PAPER • OPEN ACCESS

Quantum secrecy in thermal states II

View the article online for updates and enhancements.

Quantum secrecy in thermal states II

**Elizabeth Newton[1], Anne Ghesquière[1] , Freya L Wilson[1],
Raoul F Guiazon[1] , Benjamin T H Varcoe[1,3] and Martin Moseley[2]**

[1] Quantum Experimental Group, School of Physics and Astronomy, University of Leeds, Leeds LS2 9JT, United Kingdom
[2] Airbus Defense & Space, Germany

E-mail: b.varcoe@leeds.ac.uk

CrossMark

Abstract

In this paper we consider a scheme for cryptographic key distribution based on a variation of continuous variable quantum key distribution called central broadcast. In the continuous variable central broadcast scheme, security arises from discord present in the Hanbury Brown and Twiss effect from a thermal source. The benefit of this scheme is that it expands the range of frequencies into the microwave regime. Longer wavelengths—where the thermal photon number is higher and correlations remain robust over long distances—may even be preferable to optical wavelengths. Assuming that Alice controls the source but not the distribution of the light (e.g. satellite broadcasts), then we demonstrate that the central broadcast scheme is robust to an entangling cloner attack. We establish the security of the protocol both experimentally and theoretically.

(Some figures may appear in colour only in the online journal)

Quantum key distribution (QKD) is rapidly gaining widespread acceptance [1] as a method of secure key exchange and several high bandwidth devices have been demonstrated. However, the connection between the core network and the edge devices remains a weak link. For the end user, wireless access is the ideal use model. The user interface must be both inexpensive and accessible without compromising security and maintaining the ability to work on scales of the order of metres to tens of metres.

Recently, the potential of thermal states for QKD has been established [2, 3]. Although thermal states have sometimes been described as too noisy [4, 5], they exhibit Hanbury Brown and Twiss correlations which have been found to exhibit positive discord [6], a necessary condition for QKD [7].

Consider a central broadcast protocol in which the radiation is split between two parties, who now have correlated signals from which they can build a key. A typical central broadcast scheme is shown on figure 1. Another advantage to using thermal states is that they are easy and low-cost to produce. Whereas large-scale implementations of QKD such as those described above require specific infrastructure, thermal states central broadcasting protocols can be implemented over short distances, with low-power devices.

In the scheme proposed in [2], a thermal source is incident on a beamsplitter, with one output port connected to Alice and the other to Bob. Alice controls the source, the beamsplitter and the channels from the source to their detector, via the splitter. The eavesdropper is limited to the channel leading from the splitter to Bob and therefore, has an equal rank to Bob. We found that there is both a positive key rate and positive discord between the legal parties, both at optical frequencies (experimental result) and microwave frequencies (theoretical analysis).

In the present paper, as illustrated in figure 2, Alice and Eve switch places, giving Eve control of the higher level channel. This provides Eve with greater knowledge of the states making up the thermal radiation. She can intercept and resend bunched pairs at her leisure, pairs which are indistinguishable from

---

[3] Author to whom any correspondence should be addressed.

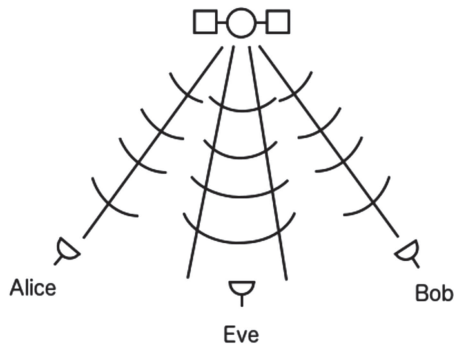J. Phys. B: At. Mol. Opt. Phys. **53** (2020) 205502

E Newton *et al*

Figure 1. In this situation, a satellite beams down a signal, which is received by Alice, Bob and Eve. Eve can have a very large portion of the signal, but she does not control the signal being emitted.
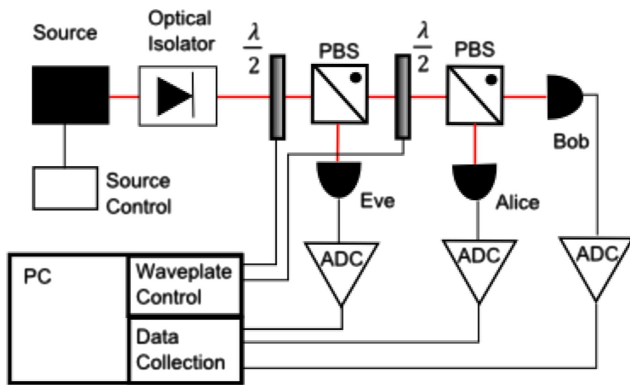

Figure 2. This is the schematic for this iteration of the protocol. A combination half-wave plate $\lambda/2$ and polarising beamsplitter is used to make a variable transmittance beamsplitter. Part of the signal is transmitted to Eve, and the other part goes through the same assembly to split between Alice and Bob. Having variable beamsplitters is especially important so that we can check the security of the protocol even if most of the signal is detected by Eve. Each signal is detected with photodiodes, and the signal is fed to the oscilloscope via the analog to digital converters for data collection.

those radiated by the source. Fortunately, the security of a central broadcast protocol naturally arises from the correlations within the pairs. Their origin itself is irrelevant. As a result, the protocol allows for quantum secure key to be distributed, even with Eve on the superior channel.

In the following, we describe the protocol and its modelling in more details. We use an optical experiment so that the eavesdropper channel is uncluttered by extraneous sources of noise. In microwave, it becomes difficult to differentiate Eve from all other sources of noises. The optical regime is the model of the perfect microwave experiment. Then we allow higher levels of noise in the theoretical modelling.

1. Protocol

This protocol is illustrated in figure 1. A source (for instance a trusted satellite) emits thermal radiation which is picked by the legal parties and the eavesdropper. We can consider that Eve can access quite a large portion of the signal, intercepting much of what should go to Alice and Bob. We model this by

giving Eve an entangling cloner, so she can divert as much of the signal to her as convenient. However, we consider that the source is trusted; this means that the eavesdropper does not use the satellite to relay her own signal.

We express the protocol formally as follows:

- Alice creates a beam from a trusted thermal source.
- On the way to their trusted beamsplitter with transmittance η_2, the signal is interfered with by Eve, via an entangling cloner denoted η_1.
- Alice uses η_2 to divert part of the signal to her detector and send the rest on to Bob.
- Similarly to [2], the bunched nature of the pairs coming out of η_1 means that fluctuations present at Alice's detector are correlated with those at Bob's detector.
- To derive their data, Alice and Bob slice these fluctuations as convenient; as an example, a fluctuation above the mean could be a 1 and a fluctuation below the mean, a 0.
- Like any QKD scheme, our protocol requires quantum correlations. To confirm that the signal from Alice and Bob are correlated is done through verifying the thermal nature of their signal. Thus, Alice sends Bob small chunks of data for him to perform a $g^{(2)}(0)$ calculation. A $g^{(2)}(0) > 1$ means that the signal is thermal.
- Alice and Bob now have a stream of independent and randomly correlated bits from which they can derive a key, the security of which they can improve with cascade and advantage distillation, as per any QKD scheme.

This scheme was implemented as shown in figure 2. A thermal source shines onto a beamsplitter which is controlled by the eavesdropper and therefore, allows her to capture as much of the signal as she wants. This is the same situation as that described in figure 1, where the eavesdropper can receive most of the signal, but does not control the source. In order to simulate high levels of noise, we consider two attenuator channels between η_2 and the legal parties, equivalent to adding a beamsplitter of transmittance η_3 between η_2 and Alice (η_4 for Bob), with an input state of variance N_3 (and N_4) at the second input arm.

Once again, this is not a prepare-and-send scheme. Alice controls the source, but the process of splitting pairs happening at the beamsplitter is stochastic, therefore unpredictable. Eve has no access to the channels between η_2 and either Alice or Bob, nor any control over their detectors.

Maurer and Wolf [8] have proved a theorem providing conditions to be satisfied for a scheme such as ours to be secure. The theorem reads as follows:

[quote]

Theorem 1. *In scenario 1, the following conditions are equivalent:*

(a) $I(A : B|E) > 0$
(b) $K(A : B \parallel E) > 0$
(c) $I(A : B \downarrow E) > 0$

[end quote] [16] where $K(A : B \parallel E)$ is the secret key rate. The third condition is actually the most restrictive. $I(A : B \downarrow E)$ is the intrinsic conditional mutual information; it determines

the unreducible amount of conditional mutual information between Alice and Bob, regardless of any attempts by Eve at acquiring more information through local operations; in other words, it is information inaccessible to Eve. Furthermore, it satisfies

$$I(A : B\downarrow E) < I(A : B|E),$$

which makes it a tighter condition on the secret key rate.

We can see its relation to the quantum discord if we recall that the latter, $D(B|A)$, is defined as the difference between the mutual information $I(A : B)$ and the classical mutual information $J(B|A)$ (or $J(A|B)$). $I(A : B)$ quantifies all possible correlations between Alice and Bob, but $J(B|A)$ quantifies those measured by local operations at Alice's and Bob's sites. Therefore, it can be understood as the intrinsic conditional mutual information as described previously. Let us therefore, rewrite the theorem as:

Theorem 2. *In our central broadcast scheme, the following conditions are equivalent:*

(a) $I(A : B|E) > 0$
(b) $K(A : B \parallel E) > 0$
(c) $D(B|A) > 0$

It is therefore enough in principle, to demonstrate that either condition is satisfied. We shall however, prove two, namely the positivity of the conditional mutual information and that of the discord. The latter will allow us to demonstrate the quantum nature of the secrecy.

1.1. Theoretical modelling

Let us recall that thermal states can be modelled using Gaussian statistics, which makes them easily defined and manipulated through their first and second moments [9, 10]. The former are contained in the displacement vector $\langle \hat{r} \rangle$, where $\hat{r}$ is the system's operator, and ρ the state's density operator. The second moments are contained in the covariance matrix γ defined as

$$\gamma_{ij} = \mathrm{Tr}\left[\rho\left\{(\hat{r}_i - \langle \hat{r}_i \rangle), (\hat{r}_j - \langle \hat{r}_j \rangle)\right\}\rho\right],$$

where we write the anti-commutator using {}. A thermal state has covariance matrix $\gamma_{\mathrm{in}} = 2(\bar{n} + 1)\boldsymbol{I}$, where $\bar{n}$ is the average photon number and $\boldsymbol{I}$ the 2×2 identity matrix, and null displacement. We consider single mode states, which is appropriate since we consider narrowband detectors.

The beamsplitters are modelled as

$$\boldsymbol{V}_i = \begin{pmatrix} \sqrt{\eta_i}\boldsymbol{I} & \mu_i\boldsymbol{I} \\ -\mu_i\boldsymbol{I} & \sqrt{\eta_i}\boldsymbol{I} \end{pmatrix},$$

where η_i is the transmittance and $\mu_i = \sqrt{1 - \eta_i}$ represents the noise. They act on the state as $\gamma_{\mathrm{out}} = \boldsymbol{V}\gamma_{\mathrm{in}}\boldsymbol{V}^{\mathrm{T}}$.

The input state at the first beamsplitter contains the thermal source and Eve's source; it has covariance matrix and displacement vector

$$\gamma_{\mathrm{in}} = \begin{pmatrix} V_{\mathrm{s}}^x & 0 & 0 & 0 \\ 0 & V_{\mathrm{s}}^p & 0 & 0 \\ 0 & 0 & V_{\mathrm{e}}^x & 0 \\ 0 & 0 & 0 & V_{\mathrm{e}}^p \end{pmatrix} \quad \mathbf{r}_{\mathrm{in}} = (x_{\mathrm{s}}; p_{\mathrm{s}}; x_{\mathrm{e}}; p_e)^{\mathrm{T}},$$

where $(V_{\mathrm{s}}^x, V_{\mathrm{s}}^p, x_{\mathrm{s}}, p_{\mathrm{s}})$ are the source parameters and $(V_{\mathrm{e}}^x, V_{\mathrm{e}}^p, x_{\mathrm{e}}, p_{\mathrm{e}})$ the eavesdropper's. The variances are given in shot noise units (SNU). We note the structure of the covariance matrix as $\gamma_{\mathrm{in}} = \gamma_{\mathrm{source}} \oplus \gamma_{\mathrm{Eve}}$. The two empty sub-matrices would represent potential pre-existing correlations between the source and Eve, which in our set-up, is unrealistic.

The output of the second beamsplitter is

$$\gamma_{\mathrm{out}} = \begin{pmatrix} \tilde{\gamma_b} & \tilde{\gamma_{ab}} & \tilde{\gamma_{eb}} \\ \tilde{\gamma_{ab}} & \tilde{\gamma_a} & \tilde{\gamma_{ea}} \\ \tilde{\gamma_{eb}} & \tilde{\gamma_{ea}} & \tilde{\gamma_e} \end{pmatrix}.$$

We make the channel between η_2 and Alice, and between η_2 and Bob thermal noise channels by inputting states of variance N_3 on Alice's branch and N_4 on Bob's as

$$N_i = \frac{\eta_i\chi_i}{1 - \eta_i}, \quad \text{with} \quad \chi_i = \frac{1 - \eta_i}{\eta_i} + \epsilon_i,$$

with $i = 3, 4$ and ϵ_i the channel excess noise [10]. The input state at η_3 and η_4 is then

$$\gamma_{\mathrm{int}} = \begin{pmatrix} N_3 & 0 \\ 0 & N_3 \end{pmatrix} \bigoplus \gamma_{\mathrm{out}} \bigoplus \begin{pmatrix} N_4 & 0 \\ 0 & N_4 \end{pmatrix},$$

where γ_{out} is the state at the output of η_2, the first block sub-matrix is the input state at η_3 and the last sub-matrix, the input state at η_4.

The output covariance matrix is

$$\Gamma_{\mathrm{out}} = \begin{pmatrix} \tilde{\Gamma_v} & \tilde{\Gamma_{va}} & \tilde{\Gamma_{ve}} & \tilde{\Gamma_{vb}} & \tilde{\Gamma_{vv'}} \\ \tilde{\Gamma_{va}} & \tilde{\Gamma_a} & \tilde{\Gamma_{ea}} & \tilde{\Gamma_{ab}} & \tilde{\Gamma_{av'}} \\ \tilde{\Gamma_{ve}} & \tilde{\Gamma_{ea}} & \tilde{\Gamma_e} & \tilde{\Gamma_{eb}} & \tilde{\Gamma_{ev'}} \\ \tilde{\Gamma_{vb}} & \tilde{\Gamma_{ab}} & \tilde{\Gamma_{eb}} & \tilde{\Gamma_b} & \tilde{\Gamma_{bv'}} \\ \tilde{\Gamma_{vv'}} & \tilde{\Gamma_{av'}} & \tilde{\Gamma_{ev'}} & \tilde{\Gamma_{bv'}} & \tilde{\Gamma_{v'}} \end{pmatrix}$$

where the block sub-matrices are given in the appendix A.

The mutual information $I(A : B)$ is given by

$$I(A : B) = S(\Gamma_a) + S(\Gamma_b) - S(\Gamma_{ab}),$$

where $S(x)$ is the von Neumann entropy and Γ_i the covariance matrices of A, B and AB respectively. The von Neumann entropy is given by

$$S(x) = \sum_{i=1}^{N} \left(\frac{x_i + 1}{2}\right)\log\left(\frac{x_i + 1}{2}\right) - \left(\frac{x_i - 1}{2}\right)\log\left(\frac{x_i - 1}{2}\right)$$

where x_i are the symplectic eigenvalues of Γ. The conditional mutual information is

$$I(A : B|E) = S(\Gamma_{ae}) + S(\Gamma_{be}) - S(\Gamma_e) - S(\Gamma_{abe}).$$

The discord is defined explicitly as

$$D(B|A) = S(\Gamma_a) - S(\Gamma_{ab}) + \min_{\Gamma_0} S(\Gamma_{b|x_A})$$

where $\Gamma_{b|x_A}$ is the covariance matrix of B conditioned by a
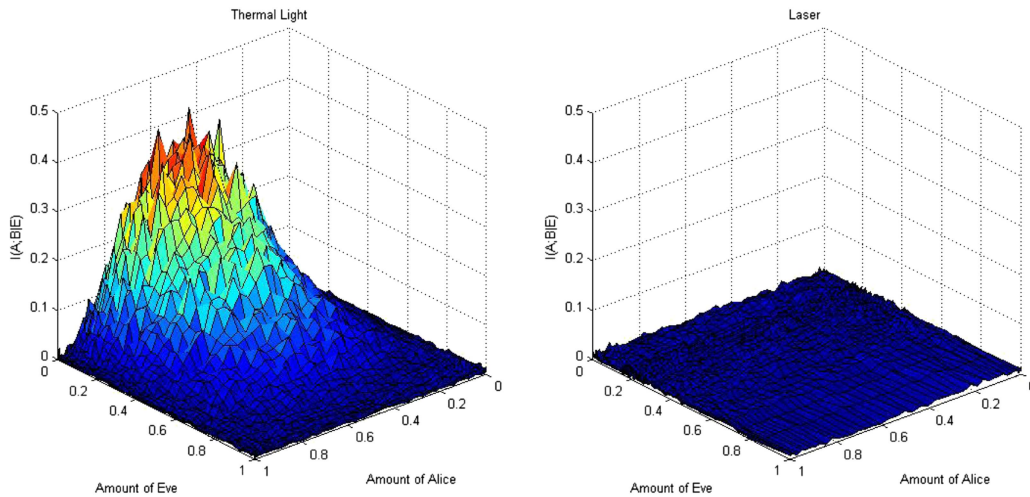
Figure 3. Conditional mutual information for thermal states (left) versus coherent states (right). We can see that when $\eta_1 \to 1$, so when there is no amount of Eve coming between the legal parties, the conditional mutual information peaks.

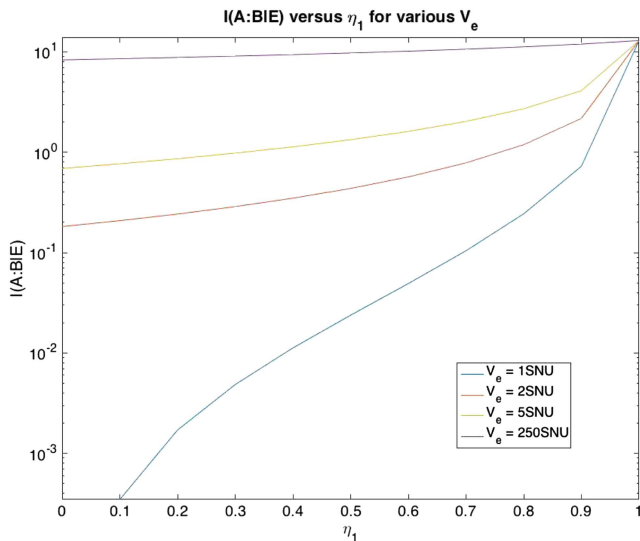**Figure 4.** We plot a numerical simulation of the conditional mutual information $I(A : B|E)$ against η_1, with $\eta_2 = 0.5$, $\eta_3 = \eta_4 = 0.2$ and $\epsilon_3 = \epsilon_4 = 10^{-2}$. Using the Bose–Einstein distribution at 30 GHz and $T = 300$ K, the input photon number is $\bar{n} = 1309$. At $\eta_2 = 0.5$, Alice and Bob share equal part of the signal.

homodyne measurement on A [11]

$$\Gamma_{b|x_A} = \Gamma_b - \Gamma_{ab}(X\Gamma_a X)^{-1}\Gamma_{ab}^T,$$

with $X = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ and $()^{-1}$ the pseudo-inverse.

2. Results and discussion

The protocol was realised experimentally, as described on figure 2. The thermal source is provided by a superluminescent diode coupled to an external cavity, making it a tuneable laser, run without any added modulation. The laser can be run separately in coherent or in thermal mode, and the thermality of the source was established in [2]. The source bandwidth

was measured at $\Delta\lambda = 0.4$ nm spread around a centre wavelength of $\lambda_0 = 780.09$ nm; this give a coherence time of $\tau_c = 4.8$ ps. The detectors are ThorLabs Det36A photodiodes with a bandwidth of 25 MHz, coupled to a LeCroy Waverunner 44xi oscilloscope of bandwidth 400 MHz; the combined integration time is 14 ns and the oscilloscope samples at 5 GSps. Thermal states are correlated in amplitudes, which can be measured in terms of the strength of the electric field and therefore, single photon detectors are not necessary.

The conditional mutual information is calculated from the sliced data strings using Shannon entropies $H(x) = -\sum p(x)\log(p(x))$ in terms of the measured frequencies $p(x)$.

Figure 3 shows that the scheme works experimentally as predicted. $I(A : B|E)$ is best as η_1 tends to 1, and at $\eta_2 = 0.5$, so when Alice and Bob gets equal shares of most of the thermal source signal. This corresponds to a situation where the eavesdropper is absent, and where there is minimal loss. As long as the $\eta_1 > 0.5$, the eavesdropper gets little of the signal and the advantage is to the legal parties. However, no matter how much signal Eve receives, the conditional mutual information is always positive, and never exhibits a sharp fall-off, typical of point-to-point schemes over the 3dB limit. This means that it is always possible to build key, albeit slowly. The key can be built from the data distributed using reconciliation schemes such as advantage distillation [12] and cascade [13].

Figure 3 allows us also to illustrate that this scheme cannot work in the coherent regime. As mentioned before in [2], coherent radiation is not bunched; therefore, it holds none of the intrinsic correlations contained in bunched pairs. There is no splitting of pairs occurring at the beamsplitters, because there are no such pairs; single photons travel through uncorrelated to Alice and Bob, who as a result can build no key from them. This is shown on the right-hand graph of the figure $I(A : B|E)$ remains constant, no matter how much Eve lets through, no matter the split between Alice and Bob.
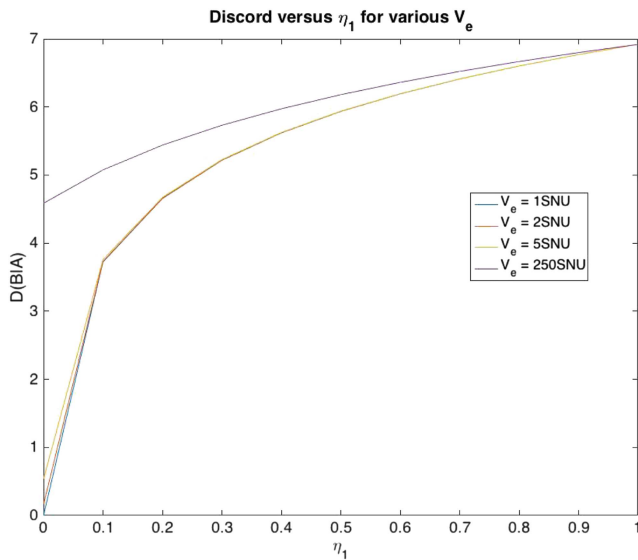
Figure 5. We plot a numerical simulation of the discord $D(B|A)$ against η_1, with $\eta_2 = 0.5$, $\eta_3 = \eta_4 = 0.2$ and $\epsilon_3 = \epsilon_4 = 10^{-2}$ and initial photon number $\bar{n} = 1309$.

Figure 6. On this figure, we see a bunched pair arriving at one input arm of the beamsplitter, and the possible outputs: $P(2_3, 0_4)$, $P(0_3, 2_4)$ or $P(1_3, 1_4)$. We show only one possible way to split the pair (photon 2 on arm 4 and photon 1 on arm 3) but the converse is obviously possible.

Let us now compare these results to those obtained through our theoretical modelling.

Figure 4 shows the behaviour of the conditional mutual information as Eve lets more and more of the signal through. When compared with figure 3, we can see that as $\eta_1 \to 1$, so as the amount of Eve's signal vanishes, $I(A:B|E)$ increases. The simulations obtained through our theoretical modelling match the experimental results. Furthermore, $I(A:B|E)$ is always positive, so by virtue of our theorem, there is always secrecy.

We can also explore how the initial state of Eve influences the secrecy between Alice and Bob. For that, we vary V_e and see that as it increases, $I(A:B|E)$ increases also. The reason for this, we have mentioned before and will detail further in the lines below.

Figure 5 illustrates the positivity of the discord, regardless of η_1. This means that there always are quantum correlations between Alice and Bob. This satisfies the third of the conditions from our theorem, and we can affirm quantum secrecy.

What is remarkable is the value of the discord when η_1 is null, so before Eve begins to let the source signal through. In this case, what is actually measured is the amount of quantum correlations within Eve's state. We have seen that the higher V_e is, the higher $I(A:B|E)$, but here we see that the discord follows a similar trend. This is particularly evident when $V_e = 250\,\text{SNU}$.

This is a result of the physics of thermal states and the reason why this scheme is secure even under Eve's intercept-and-resend. To understand this, let us step back and consider a single beamsplitter (input arms labelled 1 and 2, output arms labelled 3 and 4) with a thermal state at one input, as shown in figure 6.

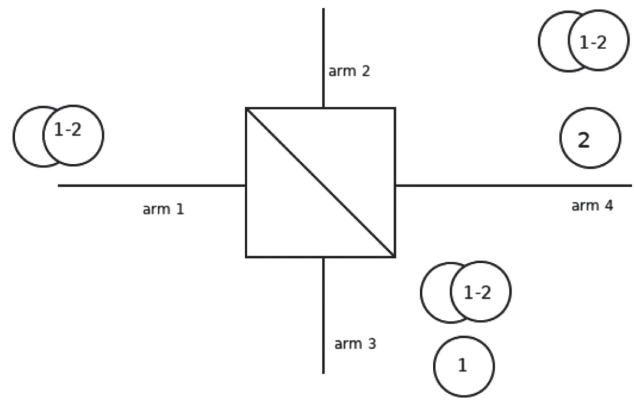Since it is bunched, there will be correlated photon pairs travelling into the beamsplitter. If both photons travel into the same input (say arm 1), we can expect three outputs [14]:

- both photons are travelling through on arm 3 $P(2_3, 0_4)$,
- both photons travel onto arm 4 $P(0_3, 2_4)$ or
- one photon for each arm $P(1_3, 1_4)$.

This corresponds to Eve inputting a vacuum or a coherent state at arm 2 and why we can in fact equate her to any loss in the channel.

On the other hand, if Eve inputs a thermal state as well, there is now a correlated pair of photons travelling into each input arm. This is illustrated in figure 7. This will gives us the following outputs: $P(4_3, 0_4)$, $P(0_3, 4_4)$, $P(2_3, 2_4)$, $P(3_3, 1_4)$, and $P(1_3, 3_4)$. The third case $P(2_3, 2_4)$, is three-degenerate; either both pairs get to the other side in one piece (which accounts for two degeneracies) or both pairs are split (the remaining degeneracy). This means that accounting for all possible outcomes, there are only two cases where there will not be at least one correlated pair travelling into η_2 to Alice and Bob: either one pair is split at η_1 and Eve gets three photons $P(3_3, 1_4)$ (mitigated by the fact that Eve would choose to let most of the signal through at η_1 in order not to be noticed) or both pairs are split at η_1, which is one of the $P(2_3, 2_4)$ degeneracies.

If $V_e = 1\,\text{SNU}$, then Eve inputs a vacuum state, and Alice and Bob build key solely from the pairs produced at the source. As a result, the discord is minimal at $\eta_1 \to 0$. If $V_e > 1\,\text{SNU}$, Eve's state can be regarded as thermal; in this case, she contributes pairs to those coming from the source. In fact, if the eavesdropper's input is too significant, the legal parties can build a quantum secure key, regardless of how much signal is coming from the source. As in any QKD, we expect that the eavesdropper will try to minimise her input, if only to escape detection. At best, she can hope to merely 'listen' in, in which case, her input is $V_e = 1\,\text{SNU}$. Yet, as soon as signal begins going through ($\eta_1 > 0.1$), the legal parties can build a quantum secure key, albeit slowly.

Let us point out that these plots have been obtained for very high level of noise on Alice's and Bob's branches. Indeed η_3 and η_4 are such that 80% of their signal is lost. Yet, even in this

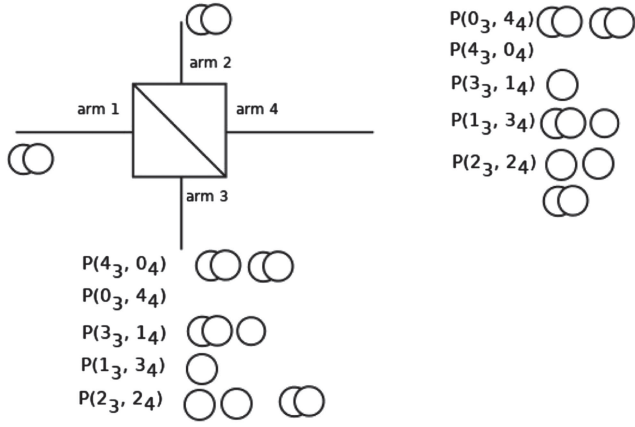J. Phys. B: At. Mol. Opt. Phys. **53** (2020) 205502

E Newton *et al*

Figure 7. This time, one bunched pair arrives at each arm of the beamsplitter, leading to the possible outputs: $P(4_3, 0_4)$, $P(0_3, 4_4)$, $P(2_3, 2_4)$, $P(3_3, 1_4)$, and $P(1_3, 3_4)$. On can see that the $P(2_3, 2_4)$ output can be arrived at either by splitting each input pair, or transmitting them intact.

case, the legal parties are able to construct a quantum secure key.

3. Concluding remarks

In our previous work, we demonstrated that a central broadcast protocol using thermal states is quantum secure. In the present work, we allowed the eavesdropper to access the higher channel and thus, to have more power and control over the signal than either of the legal parties. She can intercept and resend photons pairs at will, and she can hide in the noise effectively. However, we find that the conditional mutual information $I(A:B|E)$ is always positive, which means that Alice and Bob are able to build a secret key from their signal. Furthermore, the discord $D(B|A)$ is also always positive, so the secret key is quantum secure.

This protocol is secure as long as Alice and Bob have correlated pairs, which they show by checking that their $g^{(2)}(0) > 1$. As we have explained, the origin of the pairs itself (either the source or the eavesdropper) makes no difference to there being secrecy. The quantum discord shows that there are always correlations between Alice and Bob, even under Eve's influence.

This is the strength of this scheme. Even if Eve succeeds in hiding in the noise, if her input is not either vacuum or a perfect coherent state, she will contribute correlations to the pool which Alice and Bob can build key from, but she cannot know when or if these injected states have contributed to the key. Another option for Eve is to actually become the source; we explore this in a forthcoming publication.

This experiment was carried out at optical frequencies using a pseudo thermal source, however, the theoretical modelling was performed at values of $\bar{n}$ consistent with the microwave regime. Interferometers used in radio astronomy rely on the presence of thermal correlations being preserved over astronomical distances, and the results in this paper suggest that the results are highly portable to the microwave regime. Hence,

this method of key exchange appears to be a viable option for long distance key exchange.

Appendix A. Protocol 2

A.1. After η_2

The submatrices are as follows

$$\tilde{\gamma}_b = \begin{pmatrix} \eta_2 + \mu_2^2(\eta_1 V_s^x + \mu_1^2 V_e^x) & 0 \\ 0 & \eta_2 + \mu_2^2(\eta_1 V_s^p + \mu_1^2 V_e^p) \end{pmatrix}$$

$$\tilde{\gamma}_a = \begin{pmatrix} \mu_2^2 + \eta_2(\eta_1 V_s^x + \mu_1^2 V_e^x) & 0 \\ 0 & \mu_2^2 + \eta_2(\eta_1 V_s^p + \mu_1^2 V_e^p) \end{pmatrix}$$

$$\tilde{\gamma}_e = \begin{pmatrix} \mu_1^2 V_s^x + \eta_1 V_e^x & 0 \\ 0 & \mu_1^2 V_s^p + \eta_1 V_e^p \end{pmatrix}$$

$$\tilde{\gamma}_{ea} = \begin{pmatrix} -\mu_1\sqrt{\eta_1}\sqrt{\eta_2}(V_s^x - V_e^x) & 0 \\ 0 & -\mu_1\sqrt{\eta_1}\sqrt{\eta_2}(V_s^p - V_e^p) \end{pmatrix}$$

$$\tilde{\gamma}_{eb} = \begin{pmatrix} -\mu_1\sqrt{\eta_1}\mu_2(V_s^x - V_e^x) & 0 \\ 0 & -\mu_1\sqrt{\eta_1}\mu_2(V_s^p - V_e^p) \end{pmatrix}$$

$$\tilde{\gamma}_{ab} = \begin{pmatrix} \mu_2\sqrt{\eta_2}(\eta_1 V_s^x + \mu_1^2 V_e^x - 1) & 0 \\ 0 & \mu_2\sqrt{\eta_2}(\eta_1 V_s^p + \mu_1^2 V_e^p - 1) \end{pmatrix}.$$

A.2. After η_3 and η_4

The submatrices are as follows

$$\tilde{\Gamma}_e = \begin{pmatrix} \langle \tilde{X}_e^2 \rangle & 0 \\ 0 & \langle \tilde{P}_e^2 \rangle \end{pmatrix},$$

$$\tilde{\Gamma}_a = \begin{pmatrix} \mu_3^2 N_3 + \eta_3 \langle \tilde{X}_a^2 \rangle & 0 \\ 0 & \mu_3^2 N_3 + \eta_3 \langle \tilde{P}_a^2 \rangle \end{pmatrix}$$

$$\tilde{\Gamma}_b = \begin{pmatrix} \mu_4^2 N_4 + \eta_4 \langle \tilde{X}_b^2 \rangle & 0 \\ 0 & \mu_4^2 N_4 + \eta_4 \langle \tilde{P}_b^2 \rangle \end{pmatrix},$$

$$\tilde{\Gamma}_v = \begin{pmatrix} \eta_3 N_3 + \mu_3^2 \langle \tilde{X}_a^2 \rangle & 0 \\ 0 & \eta_3 N_3 + \mu_3^2 \langle \tilde{P}_a^2 \rangle \end{pmatrix}$$

$$\tilde{\Gamma}_{v'} = \begin{pmatrix} \eta_4 N_4 + \mu_4^2 \langle \tilde{X}_b^2 \rangle & 0 \\ 0 & \eta_4 N_4 + \mu_4^2 \langle \tilde{P}_b^2 \rangle \end{pmatrix}$$

$$\tilde{\Gamma}_{ea} = \begin{pmatrix} \sqrt{\eta_3} \langle \tilde{X}_a \tilde{X}_e \rangle & 0 \\ 0 & \sqrt{\eta_3} \langle \tilde{P}_a \tilde{P}_e \rangle \end{pmatrix}$$

$$\tilde{\Gamma}_{eb} = \begin{pmatrix} \sqrt{\eta_4} \langle \tilde{X}_b \tilde{X}_e \rangle & 0 \\ 0 & \sqrt{\eta_4} \langle \tilde{P}_b \tilde{P}_e \rangle \end{pmatrix}$$

J. Phys. B: At. Mol. Opt. Phys. **53** (2020) 205502

E Newton *et al*

$$\tilde{\Gamma_{ab}} = \begin{pmatrix} \sqrt{\eta_3}\sqrt{\eta_4}\left\langle \tilde{X}_a\tilde{X}_b\right\rangle & 0 \\ 0 & \sqrt{\eta_3}\sqrt{\eta_4}\left\langle \tilde{P}_a\tilde{P}_b\right\rangle \end{pmatrix},$$

$$\tilde{\Gamma_{vv'}} = \begin{pmatrix} -\mu_3\mu_4\left\langle \tilde{X}_a\tilde{X}_b\right\rangle & 0 \\ 0 & -\mu_3\mu_4\left\langle \tilde{P}_a\tilde{P}_b\right\rangle \end{pmatrix}$$

$$\tilde{\Gamma_{vb}} = \begin{pmatrix} \mu_3\sqrt{\eta_4}\left\langle \tilde{X}_a\tilde{X}_b\right\rangle & 0 \\ 0 & \mu_3\sqrt{\eta_4}\left\langle \tilde{P}_a\tilde{P}_b\right\rangle \end{pmatrix},$$

$$\tilde{\Gamma_{av'}} = \begin{pmatrix} -\sqrt{\eta_3}\mu_4\left\langle \tilde{X}_a\tilde{X}_b\right\rangle & 0 \\ 0 & -\sqrt{\eta_3}\mu_4\left\langle \tilde{P}_a\tilde{P}_b\right\rangle \end{pmatrix}$$

$$\tilde{\Gamma_{va}} = \begin{pmatrix} \mu_3\sqrt{\eta_3}\left(\left\langle \tilde{X}_a^2\right\rangle - N_3\right) & 0 \\ 0 & \mu_3\sqrt{\eta_3}\left(\left\langle \tilde{P}_a^2\right\rangle - N_3\right) \end{pmatrix}$$

$$\tilde{\Gamma_{bv'}} = \begin{pmatrix} \mu_4\sqrt{\eta_4}\left(N_4 - \left\langle \tilde{X}_b^2\right\rangle\right) & 0 \\ 0 & \mu_4\sqrt{\eta_4}\left(N_4 - \left\langle \tilde{P}_b^2\right\rangle\right) \end{pmatrix}$$

$$\tilde{\Gamma_{ve}} = \begin{pmatrix} \mu_3\left\langle \tilde{X}_a\tilde{X}_e\right\rangle & 0 \\ 0 & \mu_3\left\langle \tilde{P}_a\tilde{P}_e\right\rangle \end{pmatrix},$$

$$\tilde{\Gamma_{ev'}} = \begin{pmatrix} -\mu_4\left\langle \tilde{X}_b\tilde{X}_e\right\rangle & 0 \\ 0 & -\mu_4\left\langle \tilde{P}_b\tilde{P}_e\right\rangle \end{pmatrix}.$$

ORCID iDs

Anne Ghesquière ![ORCID](https://orcid.org/0000-0003-1595-7473)
Raoul F Guiazon ![ORCID](https://orcid.org/0000-0002-2212-6232)
Benjamin T H Varcoe ![ORCID](https://orcid.org/0000-0001-7056-7238)

References

[1] Marks P 2007 Quantum cryptography to protect Swiss election *New Scientist* https://institutions.newscientist.com/article/dn12786-quantum-cryptography-to-protect-swiss-election/

[2] Newton E, Ghesquière A, Wilson F L, Varcoe B T H and Moseley M 2019 Quantum secrecy in thermal states *J. Phys. B: At. Mol. Opt. Phys.* **52** 125501

[3] Qi B, Evans P G and Grice W P 2018 Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution *Phys. Rev.* A **97** 012317

[4] Weedbrook C, Pirandola S, Lloyd S and Ralph T C 2010 *Phys. Rev. Lett.* **105** 110501

[5] Weedbrook C, Pirandola S and Ralph T C 2012 *Phys. Rev.* A **86** 022318

[6] Ragy S and Adesso G 2013 2013 *Phys. Scr.* T **153** 014052

[7] Pirandola S 2014 *Sci. Rep.* **4** 6956

[8] Maurer U M and Wolf S 1999 *IEEE Trans. Inf. Theory* **45** 499–514

[9] Eisert J and Plenio M 2003 *Int. J. Quant. Inf.* **1** 479

[10] Sanchez R G-P 2007 *PhD Thesis* Université Libre de Bruxelles

[11] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621

[12] Maurer U M 1993 *IEEE Trans. Inf. Theory* **39** 733–42

[13] Brassard G and Salvail L 1994 Secret-key reconciliation by public discussion *Advances in Cryptology—Eurocrypt '93* (Berlin: Springer) pp 410–23

[14] Loudon R 2000 *The Quantum Theory of Light* 3rd edn (Oxford: Oxford University Press)

[15] Newton E 2019 *Central Broadcast Quantum Key Distribution* University of Leeds (https://doi.org/10.5518/587)

[16] Even though this is a direct quote, we have adapted the notation to our scheme.