Entropy **2015**, *17*, 4654-4663; doi:10.3390/e17074654

OPEN ACCESS
entropy
ISSN 1099-4300
www.mdpi.com/journal/entropy

Article

Continuous Variable Quantum Key Distribution with a Noisy Laser

Christian S. Jacobsen, Tobias Gehring and Ulrik L. Andersen *

Department of Physics, Technical University of Denmark, Fysikvej, 2800 Kongens Lyngby, Denmark; E-Mails: chrsch@fysik.dtu.dk (C.S.J.); tobias.gehring@fysik.dtu.dk (T.G.)

* Author to whom correspondence should be addressed; E-Mail: ulrik.andersen@fysik.dtu.dk.

Received: 12 May 2015 / Accepted: 1 July 2015 / Published: 3 July 2015

Abstract: Existing experimental implementations of continuous-variable quantum key distribution require shot-noise limited operation, achieved with shot-noise limited lasers. However, loosening this requirement on the laser source would allow for cheaper, potentially integrated systems. Here, we implement a theoretically proposed prepare-and-measure continuous-variable protocol and experimentally demonstrate the robustness of it against preparation noise stemming for instance from technical laser noise. Provided that direct reconciliation techniques are used in the post-processing we show that for small distances large amounts of preparation noise can be tolerated in contrast to reverse reconciliation where the key rate quickly drops to zero. Our experiment thereby demonstrates that quantum key distribution with non-shot-noise limited laser diodes might be feasible.

Keywords: quantum key distribution; continuous variables; quantum information

PACS classifications: 03.67.Dd; 03.67.Hk; 03.67.-a

1. Introduction

Secure communication in the post-quantum computer era will be possible using quantum key distribution (QKD) whose security principles are based on the laws of quantum mechanics [1–6]. The QKD systems of today, both proof-of-principle laboratory implementations and commercial systems, require expensive low-noise lasers and detectors. Especially QKD systems using continuous variables (CV) suffer from excess noise which rapidly decreases the secure key rate [7–12].

Prepare-and-measure CV protocols typically employ pure vacuum states randomly displaced in the amplitude and phase quadrature amplitudes of the electro-magnetic field [5]. The receiver either performs homodyne or heterodyne detection [8,11]. Homodyne detection measures a certain quadrature angle depending on the phase of the strong reference beam called the "local oscillator", which has to be switched between two orthogonal settings. In contrast, heterodyne detection measures both orthogonal quadratures simultaneously, thereby eliminating the need of switching at the expense of one extra unit of shot-noise entering the system. The classical post-processing is either based on direct or reverse reconciliation. For direct reconciliation Bob corrects his measurement outcomes to match Alice's preparation, while, as the name already implies, the reverse is true for reverse reconciliation. In the shot-noise limited regime reverse reconciliation allows for larger distances between the two parties since it overcomes the $3\,\mathrm{dB}$ loss limit of direct reconciliation [8,9,13]. Reverse reconciliation was introduced as an alternative to direct reconciliation and as a way to beat the intrinsic loss limit. It was also shown to be more efficient than direct reconciliation even for transmissions above $50\ \%$ in the limit of zero excess noise [14].

Using a shot-noise limited laser, homodyne detection and reverse reconciliation a distance between the two communicating parties of $80\,\mathrm{km}$ has already been achieved [15]. While reaching long distances is of great importance for linking neighbouring cities, bridging short distances potentially allows for secure communication of hand-held devices with terminals. However, for hand-held devices the optical components of a QKD system have to be integrated into a chip whose manufacturing costs have to be low. To enable this, relaxing the stringent requirements on the noise of the laser becomes crucial.

CV QKD using a noisy laser was first suggested in [16,17] using reverse reconciliation, however, it was realized that the preparation noise dramatically reduced the secure key rate, eventually making it impossible to obtain a secure key. To regain security purification of the state was proposed by attenuating the modulated noisy state at Alice's private trusted station. In [18] and [19] it was then suggested that short distance protocols could in fact benefit from using direct reconciliation. Surprisingly it was shown theoretically that the secure key rate for an error reconciliation efficiency of 100% does not decline to zero even for arbitrary amounts of laser noise as long as the excess noise of the channel is lower than the noise of the laser.

Here, we verify this theoretical prediction by using a noisy laser beam which is used for a prepare-and-measure Gaussian modulation protocol with heterodyne detection. For collective attacks in the asymptotic limit we show that preparation noise which in the case of reverse reconciliation yields a vanishing secure key rate, can in fact be tolerated with direct reconciliation. We furthermore experimentally show that for direct reconciliation an optimal amount of preparation noise exists leading to an increased tolerable optical loss in comparison to the case of no preparation noise.

This effect of using preparation noise to obtain greater regions of security in the parameter space can be seen as the direct reconciliation equivalent of the effect reported in [10,20]. As a result of using direct reconciliation, correspondingly shot-noise limited detection is required at the receiver. More generally, the security of QKD in the presence of trusted noise (either at the preparation or detection stage) can be related to the role of quantum discord in quantum cryptography [21].

Finally, we note that Ref. [22] proposes a protocol for two-way continuous-variable quantum key distribution also using displaced thermal states.

2. Theory

Though the performed experiment is an example of a prepare-and-measure protocol, where a modulated quantum state is prepared by Alice and sent to Bob, there is a theoretical equivalence between this protocol and an entanglement based protocol [23–25], where Alice prepares an Einstein-Podolsky-Rosen (EPR) state. In the equivalent scheme she keeps one mode of the EPR state to herself and sends the other mode to Bob. If Alice performs a conditioning measurement using a heterodyne detector, Bob's half of the EPR state will collapse to a coherent state. In that way Alice prepares a coherent state with a displacement depending on her measurement outcome.

If one disregards the problems that follow from finite key sizes [6,26,27], one arrives at a relatively simple bound on the secure key rate

$$R = \beta I(A:B) - \chi(E:X)\,, \tag{1}$$

where β is the reconciliation efficiency [3] and $I(A:B)$ is the classical mutual information between Alice and Bob expressed through the Shannon entropy of the corresponding classical stochastic variables of the measurements [28]. $\chi(E:X)$ is the Holevo quantity [1], expressed through the von Neumann entropy of the quantum state the eavesdropper shares with the honest parties. For reverse reconciliation $\chi(E:B) = S(\hat{E}) - S(\hat{E}|B)$, and for direct reconciliation $\chi(E:A) = S(\hat{E}) - S(\hat{E}|A)$ [5]. $S(\hat{X})$ is the von Neumann entropy of the quantum state ρ_X. For Gaussian states any ρ_X has a corresponding covariance matrix Γ_X, and a mean value $\langle \boldsymbol{X} \rangle$, though mean values can always be displaced out without loss of generality, as they do not contribute to the information content of the state in question. The von Neumann entropy for a Gaussian state ρ_X can be shown to be given by [5]

$$S(\hat{X}) = \sum_i g(\nu_i), \tag{2}$$

where

$$g(x) = \frac{x+1}{2}\log_2\left(\frac{x+1}{2}\right) - \frac{x-1}{2}\log_2\left(\frac{x-1}{2}\right), \tag{3}$$

and ν_i is the i'th value in the symplectic spectrum of Γ_X. The symplectic spectrum is calculated by finding the absolute eigenvalues of the matrix $i\Omega\Gamma_X$, where

$$\boldsymbol{\Omega} = \bigoplus_{k=1}^{N} \boldsymbol{\omega} \qquad , \qquad \boldsymbol{\omega} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \tag{4}$$

with N being the number of modes described by the state ρ_X. The dimension of Γ_X is $2N \times 2N$.

An attack on a continuous-variable quantum channel between Alice and Bob is usually represented by a beam splitter, controlled by the eavesdropper Eve, who is injecting one part of an EPR state into the vacant port. Eve keeps the other mode of the EPR state in a quantum memory and interferes the first mode with all the coherent states sent by Alice. Then she does a collective measurement on the memory after all quantum states have been exchanged between Alice and Bob. This collective attack is called an "entangling-cloner attack" [5,9,18,29,30] and represents the most important and realistic type of collective Gaussian attack, whose general form is discussed in [31].

A schematic of the entanglement based equivalent model is shown in Figure 1. Alice produces a noisy EPR state

$$\mathbf{\Gamma}_{\text{in}} = \begin{bmatrix} \mu \boldsymbol{I} & \sqrt{\mu^2 - 1}\boldsymbol{Z} \\ \sqrt{\mu^2 - 1}\boldsymbol{Z} & (\mu + \kappa)\boldsymbol{I} \end{bmatrix}, \tag{5}$$

with variance μ in the mode she keeps (upper left block) and $\mu + \kappa$ in the mode she sends to Bob (lower right block). κ represents the extra variance that comes from the preparation noise and

$$\boldsymbol{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad , \quad \boldsymbol{Z} = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{6}$$

Thereafter the mode sent to Bob is propagated through a beam splitter with transmittance T where Eve interferes it with one mode of her EPR state. The transmitted mode is measured by Bob, while the reflected mode is measured by Eve. We follow the work of [19] where it was shown that for heterodyne detection the mutual information is given by the expression

$$I(A:B) = \log_2 \left(\frac{(1-T)W + TV_S + TV_0 + 1}{(1-T)W + TV_0 + 1} \right), \tag{7}$$

where V_S is the variance of the Gaussian distribution used for the signal modulation, V_0 is the noise carried by the light and W is the variance of Eve's EPR mode. The entanglement based protocol is related to the prepare-and-measure scheme such that $\mu = V_S + 1$. This noise can be separated into technical and intrinsic (quantum) noise, such that $V_0 = 1 + \kappa$, in units of the shot noise. For a protocol assuming shot-noise limited state generation $\kappa = 0$.

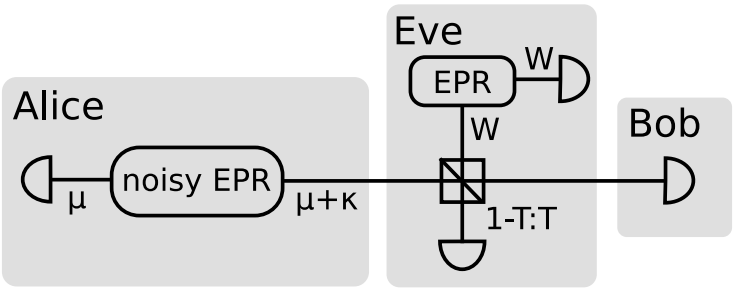

Figure 1. Equivalent entanglement based model used in the security proof. Alice produces a noisy Einstein–Podolsky–Rosen (EPR) state which she sends to Bob. The quantum channel with transmission T is controlled by the eavesdropper who injects an EPR state with variance W.

The symplectic spectrum of Eve's EPR state after it has been interfered with the signal mode is $\nu_{E\pm} = \frac{1}{2}(\sqrt{(e_V + W)^2 - 4T(W^2 - 1)} \pm (e_V - W))$, where $e_V = (1-T)V + TW$. Similar expressions are derived in [19] for the symplectic spectra of the conditional states. From these expressions of the eigenvalues one can find the Holevo information for direct and reverse reconciliation

$$\chi(E:X) = g(\nu_{E+}) + g(\nu_{E-}) - g(\nu_{E|X+}) - g(\nu_{E|X-}), \tag{8}$$

where X corresponds to either conditioning on Alice or Bob depending on whether direct or reverse reconciliation is used. The secret key rate is then easily found by combining Equations (1), (7) and (8).

The regions of positive key rate in terms of transmission and preparation noise are shown in Figure 2 for both reverse and direct reconciliation. Here one clearly sees that large preparation noise is highly detrimental to reverse reconciliation, but not to direct reconciliation which is much more robust. In fact for direct reconciliation a preparation noise of $1+\kappa \approx 3$ is beneficial since it lowers the possible channel transmission value to about $77\,\%$ in comparison to $79\,\%$ for no preparation noise. In the ideal case of $\beta = 1$ the secure region even keeps increasing with increasing preparation noise. This behaviour is displayed in the figure by the dashed line calculated in the limit of high modulation variance with ideal reconciliation and no channel excess noise. This case was thoroughly investigated in [19].

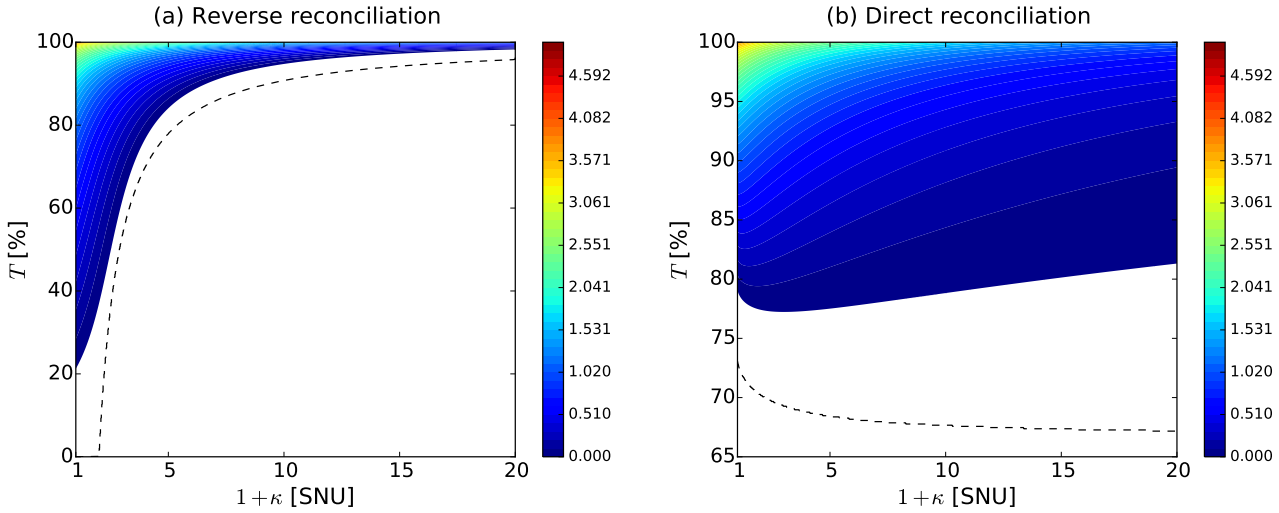

Figure 2. Contour plots of the secure key generation rate for varying preparation noise in shot-noise units (SNUs) and transmission T for (**a**) reverse reconciliation and (**b**) direct reconciliation. The error reconciliation efficiency was set to $\beta = 95\%$, the modulation variance was 32 SNUs and the channel excess noise 0.11. The dashed lines indicate the minimal possible transmission of a channel where a positive secret key rate can still be obtained, in the ideal case for $\beta = 1$, no channel excess noise and in the limit of high modulation variance. (a) For no preparation noise ($\kappa = 0$), the rate decreases asymptotically to zero as the transmission approaches zero. When the preparation noise increases the security of reverse reconciliation is quickly compromised, to the point where almost unity transmission is required to achieve security. (b) For heterodyne detection and no preparation noise the rate goes to zero at about 79% transmission, due to the extra unit of vacuum introduced by heterodyne detection. The plot shows the robustness of direct reconciliation to preparation noise.

3. Experiment

The experimental setup is shown in Figure 3. A shot-noise limited continuous-wave laser at $1064\,\text{nm}$ was used in conjunction with two electro-optical modulators and two white noise generators to simulate various degrees of preparation noise. Since the laser was shot-noise limited a simplified heterodyne detection was performed where the signal beam is interfered with a local oscillator and locked such that

the subtraction of the two photo detector signals represents the phase quadrature. At the same time, the photo detector signals were added to measure the amplitude quadrature. Note that typically such a detection approach would not eliminate any technical noise present in the noisy laser beam. In a setting where the local oscillator for heterodyne detection is also derived from the noisy laser, two separate homodyne detectors measuring orthogonal quadratures have to be employed. That way the common mode rejection ratio of the homodyne detector would provide a shot-noise limited measurement. The quantum efficiency of the photo diodes was about $90\,\%$ and the visibility at the balanced beam splitter about $93\,\%$. The optical power in the two beams was $2.8\,\mathrm{mW}$ each.

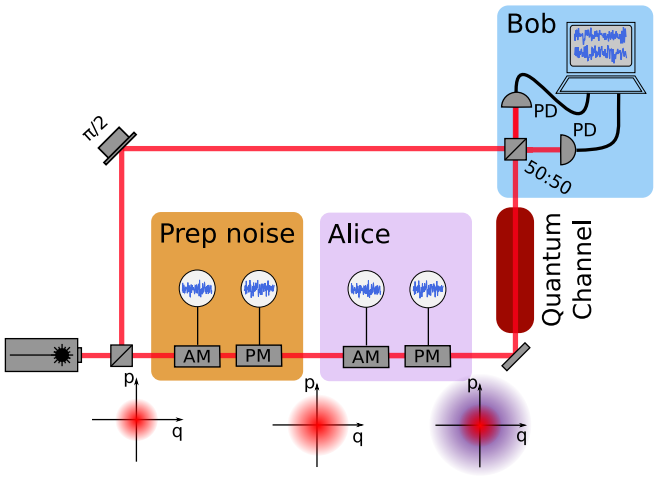

Figure 3. Schematic representation of the experiment. A shot-noise limited laser is amplitude- and phase-modulated with two independent white-noise sources to simulate a noisy laser. Subsequently, Alice modulates the noisy laser beam in amplitude and phase using a known modulation and sends it to Bob through the quantum channel who performs heterodyne detection. The quantum channel's transmission was simulated by an (for coherent states) equivalent reduction of the modulation variances. AM: Amplitude Modulation. PM: Phase Modulation. PD: Photo Detector.

The signal modulations were delivered by two white noise generators, whose outputs were sent both to the modulators and to the data acquisition. The acquired data from Alice's modulations and from Bob's amplitude and phase quadrature measurements represent the raw key. To determine the secure key rate using Equation (1) the mutual information between Alice's and Bob's data were calculated and the transmission as well as the excess noise of the channel was estimated from the data. Transmission was estimated from a calibration measurement where the states experienced only the intrinsic loss of the setup. This defines unity transmission, which is possible because of the scaling of coherent states under losses. Transmission values were calculated by relating the measured variances to this calibration measurement. Excess noise was determined by a suitable minimization of the subtraction of the performed modulation and the measurement outcomes. The remaining variance above shot-noise was ascribed to excess noise.

Figure 4 shows the experimentally obtained secret key rate for both reverse reconciliation and direct reconciliation for various levels of preparation noise κ. The modulation variance at Alice's station was set to about 32 shot-noise units (SNU). The channel excess noise parameter W was determined to 1.11

SNUs. To keep the shot-noise to electronic-noise clearance for all measurements constant and because the optical power in the two beams had to be the same to perform heterodyne detection, we simulated optical loss between Alice's and Bob's station. The simulation was achieved by scaling the levels of the preparation noise and the signal modulations appropriately which is equivalent to transmission loss for coherent states.

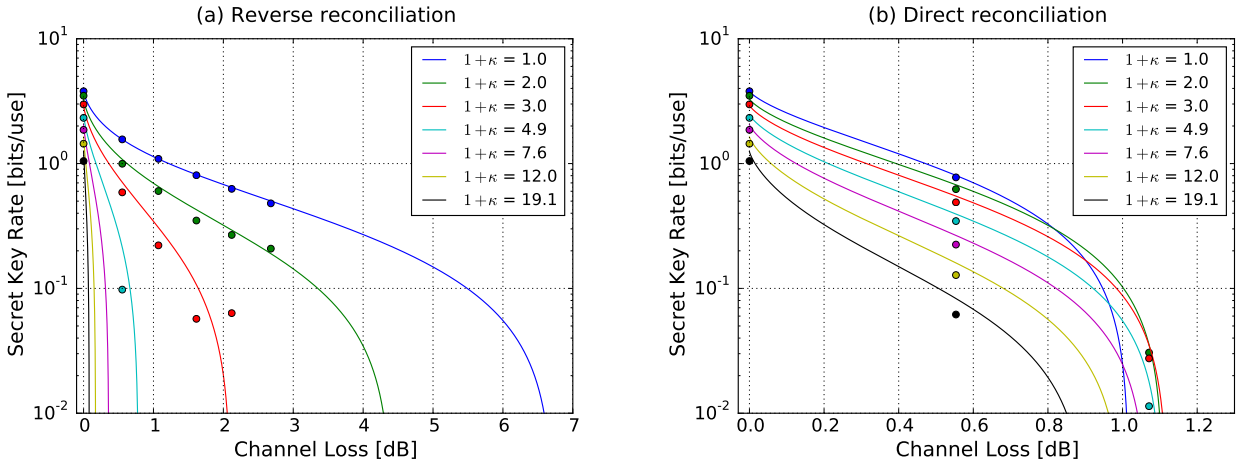

Figure 4. Measured data and theory curves for different levels of preparation noise using (**a**) reverse reconciliation and (**b**) direct reconciliation in the post-processing. Error reconciliation efficiency $\beta = 95\,\%$. Due to our simulation of losses (see main text) the error bars on the channel loss are negligibly small and, thus, not shown in the figure.

From Figure 4a, which shows the achieved secure key rate for reverse reconciliation, it is clearly visible that with increasing preparation noise not only does the secret key rate become smaller, so does the possible channel loss. Especially for very high preparation noise the tolerable channel loss becomes very small. For the highest investigated preparation noise value of $1 + \kappa \approx 19$ a channel loss of merely about $0.06\,\mathrm{dB}$ is possible. This is in contrast to direct reconciliation, shown in Figure 4b, where for this value of preparation noise about $0.85\,\mathrm{dB}$ channel loss can be reached. While the strength of the direct reconciliation protocol lies in this region of high preparation noise, the theoretical behaviour seen in Figure 2 of preparation noise enhanced tolerable channel loss is also resembled in the measurement. For a preparation noise of $1 + \kappa \approx 3$ the channel loss can be as large as $1.1\,\mathrm{dB}$ in comparison to about $1\,\mathrm{dB}$ without preparation noise. This behaviour is, however, of purely theoretical interest since for these moderate values of preparation noise, reverse reconciliation still offers larger distances.

4. Conclusions

In conclusion, we have provided an experimental demonstrator for CV QKD with a noisy laser source. Using direct reconciliation we have shown that preparation noise of about 19 SNUs can easily be tolerated, even though secret key rate and possible channel transmission become lower. Theoretical calculations show that in fact the preparation noise can be arbitrarily high and still it should be possible to extract a secret key [19].

While in our experiment we simulated the effect of preparation noise in a controlled fashion, implementing the protocol with a noisy diode laser instead will demonstrate the protocol's ability to provide secret keys over short distances despite the noise of the source.

Acknowledgments

This research was supported by the Danish Council for Independent Research, Technology and Production Sciences (Sapere Aude program). T.G. acknowledges support from the H.C. Ørsted postdoctoral programme.

Author Contributions

All authors conceived the experiment. Christian S. Jacobsen implemented the setup under supervision of Tobias Gehring and Ulrik L. Andersen. Christian S. Jacobsen and Tobias Gehring performed the experiment, Christian S. Jacobsen analysed the experimental data. Christian S. Jacobsen and Tobias Gehring wrote the manuscript with contributions from Ulrik L. Andersen. All authors have read and approved the final manuscript.

Conflicts of Interest

The authors declare no conflict of interest.

References

1. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2000.
2. Braunstein, S.L.; van Loock, P. Quantum information with continuous variables. *Rev. Mod. Phys.* **2005**, *77*, 513–577.
3. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350.
4. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195.
5. Weedbrook, C.; Pirandola, S.; García-Patrón, R.; Cerf, N.J.; Ralph, T.C.; Shapiro, J.H.; Lloyd, S. Gaussian quantum information. *Rev. Mod. Phys.* **2012**, *84*, 621–669.
6. Renner, R.; Gisin, N.; Kraus, B. Information-theoretic security proof for quantum-key-distribution protocols. *Phys. Rev. A* **2005**, *72*, 012332.
7. Cerf, N.J.; Levy, M.; van Assche, G. Quantum Distribution of Gaussian Keys with Squeezed States. *Phys. Rev. A* **2001**, *63*, 052311.
8. Grosshans, F.; Grangier, P. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.* **2002**, *88*, 057902.
9. Grosshans, F.; van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238–241.

10. García-Patrón, R.; Cerf, N.J. Continuous-variable quantum key distribution protocols over noisy channels. *Phys. Rev. Lett.* **2009**, *102*, 130501.
11. Lance, A.M.; Symul, T.; Bowen, W.P.; Sanders, B.C.; Tyc, T.; Ralph, T.C.; Lam, P.K. Continuous-variable quantum-state sharing via quantum disentanglement. *Phys. Rev. A* **2005**, *71*, 033814.
12. Madsen, L.S.; Usenko, V.C.; Lassen, M.; Filip, R.; Andersen, U.L. Continuous variable quantum key distribution with modulated entangled states. *Nature Commun.* **2012**, *3*, doi:10.1038/ncomms2097.
13. Silberhorn, C.; Ralph, T.C.; Lütkenhaus, N.; Leuchs, G. Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit. *Phys. Rev. Lett.* **2002**, *89*, 167901.
14. Grosshans, F.; Grangier, P. Reverse Reconciliation Protocols for Quantum Cryptography with Continuous Variables. In Proceedings of the Sixth International Conference on Quantum Communication, Measurement and Computing, Cambridge, MA, USA, 22–26 July 2002; pp. 351–356.
15. Jouguet, P.; Kunz-Jacques, S.; Leverrier, A.; Grangier, P.; Diamanti, E. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photon.* **2013**, *7*, 378–381.
16. Filip, R. Continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **2008**, *77*, 022310.
17. Usenko, V.C.; Filip, R. Feasibility of continuous-variable quantum key distribution with noisy coherent states. *Phys. Rev. A* **2010**, *81*, 022318.
18. Weedbrook, C.; Pirandola, S.; Lloyd, S.; Ralph, T.C. Quantum cryptography approaching the classical limit. *Phys. Rev. Lett.* **2010**, *105*, 110501.
19. Weedbrook, C.; Pirandola, S.; Ralph, T. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A* **2012**, *86*, 022318.
20. Pirandola, S.; García-Patrón, R.; Braunstein, S.L.; Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.* **2009**, *102*, 050503.
21. Pirandola, S. Quantum discord as a resource for quantum cryptography. *Sci. Rep.* **2014**, *4*, doi:10.1038/srep06956.
22. Weedbrook, C.; Ottaviani, C.; Pirandola, S. Two-way quantum cryptography at different wavelengths. *Phys. Rev. A* **2014**, *89*, 012309.
23. Ralph, T.C. Security of continuous-variable quantum cryptography. *Phys. Rev. A* **2000**, *62*, 062306.
24. Reid, M.D. Quantum cryptography with a predetermined key, using continuous-variable Einstein–Podolsky–Rosen correlations. *Phys. Rev. A* **2000**, *62*, 062308.
25. Hillery, M. Quantum cryptography with squeezed states. *Phys. Rev. A* **2000**, *61*, 022309.
26. König, R.; Renner, R.; Bariska, A.; Maurer, U. Small accessible quantum information does not imply security. *Phys. Rev. Lett.* **2007**, *98*, 140502.
27. Leverrier, A.; Grosshans, F.; Grangier, P. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A* **2010**, *81*, 062343.
28. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*, 2nd ed.; Wiley: Hoboken, NJ, USA, 2006.

29. García-Patrón, R.; Cerf, N.J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.* **2006**, *97*, 190503.
30. Navascués, M.; Grosshans, F.; Acín, A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. *Phys. Rev. Lett.* **2006**, *97*, 190502.
31. Pirandola, S.; Braunstein, S.L.; Lloyd, S. Characterization of collective Gaussian attacks and security of coherent-state quantum cryptography. *Phys. Rev. Lett.* **2008**, *101*, 200504.