable quantum information processing. *Laser Photon. Rev.* **4**, 337–354 (2010).
10. Bash, B. A. et al. Quantum-secure covert communication on bosonic channels. *Nat. Commun.* **6**, 8626 (2015).
11. Arrazola, J. M. & Scarani, V. Covert quantum communication. *Phys. Rev. Lett.* **117**, 250503 (2016).
12. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. Secure key from bound entanglement. *Phys. Rev. Lett.* **94**, 160502 (2005).
13. Dobek, K., Karpiński, M., Demkowicz-Dobrzański, R., Banaszek, K. & Horodecki, P. Experimental extraction of secure correlations from a noisy private state. *Phys. Rev. Lett.* **106**, 030501 (2011).
14. Cerf, N. J., Lévy, M. & Van Assche, G. Quantum distribution of Gaussian keys using squeezed states. *Phys. Rev. A* **63**, 052311 (2001).

15. Silberhorn, C., Ralph, T. C., Lutkenhaus, N. & Leuchs, G. Continuous variable quantum cryptography: beating the 3 db loss limit. *Phys. Rev. Lett.* **89**, 167901 (2002).
16. Garca-Patrón, R. & Cerf, N. J. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **102**, 130501 (2009).
17. Pirandola, S., Mancini, S., Lloyd, S. & Braunstein, S. L. Continuous variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **4**, 726–730 (2008).
18. Grosshans, F. & Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **88**, 057902 (2002).
19. Weedbrook, C. et al. Quantum cryptography without switching. *Phys. Rev. Lett.* **93**, 170504 (2004).
20. Reid, M. D. Quantum cryptography with a predetermined key, using continuous-variable einstein-podolsky-rosen correlations. *Phys. Rev. A* **62**, 062308 (2000).
21. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **61**, 022309 (2000).
22. Ralph, T. C. Security of continuous-variable quantum cryptography. *Phys. Rev. A* **62**, 062306 (2000).
23. Shannon, C. E. A Mathematical Theory of Communication, Part 3. *Bell Syst. Tech. J.* **27**, 623–656 (1948).
24. Holevo, A. S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Inf. Transm.* **9**, 3–11 (1973).
25. Leverrier, A., Alléaume, R., Boutros, J., Zémor, G. & Grangier, P. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Phys. Rev. A* **77**, 042325 (2008).
26. Eberle, T. et al. Gaussian entanglement for quantum key distribution from a single-mode squeezing source. *New J. Phys.* **15**, 053049 (2013).
27. Lance, A. M. et al. No-switching quantum key distribution using broadband modulated coherent light. *Phys. Rev. Lett.* **95**, 180503 (2005).
28. 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).
29. Grosshans, F. et al. Quantum key distribution using gaussian-modulated coherent states. *Nature* **421**, 238–241 (2003).
30. 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).
31. Heim, B. et al. Atmospheric channel characteristics for quantum communication with continuous polarization variables. *Appl. Phys. B* **98**, 635–640 (2010).
32. Garca-Patrón, R. & Cerf, N. J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **97**, 190503 (2006).
33. Nielsen, M. A. & Chuang, I. L. *Quantum Computation and Quantum Information*, 10th edn (Cambridge University Press, 2010).
34. Araki, H. & Lieb, E. H. Entropy inequalities. *Commun. Math. Phys.* **18**, 160–170 (1970).
35. Navascués, M., Grosshans, F. & Acín, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **97**, 190502 (2006).
36. Grosshans, F., Cerf, N., Wenger, J., Tualle-Brouri, R. & Grangier, P. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *Quantum Inf. Comput.* **3**, 535 (2003).
37. Usenko, V. C. & Grosshans, F. Unidimensional continuous-variable quantum key distribution. *Phys. Rev. A.* **92**, 062337 (2015).
38. Gehring, T., Jacobsen, C. S. & Andersen, U. L. Single-quadrature continuous-variable quantum key distribution. *Quantum Inf. Comput.* **16**, 1081 (2016).
39. Derkach, I., Usenko, V. C. & Filip, R. Preventing side-channel effects in continuous-variable quantum key distribution. *Phys. Rev. A* **93**, 032309 (2016).
40. Serafini, A., Illuminati, F. & De Siena, S. Symplectic invariants, entropic measures and correlations of Gaussian states. *J. Phys. B. At. Mol. Opt. Phys.* **37**, 21–28 (2004).
41. Holevo, A. S., Sohma, M. & Hirota, O. Capacity of quantum Gaussian channels. *Phys. Rev. A - At. Mol. Opt. Phys.* **59**, 1820–1828 (1999).
42. Usenko, V. C. & Filip, R. Squeezed-state quantum key distribution upon imperfect reconciliation. *New J. Phys.* **13**, 113007 (2011).
43. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
44. Renner, R. & Cirac, J. I. de Finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography. *Phys. Rev. Lett.* **102**, 110504 (2009).
45. Leverrier, A., Grosshans, F. & Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **81**, 062343 (2010).
46. Furrer, F., Åberg, J. & Renner, R. Min- and max-entropy in infinite dimensions. *Commun. Math. Phys.* **306**, 165–186 (2011).
47. Braunstein, S. L. Squeezing as an irreducible resource. *Phys. Rev. A* **71**, 055801 (2005).
48. Usenko, V. C. & Filip, R. Trusted noise in continuous-variable quantum key distribution: a threat and a defense. *Entropy* **18**, 20 (2016).
49. Lassen, M., Berni, A., Madsen, L. S., Filip, R. & Andersen, U. L. Gaussian error correction of quantum states in a correlated noisy channel. *Phys. Rev. Lett.* **111**, 180502 (2013).
50. Filip, R., Mišta, L. & Marek, P. Elimination of mode coupling in multimode continuous-variable key distribution. *Phys. Rev. A - At. Mol. Opt. Phys.* **71**, 012323 (2005).