Towards quantum key distribution with noisy communication sources

A Walton$^{1,3}$, A Ghesquière$^1$, D Jennings$^{1,2}$ and B Varcoe$^1$

1 School of Physics and Astronomy, University of Leeds, Leeds, LS2 9JT, United Kingdom
2 Department of Physics, Imperial College London, London, SW7 2AZ, United Kingdom
3 Email: pyaw@leeds.ac.uk

Abstract. A beam emitted by a displaced thermal source, incident on a beam splitter, is used as the source in a central broadcast quantum key distribution protocol. These displaced thermal states have parallels to signals produced through phase-shift keying, already commonly used in a variety of microwave-based communications equipment. Here, we analyse a thermal state quantum key distribution protocol for which there is no dependency on displacement. Our analysis suggests the ability to carry out QKD using widely available broadcasting equipment. We also consider the effects of the introduction of loss at several points in the protocol, and find that, while increasing loss in Alice’s channel eventually results in advantage distillation being required, security is still maintained.

Keywords: Thermal State, Displacement, Quantum Computing, Quantum Key Distribution, QKD, Correlation, Continuous Variables
1. Introduction

Quantum Key Distribution (QKD) is the process by which multiple parties, here two, referred to as Alice and Bob, attempt to establish secure communication over insecure channels through applications of the principles of quantum mechanics [1]. For symmetric-key cryptography, this is accomplished by having Alice and Bob share a cryptographic key which can be used to encrypt and decrypt messages. Meanwhile Eve, who is eavesdropping on the channel, does not know the key. Here, the difficulty lies in initially sharing a secret key between Alice and Bob while Eve is eavesdropping.

A large section of work in QKD explores the use of coherent sources [2] [3] to produce a key, such as in the Gaussian Modulated Coherent State protocol [4]. An advantage to this being that coherent states are accessible through lasers. However, here we will focus on the use of thermal states [5, 6, 7] which are commonly used in modern wireless communication.

Previous work involving thermal states in a central broadcast QKD protocol [8] showed the ability to generate a key using a beam splitter to direct a signal from an unmodulated thermal source to Alice and Bob. While interesting, communications equipment do not typically broadcast signals without some form of modulation, limiting the applicability of the previous theory in current devices.

Signal modulation is ubiquitous in communications equipment. Specifically we call attention to Phase-Shift Keying (PSK), transmitting data through modulation of the phase of a signal to one of a finite number of values, different variations of which see widespread use in areas such as Wifi, Bluetooth, satellite and mobile communication. Compared to the previous paper [8], which concerned a single thermal state centred at the origin in phase space, this is instead equivalent to a series of displaced thermal states equally spaced around a circle centred at the origin. An example of one form of PSK, quadrature phase-shift keying, is shown in Figure 1.

Given that current microwave-based devices already broadcast displaced thermal states, it is then of interest to test if treatment of the thermal state protocol can be extended to allow for the use of displaced thermal sources, as success would suggest that QKD can be performed using widely available wireless equipment.

In this paper, Section 2 introduces thermal states and the displacement operator, then the protocol is described in Section 3. This is followed by descriptions of the mathematical modelling and results in Section 4. Finally, the effects of the addition of loss at various points on the key rate is analysed in Section 5.
Towards quantum key distribution with noisy communication sources

2. Thermal states and displacement

If the creation and annihilation operators are given by $\hat{a}^\dagger$ and $\hat{a}$ respectively, the displacement operator is defined as $\hat{D}(\alpha) = \exp(\alpha \hat{a}^\dagger - \alpha^* \hat{a})$, where $\alpha \in \mathbb{C}$ is the displacement parameter. The displacement operator can be applied to $\hat{a}^\dagger$, $\hat{a}$ and a thermal state $\rho_{Th}$ as shown in equations (1) and (2) with equation (2) describing a displaced thermal state, shown in Figure 2. In phase space, the displacement operator has the effect of translating a distribution by $(|\alpha| \cos(\theta), |\alpha| \sin(\theta))^T$, where $\alpha = |\alpha|e^{i\theta}$.

$$\hat{D}(\alpha) \hat{a}^\dagger \hat{D}^\dagger(\alpha) = \hat{a}^\dagger - \alpha^*$$  \hspace{1cm} (1)

$$\rho_{DTh}(\alpha) = \hat{D}(\alpha) \rho_{Th} \hat{D}^\dagger(\alpha).$$  \hspace{1cm} (2)

Here, the thermal state distribution is given in the Fock basis as $\rho_{Th} = \sum_{n=0}^{\infty} p_n |n\rangle \langle n|$, with $p_n = \frac{\exp(-n\beta \omega)}{1-\exp(-\beta \omega)}$, where $\beta$ is the thermodynamic beta. Unlike a coherent source [5], it is known that a beam from a thermal source, when incident on a beamsplitter, produces a pair of output beams which have correlated intensity measurements when the output modes are compared. [10, 11]. This is due to the bunched nature of photons in thermal light causing high variance in measurements of intensity. We aim to use these correlations to produce a secure key. This will be done by using a series of beamsplitters to direct a beam from a displaced thermal source to Alice, Bob and Eve. They will each perform quadrature measurements on a received beam, which will yield correlated results due to the Hanbury Brown and Twiss effect [10].

The protocol we will analyse is similar to others which use modulated coherent states [12, 13, 14, 15]. In these Gaussian Modulated Coherent State (GMCS) protocols, pairs of values, $x_i, y_i$ are repeatedly drawn at random from a Gaussian distribution and
used by Alice to produce displaced coherent states with displacement vector \((x_i, y_i)\). These are sent to Bob for measurement, with Eve able to access the channel between Alice and Bob for interception.

From Bob and Eve’s perspective, these random coherent states are indistinguishable from the output of a thermal source. Therefore, an equivalent protocol involves instead splitting the output of a thermal source, with outputs directed to Alice and Bob. The use of an actual thermal source in this protocol allows for implementation on devices which already utilise such sources.

**Figure 2. Displacing a state.** Visualisation of displacing a thermal state in phase space, represented by the transformation \(\rho_{DTh}(\alpha) = \hat{D}(\alpha) \rho_{Th} \hat{D}^\dagger(\alpha)\), with \(\alpha = |\alpha| e^{i\theta} \in \mathbb{C}\). The distribution is translated by \((|\alpha| \cos(\theta), |\alpha| \sin(\theta))^T\).

### 3. Protocol

**Figure 3. The thermal state protocol.** A beam produced by a thermal source is incident on a 50:50 beamsplitter. One output is sent to Alice, with the other being sent to Bob. The beam sent towards Bob is not under Alice’s control, and this insecure channel is the point in which Eve will perform the interception. This diagram was originally used in "Thermal state quantum key distribution" [8], and is licensed under CC-BY 4.0 [16].
Building on prior work [5, 8], we use a central broadcast protocol in which a beam emitted from a thermal source is incident on a 50:50 beamsplitter, the outputs of which are sent to the two parties, Alice and Bob. The eavesdropper, Eve will perform the interception using an entangling cloner attack, inserting a beamsplitter of transmittance $T$ in the channel between the initial beamsplitter and Bob. Previously [8], a reduction in conditional mutual information, and therefore the key rate was observed as the reflectance of Eve’s intercepting beam splitter increased. However, the produced bit strings were consistently suitable for key distillation provided the transmittance did not drop to 0% in a noiseless scenario.

We assume that Alice is in control of the source and their own measurement apparatus, along with the channels in between them, as shown in Figure 3. Bob is also in control of their own measurement apparatus, but the channel leading there from the initial beamsplitter is insecure. Each person will split their received beam into a pair of outputs with a 50:50 beamsplitter, then they perform a series of pairs of measurements, $\{x_i, p_i\}$ on the X quadrature of one beam, and the P quadrature of their second beam. Here, the X and P quadratures are defined as:

$$\hat{X}(\theta) = \frac{1}{2} (\hat{a}^\dagger e^{i\theta} + \hat{a} e^{i\theta}) ,$$

$$\hat{P}(\theta) = \frac{i}{2} (\hat{a}^\dagger e^{i\theta} - \hat{a} e^{i\theta}) ,$$

where these quadratures are measured through heterodyne detection, by mixing the beams to be measured with a beam from a coherent source at a beamsplitter and measuring the output intensities. This is done as an alternative method to measuring in random bases, and has been successfully employed in other QKD protocols [15].

For each pair of measurements, each person calculates $z_i = \sqrt{x_i^2 + p_i^2}$ to find a string of $z_i$ values. The median of these $z_i$ values are found for each person, and a value of 0 or 1 is assigned to each measurement depending on if the $z_i$ value is above or below that person’s median. This produces a bit string for each person which may be used for key distribution.

Unlike in the previous paper [8], the thermal source will be displaced to set positions in order to measure the effects of displacement on the key rate bounds. These displaced states would appear in practical implementations of the protocol, in the same way that modulated signals are used in modern microwave communication.

We do not employ random displacement [17] in a prepare-and-measure scheme, instead using a single thermal source displaced by a constant amount. As amplitude measurements are used to produce bit strings in this protocol, results from this single state is easily expanded to multiple thermal states separated by phase differences, in the manner shown in Figure 1.

The results of QKD with random displacement of thermal states in a prepare-and-measure protocol [17] showed a small region of secure key generation in the microwave region when transmittance to Bob was very high ($> 98\%$). By replacing this with a
Towards quantum key distribution with noisy communication sources

central broadcast setup, we allow for much lower transmittance, here we perform the protocol with a transmittance of 50% to Bob.

Previous simulations of this protocol with thermal states centred at the origin in phase space showed that, in the absence of noise and loss, the lower bound on the key rate was greater than zero provided the beamsplitter used for Eve’s interception had nonzero transmittance [8]. This was supported by covariance matrix calculations employed to calculate von Neumann mutual information. Here, we will perform similar calculations for a state with nonzero displacement.

4. System modelling

As mentioned in Section 2, from Bob and Eve’s perspective the outputs of a thermal source are equivalent to those from the sources in Gaussian Modulated Coherent State protocols. This allows the application of existing security proofs for GMCS QKD to the thermal state protocol. These include tests of composable security in the case of collective attacks [18, 19, 20] and finite key effects [20, 21].

4.1. Covariance

The covariance matrix of the system can be used to calculate entropy, and therefore the bounds on the key rate. In this protocol, we can completely describe the state of the system through the first and second moments as there are only Gaussian modes involved. For an N-mode system, the covariance matrix is defined as [22]:

$$\gamma_{ij} = \text{Tr} \left[ \frac{1}{2} \{ (\hat{r}_i - d_i), (\hat{r}_j - d_j) \} \right],$$

$$d_i = \langle \hat{r}_i \rangle,$$

$$r = \left( \hat{X}_1, \hat{P}_1, ..., \hat{X}_N, \hat{P}_N \right).$$

Here, \(\hat{X}_i\), and \(\hat{P}_i\) are the pair of quadrature operators for mode \(i\) of the system and \(\{a, b\} = ab + ba\) is the anticommutator. When considering only the two modes incident on the initial beamsplitter, the input for a displaced thermal source is given by:

$$d_1 = \begin{bmatrix} d_x \\ d_p \\ v_{1x} \\ v_{1p} \end{bmatrix},$$

where \(d_x\) and \(d_p\) describe the quadratures of the source beam. Vacuum noise added in the second input is described by \(v_{1x}\) and \(v_{1p}\). The beamsplitters shown in the protocol are applied in succession to the relevant modes through the use of the beamsplitter transformation \(S (T, R)\):

$$S (T, R) = \begin{bmatrix} T & R \\ -R & T \end{bmatrix} \otimes I.$$
Towards quantum key distribution with noisy communication sources

Here, \( T \) and \( R \) are the transmittance and reflectance of the beamsplitter, defined such that \( T^2 + R^2 = 1 \). With the exception of Eve’s beamsplitter, which has unknown transmittance, each of the beamsplitters used in this protocol will be 50:50, with \( T^2 = R^2 = \frac{1}{2} \). We can find the final output vector and covariance matrix of the system. Considering only the X-quadratures, we can find half of the output vector:

\[
\begin{align*}
\mathbf{r}_x &= \begin{bmatrix}
\frac{t_a}{2} (d_x + v_{1x}) + \frac{t_a}{\sqrt{2}} v_{2x} + r_av_{A_1} \\
-\frac{t_a}{2} (d_x + v_{1x}) + \frac{t_a}{\sqrt{2}} v_{2x} + r_av_{A_2} \\
-\frac{T t_b}{2} (d_x - v_{1x}) + \frac{R t_b}{\sqrt{2}} v_{3x} + \frac{t_b}{\sqrt{2}} v_{4x} + r_bv_{B_1} \\
\frac{t_b}{2} (d_x - v_{1x}) + \frac{t_b}{\sqrt{2}} v_{3x} + \frac{R t_b}{\sqrt{2}} v_{5x} + r_e v_{E_1} \\
-\frac{t_e}{2} (d_x - v_{1x}) - \frac{T t_e}{\sqrt{2}} v_{3x} + \frac{t_e}{\sqrt{2}} v_{5x} + r_e v_{E_2}
\end{bmatrix}.
\end{align*}
\]

The P-quadrature results, \( \mathbf{r}_p \), follow the same pattern, giving a final output vector of \( \mathbf{r} = [r_{x1}, r_{p1}, r_{x2}, r_{p2}, \ldots, r_{x6}, r_{p6}]^T \). Eve performs the interception using a beamsplitter with transmittance \( T \) and reflectance \( R \). Here, \( v_{1-5} \) describe vacuum noise added by the beamsplitters in the order labelled in Figure 4.

Detector efficiency is modelled using an additional beamsplitter at each of the six detectors, with added vacuum noises \( v_{A_1}, v_{A_2}, v_{B_1}, v_{B_2}, v_{E_1}, \) and \( v_{E_2} \). The beamsplitters modelling Alice’s pair of detectors are both assumed to have transmittance \( t_a \) and reflectance \( r_a \), allowing loss to be introduced during detection. To model detection loss at Bob and Eve’s pairs of detectors, \( t_b, r_b, t_e, \) and \( r_e \) are similarly defined.

\[
\begin{align*}
\gamma_{A_1A_2 B_1B_2 E_1E_2} &= \begin{bmatrix}
\gamma_{A_1 A_2} & C_{AB} & C_{AE} \\
C_{AB}^T & \gamma_{B_1 B_2} & C_{BE} \\
C_{AE}^T & C_{BE}^T & \gamma_{E_1 E_2}
\end{bmatrix},
\end{align*}
\]

We can calculate the covariance matrix using the final vector. We set \( v = \text{Var}(d_x) = \text{Var}(d_p) \) to be the variance of the initial state, and take the added noise to have mean zero and variance one. This yields:

\[
\begin{align*}
\gamma_{A_1A_2 B_1B_2 E_1E_2} &= \begin{bmatrix}
\gamma_{A_1 A_2} & C_{AB} & C_{AE} \\
C_{AB}^T & \gamma_{B_1 B_2} & C_{BE} \\
C_{AE}^T & C_{BE}^T & \gamma_{E_1 E_2}
\end{bmatrix},
\end{align*}
\]
Towards quantum key distribution with noisy communication sources

Where the sub-matrices are given by:

\[
\gamma_{A_1A_2} = \begin{bmatrix}
\frac{t_a^2}{4} (v + 3) + r_a^2 & \frac{t_a^2}{4} (1 - v) \\
\frac{t_a^2}{4} (1 - v) & \frac{t_a^2}{4} (v + 3) + r_a^2
\end{bmatrix} \otimes I
\] (12)

\[
\gamma_{B_1B_2} = \begin{bmatrix}
\frac{t_b^2}{4} (v + 1) + \frac{t_b^2}{2} (r^2 + 1) + r_b^2 & -\frac{t_b^2}{4} (v + 1) + \frac{t_b^2}{2} (1 - R^2) \\
-\frac{t_b^2}{4} (v + 1) + \frac{t_b^2}{2} (1 - R^2) & \frac{t_b^2}{4} (v + 1) - \frac{t_b^2}{2} (R^2 + 1) + r_b^2
\end{bmatrix} \otimes I
\] (13)

\[
\gamma_{E_1E_2} = \begin{bmatrix}
\frac{t_e^2 R^2}{4} (v + 1) + \frac{t_e^2 (T^2 + 1)}{2} + r_e^2 & -\frac{R^2 t_e^2}{4} (v + 1) + \frac{t_e^2 (1 - T^2)}{2} \\
-\frac{R^2 t_e^2}{4} (v + 1) + \frac{t_e^2 (1 - T^2)}{2} & \frac{t_e^2 R^2}{4} (v + 1) - \frac{t_e^2 (T^2 + 1)}{2} + r_e^2
\end{bmatrix} \otimes I
\] (14)

\[
C_{AB} = \begin{bmatrix}
\frac{T_{a_1b_1}}{4} (1 - v) & \frac{T_{a_1b_1}}{4} (v - 1) \\
\frac{T_{a_1b_1}}{4} (v - 1) & \frac{T_{a_1b_1}}{4} (1 - v)
\end{bmatrix}
\] (15)

\[
C_{AE} = \begin{bmatrix}
\frac{R_{a_1e_1}}{4} (v - 1) & \frac{R_{a_1e_1}}{4} (1 - v) \\
\frac{R_{a_1e_1}}{4} (1 - v) & \frac{R_{a_1e_1}}{4} (v - 1)
\end{bmatrix}
\] (16)

\[
C_{BE} = \begin{bmatrix}
\frac{T_{R_{b_1e_1}}}{4} (1 - v) & \frac{T_{R_{b_1e_1}}}{4} (v - 1) \\
\frac{T_{R_{b_1e_1}}}{4} (v - 1) & \frac{T_{R_{b_1e_1}}}{4} (1 - v)
\end{bmatrix}
\] (17)

This describes the covariances of the modes received by Alice, Bob, then Eve’s pairs of detectors.

### 4.2. Final State Entropy

Using the covariance matrix, we can calculate von Neumann joint entropy between pairs of modes, which can be used to place bounds on the key rate in the case of a collective attack by Eve. Here, Eve stores their received states in memory, and performs measurements after all classical communication concerning privacy amplification between Alice and Bob has ended. The von Neumann entropy of a state \( \rho \) is given by [22]:

\[
S(\rho) = \sum_i G \left( \frac{\lambda_i - 1}{2} \right),
\] (18)

\[
G(x) = (x + 1) \log_2 (x + 1) - x \log_2 x,
\] (19)

where \( \lambda_i \) denotes the symplectic eigenvalues of the final state of the system. Here, \( \lambda^2 = |\gamma_1| \) for a one mode system, while for two modes we can calculate:

\[
(\lambda_{1,2})^2 = \frac{1}{2} \left( \Delta \pm [\Delta^2 - 4|\gamma_{12}|^{\frac{1}{2}}] \right),
\] (20)

\[
\Delta = |\gamma_1| + |\gamma_2| - 2|C|.
\] (21)
Towards quantum key distribution with noisy communication sources

By defining the mutual information between two modes as $I(A; B) = S(A) + S(B) - S(AB)$, and the conditional mutual information as $I(A; B|E) = S(AE) + S(BE) - S(ABE) - S(E)$ we can place limits on the key rate, $K(A; B|E)$ \[23\].

$$K(A; B|E) \geq \max [I(A; B) - I(A; E), I(A; B) - I(B; E)],$$

(22)

$$K(A; B|E) \leq \min [I(A; B), I(A; B|E)],$$

(23)

From equations \[18\]-\[21\] as well as the covariance matrix shown in equation \[14\] we find that displacement does not have any effect on the key rate bounds. Dependency on $d_x$ and $d_p$ disappears in the final matrix, leaving only dependency on the thermal state variance. Therefore, calculating mutual information values using elements of the covariance matrix will produce limits which are also not dependent on displacement. From this we can see that the protocol can be carried out without requiring a source with zero displacement. Having shown that the protocol functions in a no-loss scenario with displaced thermal states, we can consider cases where loss is present.

5. Loss

We now analyse the effects of loss in the system, with Eve performing interception using a 50:50 beamsplitter. Here, we choose to model loss through the use of beam splitters at the detectors. This allows us to apply loss to Alice’s beam before measurement can occur, as well as on Bob’s beam before or after Eve performs interception. We consider the value $K = I(A; B) - I(B; E)$, a lower bound on the key rate, due to $K$ being a positive function when testing without loss, with $K > 0$ being a requirement \[24\] for QKD to take place via reverse reconciliation. This is calculated using equation \[18\]. Also considered in the conditional mutual information, as secrecy can be ensured through advantage distillation provided conditional mutual information is positive \[25\]. The results of these calculations for the three scenarios are displayed in Figures \[3\]-\[7\]. When loss is introduced into Alice’s channel, Alice and Bob will eventually no longer have the superior channel, with $K = 0$ occurring at approximately 50% loss. However when loss is introduced into Bob’s channel, either before or after Eve performs interception, $K = I(A; B) - I(B; E)$ remains positive.

In the case where Eve’s channel is superior, advantage distillation \[23\]-\[26\] can be used. There, an authenticated public channel is used by Alice and Bob to improve their mutual information. Otherwise, reverse reconciliation is sufficient to produce a key.
**Figure 5. Alice’s loss.** Changes in von Neumann mutual information as loss is introduced at Alice’s detectors, calculated using the covariance matrix. \( K = I(A; B) - I(B; E) \) becomes negative before total loss is reached.

**Figure 6. Bob’s loss.** Changes in von Neumann mutual information as loss is introduced at Bob’s detectors, calculated using the covariance matrix. As long as Bob receives some of the signal sent to him, a key can be produced.
Towards quantum key distribution with noisy communication sources

Figure 7. Loss before interception. Changes in von Neumann mutual information with equal loss added at Bob and Eve’s detectors, this simulates loss added before Eve’s interception. In this final case, communication is secure for nonzero transmittance. This is relevant for wireless scenarios, as then Eve will not realistically be able to detect every part of the signal that is not detected by Alice and Bob.

These results were compared to the outputs of Monte Carlo simulations of the protocol that were performed using QuTiP [27, 28], with Shannon entropy calculations performed on bit strings derived from measurements recorded by Alice, Bob and Eve. When loss is introduced on Alice’s channel, or in Bob’s channel before or after interception, as shown in Figure 8 changes in conditional mutual information values derived from bit strings mirror the curves calculated through the covariance matrix, given in Figures 5-7. As in previous work [8], it is expected that the von Neumann entropy is of greater magnitude, due to the presence of discord in the system.
Figure 8. Simulation results. Shannon mutual information measurements calculated using bit strings produced through simulation, these each follow the trends predicted by the covariance matrix calculations.

6. Conclusions

Calculating the final covariance matrix of the system shows that the dependency on displacement, observed in the vector describing the input state, is removed. This means that the bounds on the key rate also have no displacement dependency. Therefore the thermal state protocol can be generalised to include displaced thermal sources without sacrificing the key rate or security. When loss was introduced into the system for Alice, Alice and Bob were eventually put into an inferior position compared to Eve, so effort should be made to minimise loss across this section of the system in experimental work. However, loss in any case still allowed a key to be produced through advantage distillation. In future work, the protocol will be implemented experimentally using software-defined radios, allowing realistic noise and loss to be described. This would allow the creation of a real key via privacy amplification, showing it is experimentally possible to produce keys using this protocol using easily accessible equipment.

Acknowledgements

This work was undertaken on ARC4, part of the High Performance Computing facilities at the University of Leeds, UK. DJ is supported by the Royal Society and also a University Academic Fellowship. The data used in Figure 8 is available at https://doi.org/10.5518/1056.
Towards quantum key distribution with noisy communication sources

References

[1] Charles H. Bennett, François Bessette, Gilles Brassard, Louis Salvail, and John Smolin. Experimental quantum cryptography. In *Proceedings of the Workshop on the Theory and Application of Cryptographic Techniques on Advances in Cryptology, EUROCRYPT ’90*, pages 253–265, Berlin, Heidelberg, 1991. Springer-Verlag.

[2] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621–669, May 2012.

[3] T. C. Ralph. Continuous variable quantum cryptography. *Physical Review A*, 61(1), Dec 1999.

[4] Bing Qi, Philip G. Evans, and Warren P. Grice. Passive state preparation in the gaussian-modulated coherent-states quantum key distribution. *Physical Review A*, 97(1), Jan 2018.

[5] Elizabeth Newton, Anne Ghesquiére, Freya L Wilson, Benjamin T H Varcoe, and Martin Moseley. Quantum secrecy in thermal states. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 52(12):125501, May 2019.

[6] Elizabeth Newton, Anne Ghesquiére, Freya L Wilson, Raoul F Guiazone, Benjamin T H Varcoe, and Martin Moseley. Quantum secrecy in thermal states II. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 53(20):205502, Sep 2020.

[7] Anne Ghesquiére and Benjamin T H Varcoe. Quantum secrecy in thermal states III. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 54(2):025501, Jan 2021.

[8] Adam Walton, Anne Ghesquiere, George Brumpton, David Jennings, and Benjamin T H Varcoe. Thermal state quantum key distribution. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 2021.

[9] Flavio Augusto Paes De Oliveira, Myungshik S. Kim, Peter L. Knight, and Vladimir Bužek. Properties of displaced number states. *Phys. Rev. A*, 41:2645–2652, Mar 1990.

[10] Sammy Ragy and Gerardo Adesso. Unveiling the hanbury brown and thwiss effect through renyi entropy correlations. *Physica Scripta Volume T*, T153, 10 2012.

[11] Rodney Loudon. Photon bunching and antibunching. *Physics Bulletin*, 27(1):21–23, Jan 1976.

[12] Frederic Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[13] Frederic Grosshans, Gilles Van Assche, Jerome Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421:238–241, 2003.

[14] Bing Qi, Lei-Lei Huang, Li Qian, and Hoi-Kwong Lo. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A*, 76:052323, Nov 2007.

[15] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Coherent-state quantum key distribution without random basis switching. *Phys. Rev. A*, 73:022316, Feb 2006.

[16] Ce-by license. [https://creativecommons.org/licenses/by/4.0/](https://creativecommons.org/licenses/by/4.0/)

[17] Christian Weedbrook, Stefano Pirandola, and Timothy C. Ralph. Continuous-variable quantum key distribution using thermal states. *Phys. Rev. A*, 86:022318, Aug 2012.

[18] Alexander G. Mountogiannakis, Panagiotis Papanastasiou, Boris Braverman, and Stefano Pirandola. Composably secure data processing for gaussian-modulated continuous variable quantum key distribution. *Physical Review Research*, November 2021. Accepted version. The code for data-processing is available on github at [https://github.com/softquanta/homCVQKD](https://github.com/softquanta/homCVQKD).

[19] Anthony Leverrier. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.*, 114:070501, Feb 2015.

[20] Nitin Jain, Hou-Man Chin, Hossein Mani, Cosmo Lupo, Dino Solar Nikolic, Arne Kordts, Stefano Pirandola, Thomas Brochmann Pedersen, Matthias Kolb, Bernhard Ömer, Christoph Pacher, Tobias Gehring, and Ulrik L. Andersen. Practical continuous-variable quantum key distribution
with composable security, 2021, arXiv:2110.09262 [quant-ph].

[21] Anthony Leverrier, Frederic Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Phys. Rev. A*, 81:062343, Jun 2010.

[22] Raul Garcia-Patron Sanchez and Nicolas J. Cerf. Quantum information with optical continuous variables: from bell tests to key distribution. 2007, PhD Thesis, Université Libre de Bruxelles.

[23] Ueli Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[24] Frederic Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables, 2002.

[25] Ueli Maurer and Stefan Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Transactions on Information Theory*, 45(2):499–514, 1999.

[26] Shengli Liu, Henk Tilborg, and Marten van Dijk. A practical protocol for advantage distillation and information reconciliation. *Des. Codes Cryptography*, 30:39–62, 08 2003.

[27] Jan R. Johansson, Paul D. Nation, and Franco Nori. Qutip: An open-source python framework for the dynamics of open quantum systems. *Computer Physics Communications*, 183(8):1760–1772, Aug 2012.

[28] Jan R. Johansson, Paul D. Nation, and Franco Nori. Qutip 2: A python framework for the dynamics of open quantum systems. *Computer Physics Communications*, 184(4):1234–1240, Apr 2013.

[29] Adam Walton, Anne Ghesquière, David Jennings, and Ben Varcoe. Displaced thermal state qkd simulation data set: Mutual information changes with loss. doi: [https://doi.org/10.5518/1056](https://doi.org/10.5518/1056). *University of Leeds*, 2021.